SR101EDUA Digital Learning Suite

KEYSIGHT

INSTALLATION GUIDE

Notices

Copyright Notice

Manual Part Number

SR101-90000

Edition

Edition 6, April 2025

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 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 DOCU- MENT 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

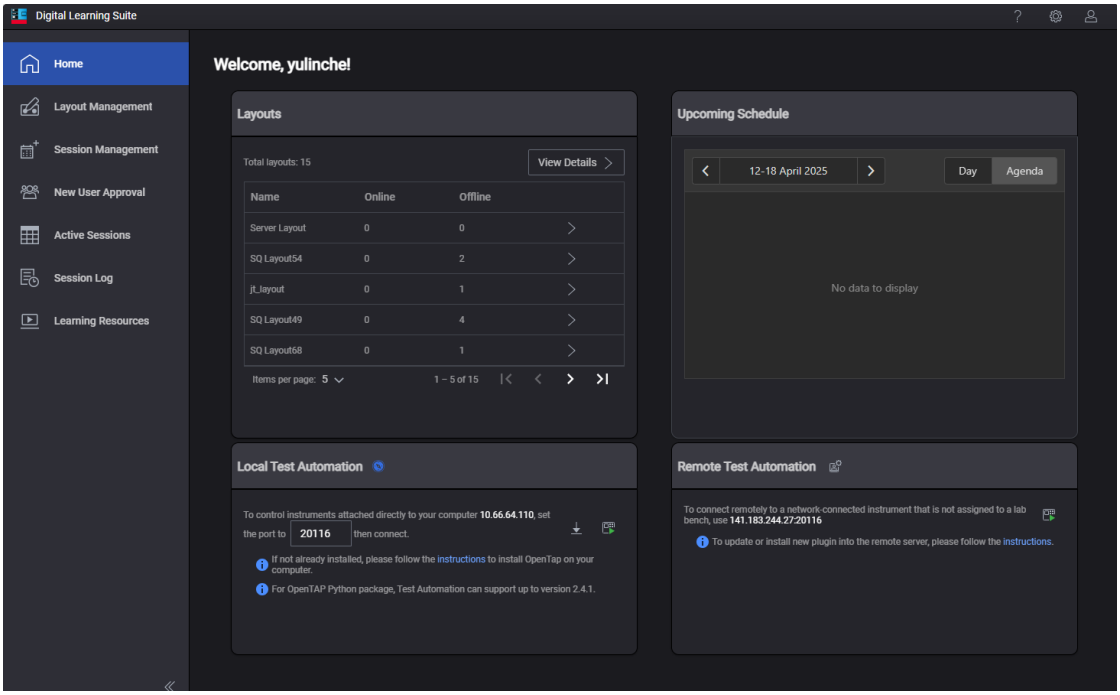
To contact Keysight for sales and technical support, refer to the support links on the following Keysight websites:

- Product-specific information and support, software, and documentation updates
  https://www.keysight.com/us/en/support/SR101EDUA/digital-learning-platform.html
- Worldwide contact information for repair and service
  www.keysight.com/find/assist

Table of Contents

Overview

The Keysight SR101EDUA Digital Learning Suite is a unified web-based digital learning platform with secure one-stop access to university engineering lab resources, measurement data analysis tools, and industry-relevant learning resources.



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 are 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 the 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 similar practical skills and application knowledge as industry engineers conducting their work in the lab today.

Intended Use of the Installation Guide

The Installation Guide is intended for use by lecturers and University Teaching Lab Managers as a guide to configure the software and other deployment settings for the Keysight SR101EDUA Digital Learning Suite.

Introduction

The Keysight SR101EDUA Digital Learning Suite is available as an Ubuntu Linux Virtual Machine (VM) image provided by Keysight. It is designed as a server software rather than a desktop software. There is no need to manually install the Digital Learning Suite (DLS) as the Ubuntu Linux VM image comes **pre-installed** with all the necessary software and is pre-configured to minimize setup steps.

For trial purposes, we recommend using the **Oracle VM VirtualBox Manager** to run the VM image. The Oracle VM VirtualBox is a desktop application-based user interface and is freely available as an Open Source Software under the terms of the GNU General Public License (GPL) version 2. Download the latest version here: Oracle VM VirtualBox.

Ensure that your computer has **more than 16 GB of RAM** available as the VM image is already configured to utilize 16 GB of your physical machine's RAM. If you intend to have more than **20 concurrent users,** we recommend increasing the RAM to **32 GB or higher** to accommodate the additional load.

The Ubuntu Linux VM provided with the Keysight SR101EDUA Digital Learning Suite can also run on a **Proxmox Virtual Environment (VE) server**, which is another virtualization platform. The Proxmox VE is a complete open-source platform that tightly integrates KVM hypervisor and LXC containers, software-defined storage, and networking functionality on a single platform, and easily manages high availability clusters and disaster recovery tools with the built-in web management interface.

Both VirtualBox and Proxmox have distinct features suitable for different use cases.

Types of Virtualization

- **VirtualBox** is a Type 2 hypervisor that runs on top of an existing operating system (host OS). It establishes a virtualization layer within the host OS, enabling the execution of virtual machines.
- **Proxmox** is a Type 1 hypervisor that operates directly on the hardware, creating a dedicated virtualization environment. It utilizes KVM (Kernel-based Virtual Machine) technology for running virtual machines.

In summary, VirtualBox is more suitable for individual users and desktop virtualization, providing a simpler and user-friendly experience. On the other hand, Proxmox is a robust virtualization and containerization platform primarily designed for data centres and enterprise environments. It offers advanced features and management capabilities.

If you are unfamiliar with virtual machines, consult your IT staff before starting.

System Requirements

NOTE See Introduction to get a basic overview of **VirtualBox** and **Proxmox**.

Item	Recommended	Minimum
RAM	32 GB RAM or higher	16 GB RAM or higher
Hard Disk Space	50 GB free disk space for the Digital Learning Suite pre-configured Virtual Machine	
Processor	64-bit, Quad-core CPU	
Operating System Requirements	Windows 10 or Proxmox Virtual Environment	
Virtual Machine Hypervisor Supported	Oracle VM VirtualBox Manager (Windows 10) version 7.0.4 Proxmox version 7.1-7.4	
Others	Requires Internet access	

NOTE The minimum requirement of 16 GB RAM is intended to cater to a maximum of 20 users. If there is a need to accommodate more users, we highly recommend modifying or enhancing the system configuration of the Ubuntu Virtual Machine accordingly.

Software Requirements

Required Third Party Software	For Windows 10 1 VirtualBox – https://www.virtualbox.org/ 2 FileZilla – https://filezilla-project.org/download.php?type=client 3 PuTTY – Latest release (0.78) For Proxmox Virtual Environment 1 FileZilla – https://filezilla-project.org/download.php?type=client 2 PuTTY – Latest release (0.78)
Supported LTI Compliant LMS Integration	Moodle v3.9 and above Canvas For other LTI compliant LMS platforms, please contact Keysight Technologies for further information.
Supported Web Browsers	Microsoft Edge v107.0.1418.62 and above Google Chrome v108.0.5359.94 and above Mozilla Firefox v107.0.1 and above

Get Started

Before you proceed with the setup and installation, take note of the following requirements:

- A valid SSL certificate for security purposes.
- Software licenses (see Software License).

Software License

NOTE

You need to download the software license for **both** modules:

- Hybrid Collaborative Learning Module (PW9300EDU)
- Test Sequencing and Control Module (KS8400EDU)

Trial License

NOTE

You need the host ID before you can obtain a trial license. See Step 8: Install License Files on how to retrieve the **host ID**.

Click on the links below to obtain a trial license:

- PW9300EDU
  PW9300EDU Trial License
- KS8400EDU
  KS8400EDU Trial License

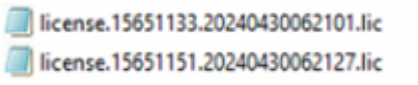
Full License

To obtain the full license for PW9300EDU and KS8400EDU, please contact your local Keysight representative.

NOTE

These license files are required when accessing the DLS application. Rename the files before you load or install them onto your PC.

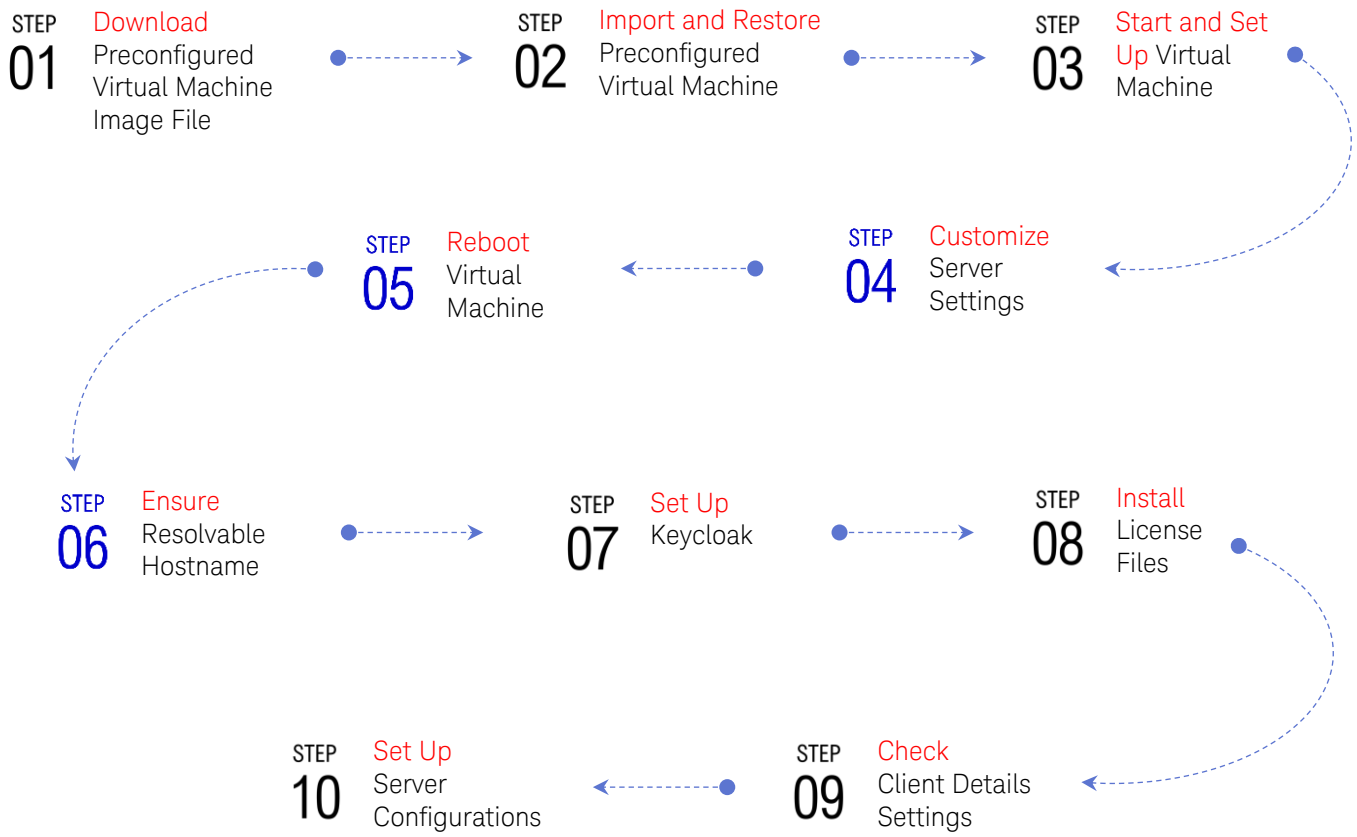
Download and save the license files to a folder on the Windows PC:



Overview: Installation Flow

This section will guide you through the steps to download, set up, and configure the virtualization platform for the Keysight SR101EDUA Digital Learning Suite.

NOTE You can skip **Steps 4** to **6** if you are not going to change your hostname and/or domain name.



NOTE See Introduction to get a basic overview of the different virtualization platforms: **VirtualBox** and **Proxmox**.

Step 1: Download Preconfigured Virtual Machine Image File

Depending on the virtualization platform you are using, download the image file here: https://www.keysight.com/us/en/lib/software-detail/computer-software/sr101edua-digital-learning-suite-and-180-days-trial-license.html

- VirtualBox Image File: *dls1v21_12Apr25.ova*
- Proxmox Image File: *vzdump-qemu-2903-12042025.vma.zst*

NOTE

Follow the steps below to verify the integrity of your download.

a On Windows, use the built-in **`certUtil`** command-line utility to compute the MD5 checksum on the file:

```
C:\> certUtil -hashfile <PATH_TO_FILE> <HASH_ALGORITHM>
```

MD5 checksum example: **`C:\> certUtil -hashfile C:\DLS.zst MD5`**

b Compare the computed MD5 checksum against the MD5 checksum on the download page: https://www.keysight.com/us/en/lib/software-detail/computer-software/sr101edua-digital-learning-suite-and-180-days-trial-license.html

---

Step 2: Import and Restore Preconfigured Virtual Machine

VirtualBox

NOTE

If VirtualBox is not installed/running on your Windows 10, follow steps **a** and **b** below to set up the Oracle VirtualBox on your PC before proceeding to import and restore the preconfigured VM.

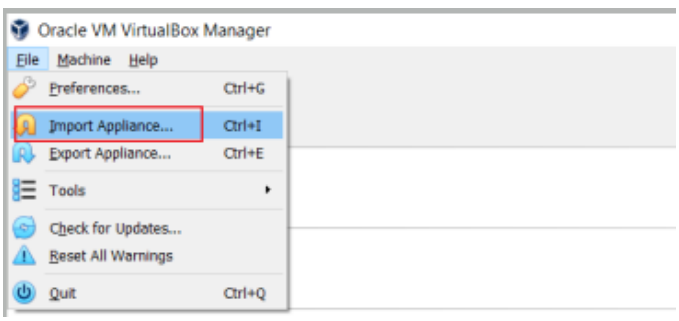
a Download the latest version of Oracle VM VirtualBox Manager here: Oracle VM VirtualBox.

b Refer to the User Manual and follow the instructions to install VirtualBox on a Windows host.

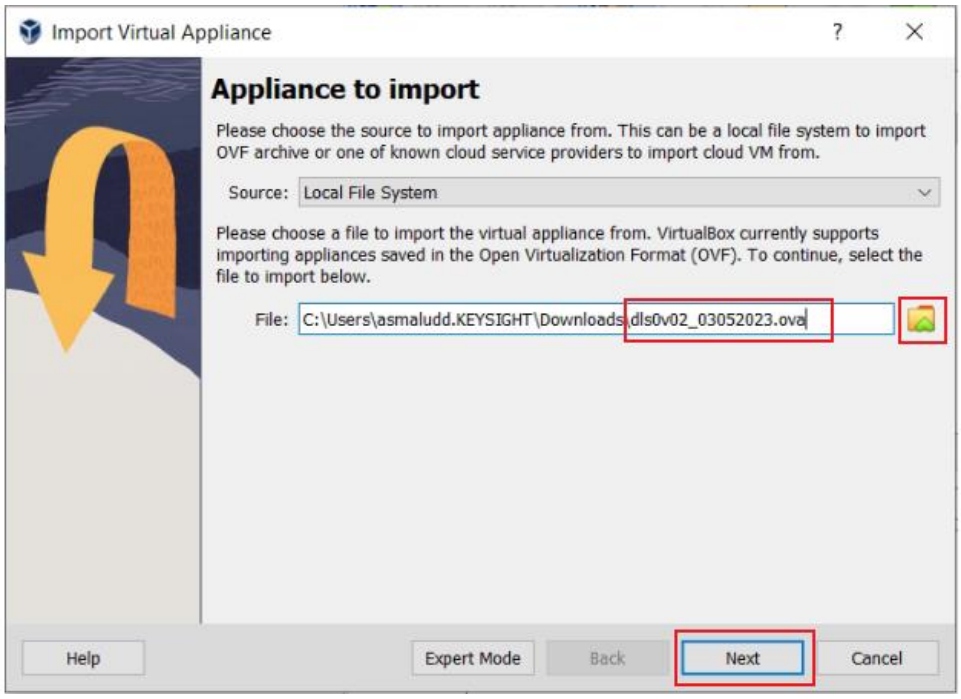
---

1 Click on the **Oracle VM VirtualBox** icon to launch the application.

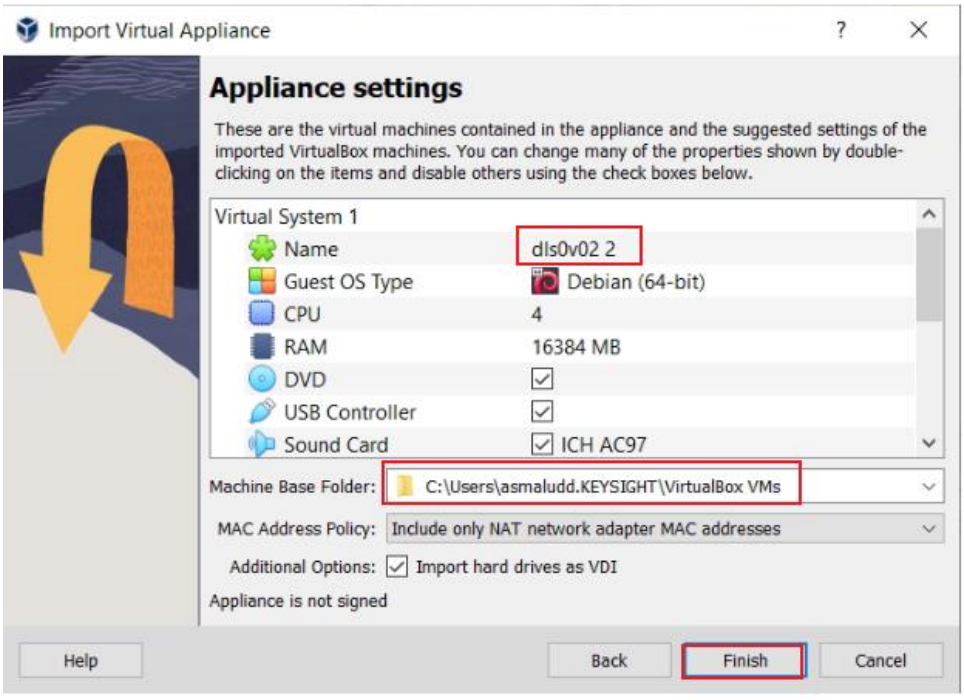
2 Go to **File** and click on **Import Appliance...**.



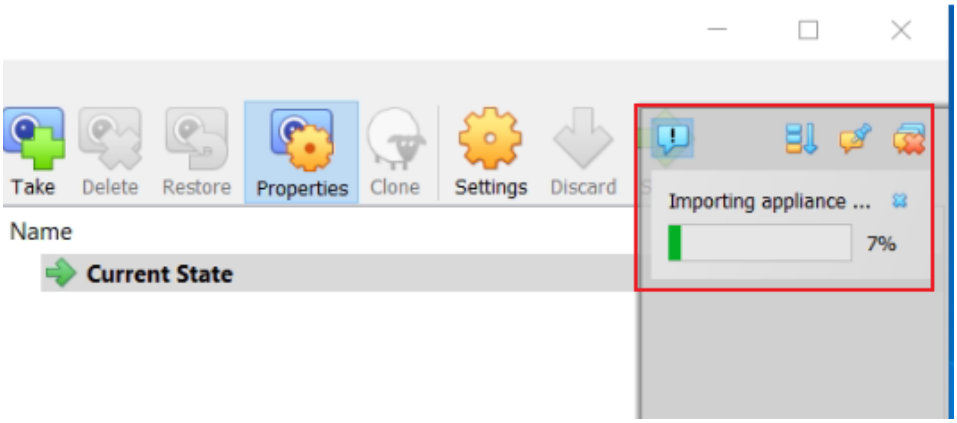
3 Browse to the folder where you have downloaded the VirtualBox image file and select *dls0v02_03052023.ova*. Click **Next** to proceed.



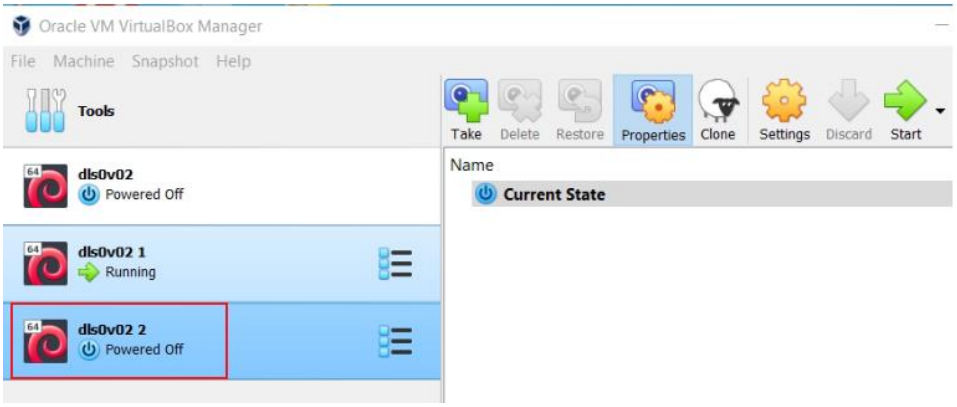
4 If required, change the name and default path of the Virtual Machine (VM) as shown below and click **Finish**.



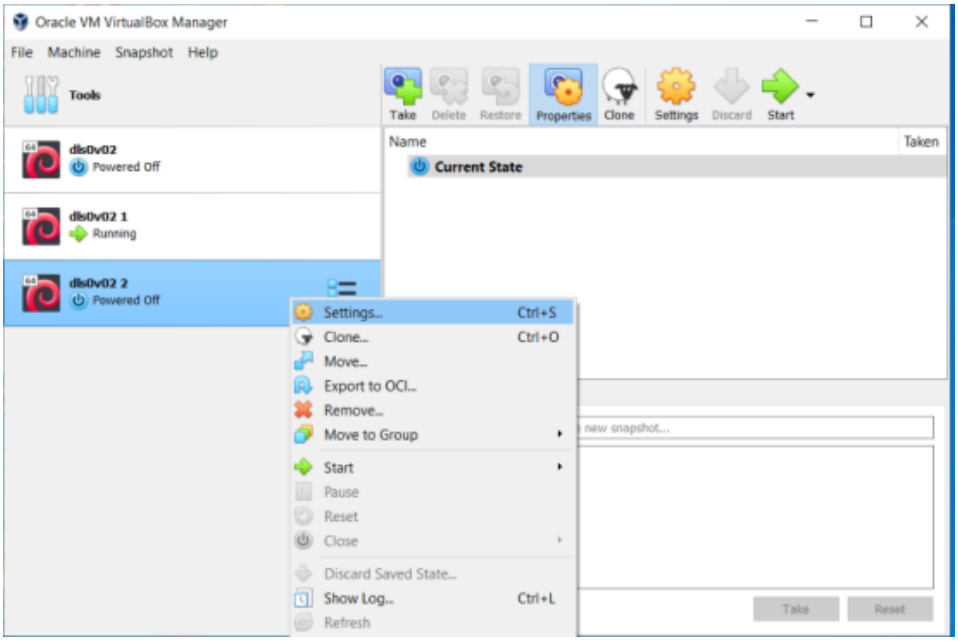
5 The application will now create a new Virtual Machine. Wait until the process is complete.



6 Once the process is complete, the new Virtual Machine is available, in power-off mode, in the left-pane of the Oracle VM VirtualBox Manager.



7 To ensure the correct Network settings for Bridged Adapter mode, right click on the new Virtual Machine and select **Settings**.

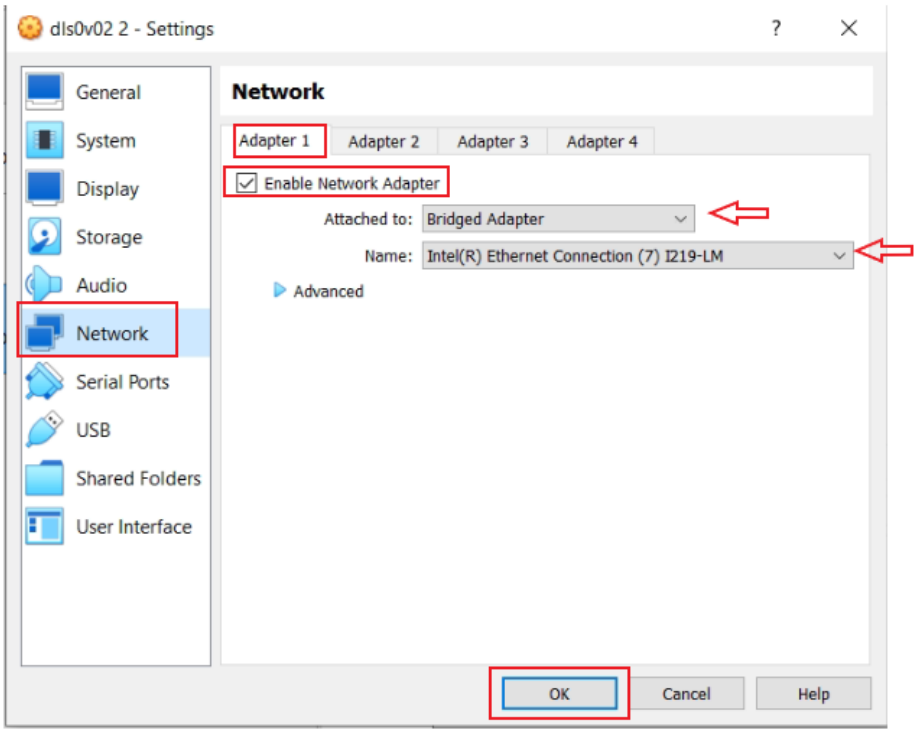


Click on **Network** and select the tab for **Adapter 1**. Set the following:

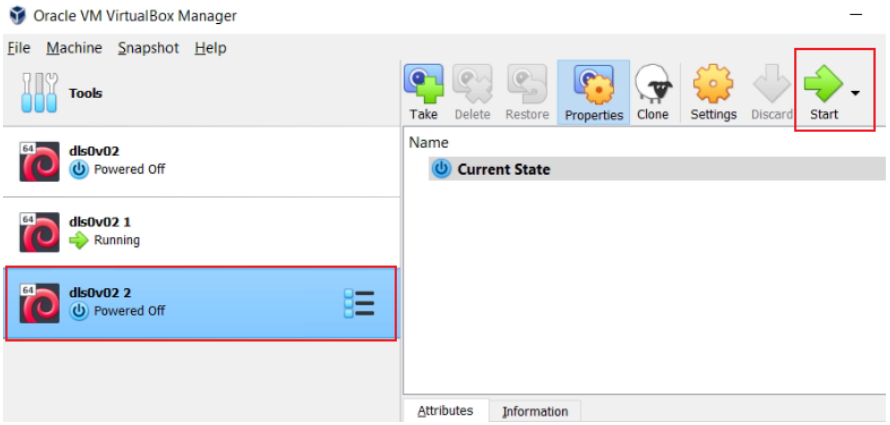
- Select the **Enable Network Adapter** checkbox.
- For **Attached to:**, choose **Bridged Adapter** from the scroll down list.
- For **Name**, select the ethernet or Wi-Fi interface.

NOTE If you are unable to connect to the Internet using the Wi-Fi interface, try using other available network interfaces, preferably a wired network connection such as an ethernet or an ethernet to USB (Universal Serial Bus) converter connection. Make sure that the network interface has a valid Internet connection.

Click **OK** to proceed.



8 Select the new Virtual Machine in the left-pane of the Oracle VM VirtualBox Manager and click on **Start** to start the Virtual Machine.

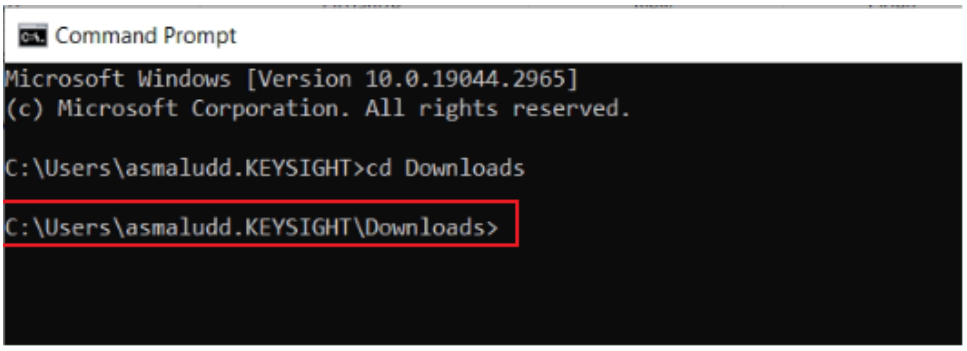


Proxmox Virtual Environment (VE)

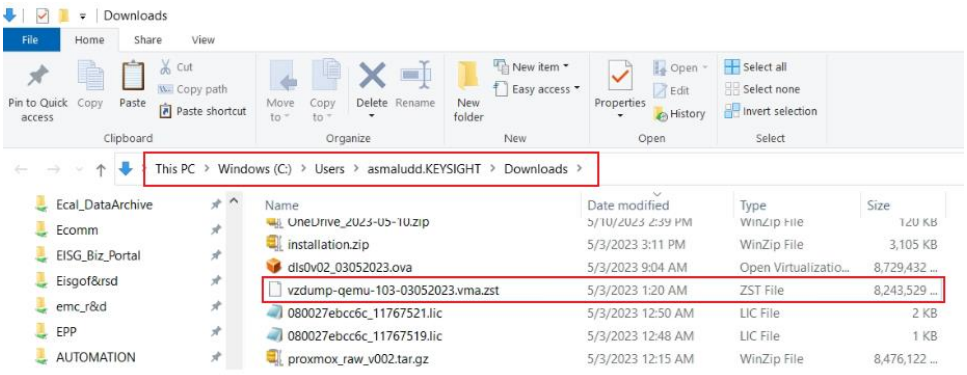
1 Transfer the Proxmox image file, *vzdump-qemu-103-03052023.vma.zst*, to your Proxmox VE server using the Windows command line, PuTTY, or FileZilla.

2 Follow the steps below to transfer the Proxmox image file using the Windows command line:

a Open the Windows command terminal and use the **cd** command to go to the folder where the downloaded *vzdump-qemu-103-03052023.vma.zst* file is stored.

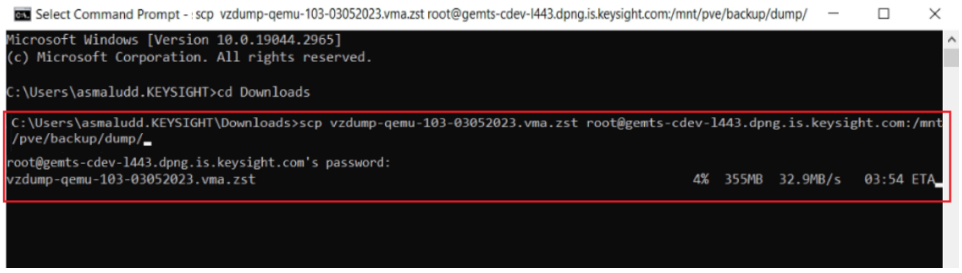


In this example, the Proxmox image file is stored in the **Downloads** folder.

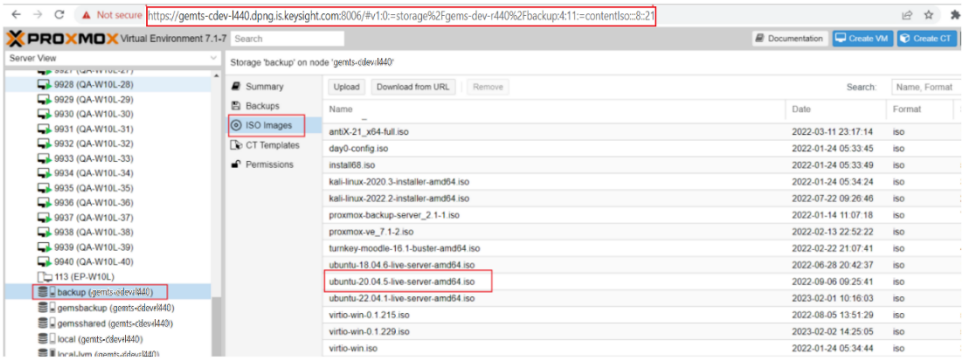


b Run this command, replacing *gemts-cdev-l440.dpng.is.keysight.com* seen in the image below with your Proxmox server URL: `scp vzdump-qemu-103-03052023.vma.zst <your username>@<your proxmox server url>:/mnt/pve/backup/dump/`

Type in your Proxmox server's SSH login password to start the file transfer.



c Once the file transfer is complete, check to make sure that the image file, *ubuntu-20.04.5-live-server-amd64.iso*, is available in your Proxmox server backup. You can do this directly at the Proxmox server webpage > backup > ISO images > <here>.



OR

Follow the steps below:

i Open the Windows command terminal.

ii Run the command `#ssh <username>@<proxmox server url>` and log in with your password.

iii Run the following commands:

```
#cd /mnt/pve/backup/template/iso
#ls -la | grep ubuntu-20.04.5-live-server-amd64.iso
```

iv If the Ubuntu image file is available on your Proxmox server, you will get the following output:

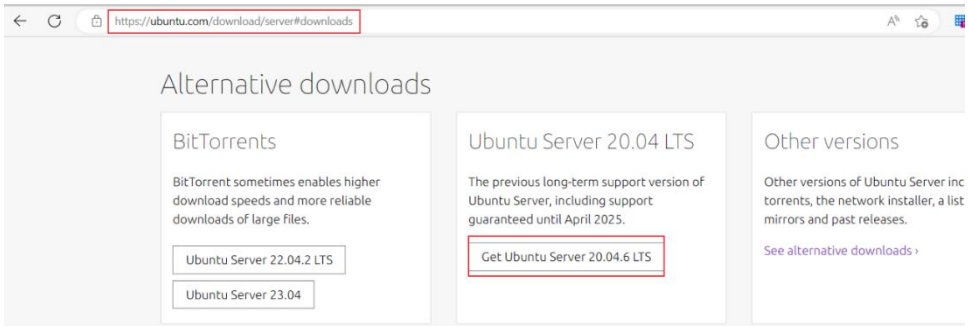
```
root@gemts-cdev-l440:/mnt/pve/backup/template/iso# ls -la | grep ubuntu-20.04.5-live-server-amd64.iso
-rwxrwxrwx 1 root root  1406533632 Aug 31  2022 ubuntu-20.04.5-live-server-amd64.iso
```

OR

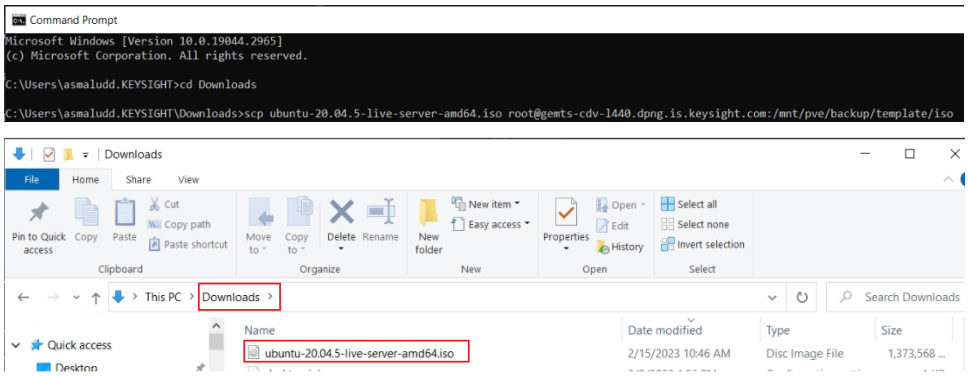
If the Ubuntu image file is not available on your Proxmox server, you will see this:

```
root@gemts-cdev-l440:/mnt/pve/backup/template/iso# ls -la | grep ubuntu-20.04.5-live-server-amd64.iso
root@gemts-cdev-l440:/mnt/pve/backup/template/iso#
```

If this happens, go to the Ubuntu webpage to download the image file.

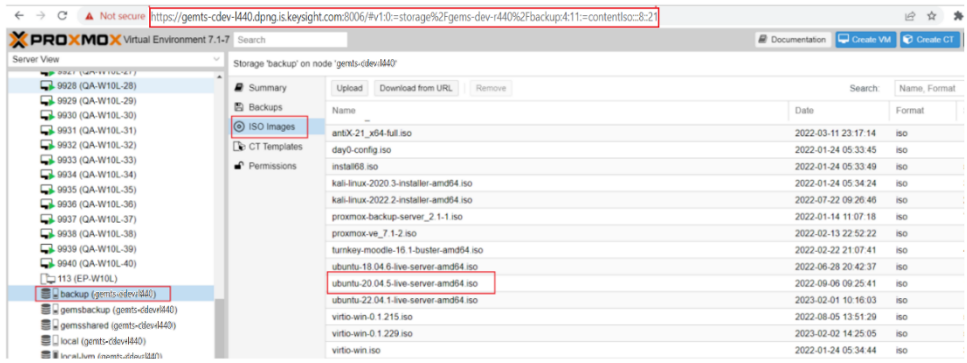


Use the **cd** command at windows command line to go to where the downloaded Ubuntu server image file, *ubuntu-20.04.5-live-server-amd64.iso*, is stored.

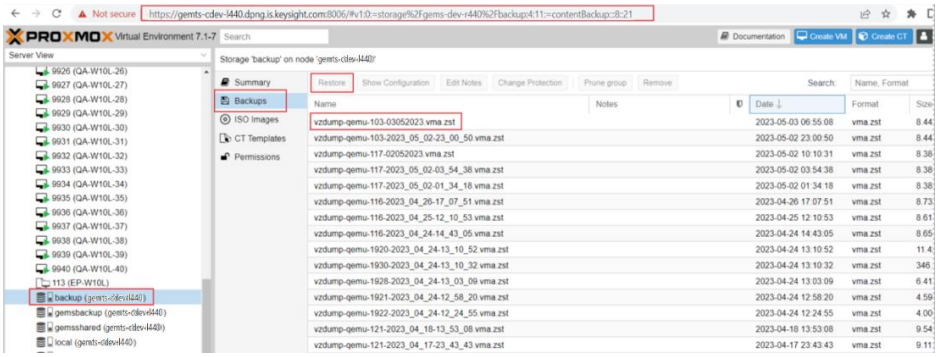


Use this command to transfer the Ubuntu server image to your Proxmox server: `scp ubuntu-20.04.5-live-server-amd64.iso <your username>@<your proxmox server url>:/mnt/pve/backup/template/iso`

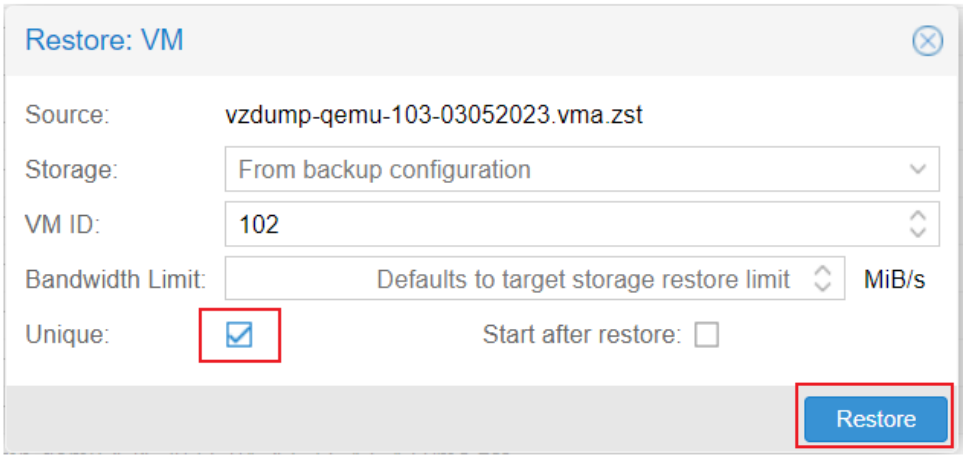
v Verify that the image file, *ubuntu-20.04.5-live-server-amd64.iso*, is available in your Proxmox server backup at the Proxmox server webpage > backup > ISO images > <here>.



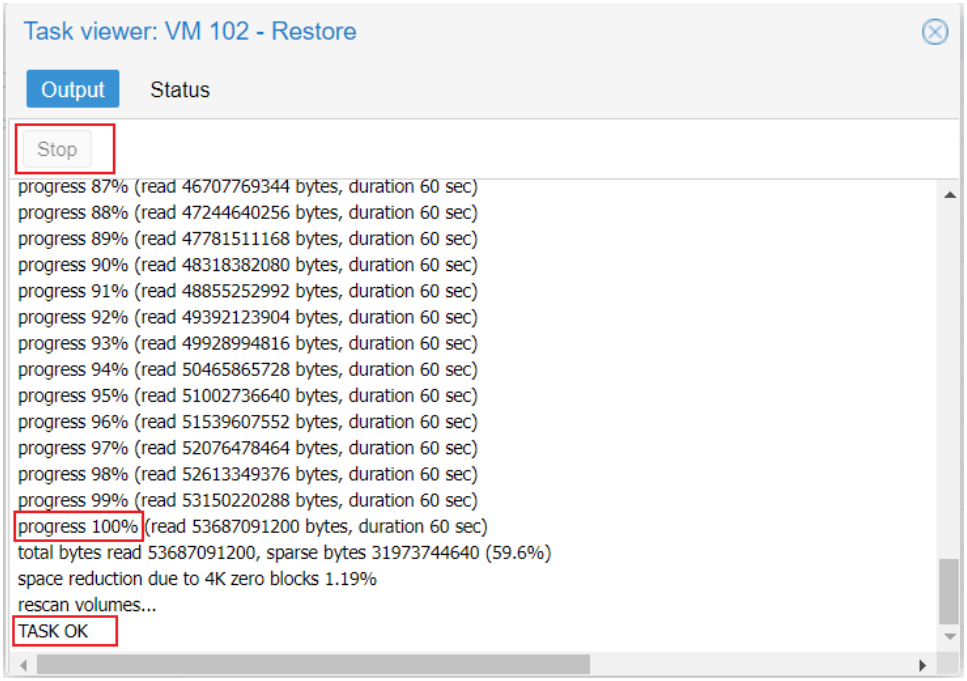
3 Once the transfer is successful, go to the Proxmox server webpage > backup and select the *vzdump-qemu-103-03052023.vma.zst* file from the right-pane. Click **Restore**.



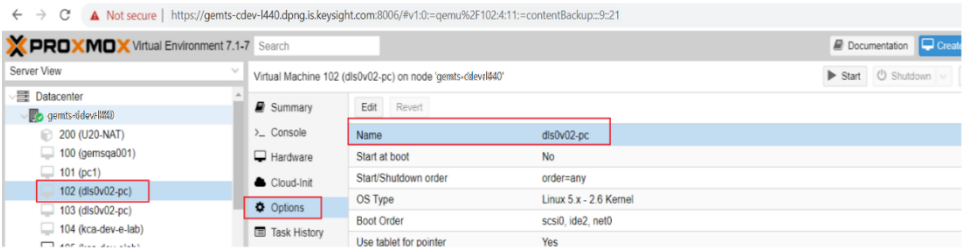
4 The **VM ID** is automatically assigned. Select the **Unique** checkbox and click **Restore**.



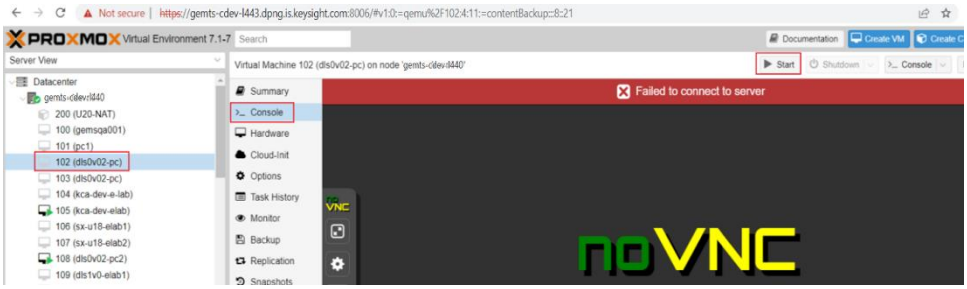
5 The program will now create a Virtual Machine on your device. Wait until the process is complete and shows **progress 100%**, with **TASK OK**, and a disabled **Stop** button. Close the dialog box.



You will find the new Virtual Machine listed in the left-pane, with the automatically assigned **VM ID**. To change the name, click on **Options** and then double click on the **Name** in the right-pane to open an **Edit** box.



6 Click on **Console** and then on **Start** to start the Virtual Machine.



NOTE If you wish to upgrade to **DLS Version 1.2.1**, follow the steps in (Optional) Upgrade from DLSv1.1.4 to DLSv1.2.1.

Step 3: Start and Set Up Virtual Machine

1 In the Proxmox web interface, click **Start** for your restored Virtual Machine (VM).

NOTE First Boot Behavior:

The VM will immediately auto reboot.

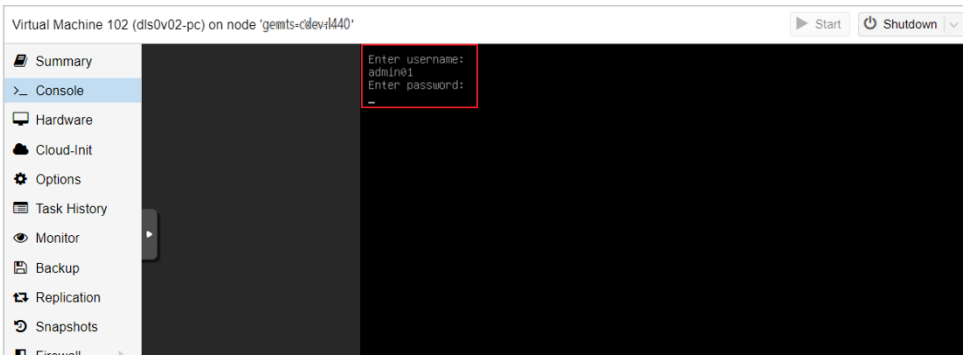
---

2 Each time you start the VM:

If GRUB Security is Enabled

i Enter the following credentials at the bootloader login screen for the bootloader login:

- Username: **admin01**
- Default password: **KeyS1ght4u!D!s**



ii The system will continue the boot process after a successful login. At the end of the boot prosess, you will see a user login prompt.

OR

If GRUB Security is Disabled

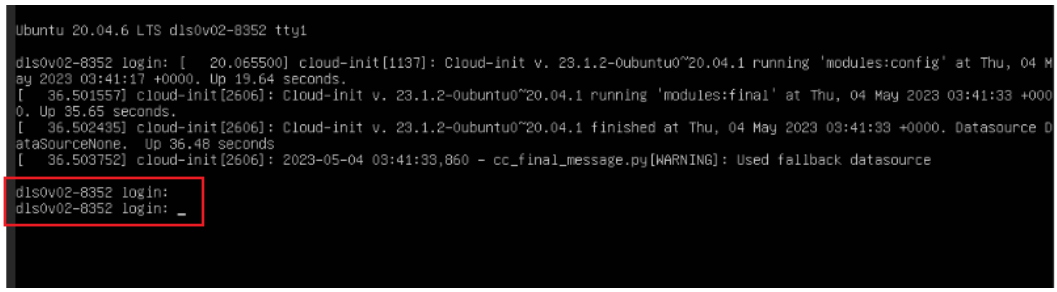
The VM will skip the bootloader login screen and boot directly to the user login prompt.

NOTE For VirtualBox, you may see a blank black screen after pressing **Start**. Click anywhere on the black screen and press **Enter** to go to the bootup login screen.

---

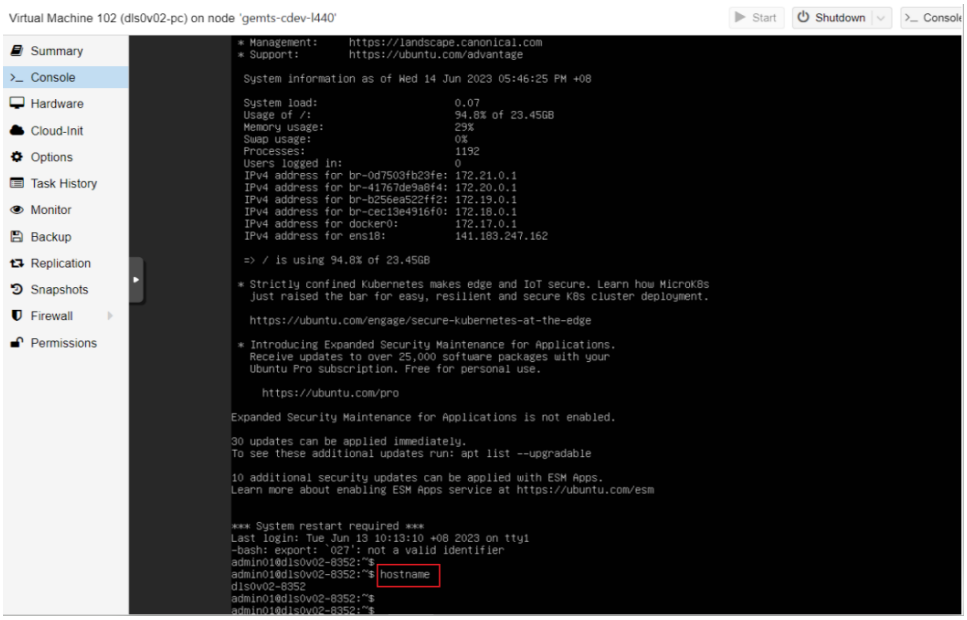
3 Regardless of the GRUB security status and first boot behavior, enter the following credentials at the user login prompt once bootup is complete:

- Username: **admin01**
- Default password: **KeyS1ght4u!D!s**

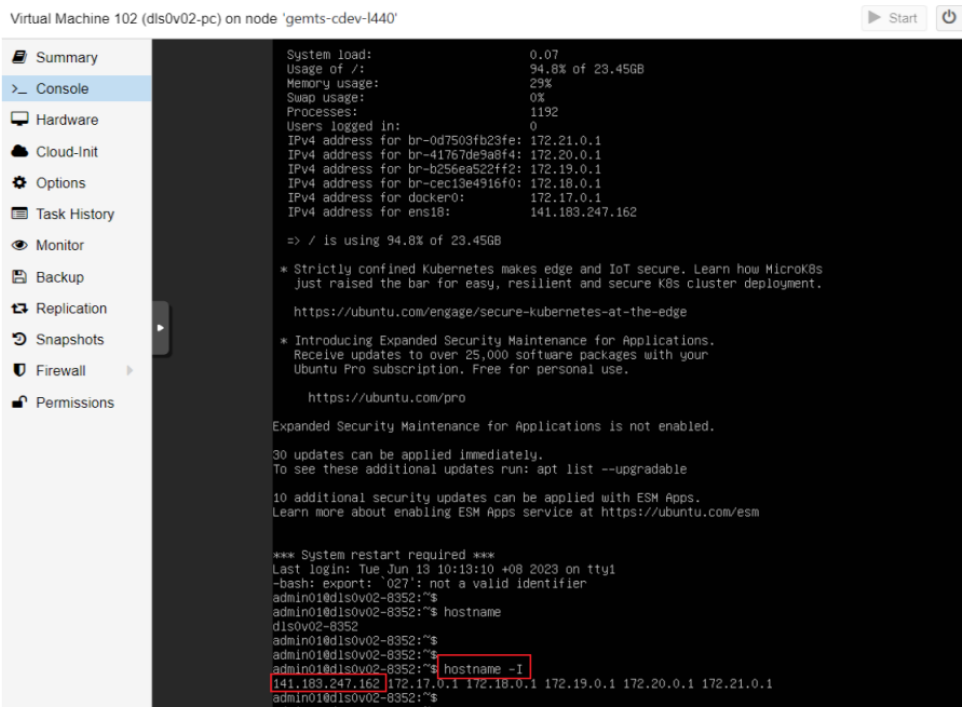


4 Follow the steps below to identify the IPv4 address and hostname as an <ip address> <server url> entry in the Windows hosts file.

a At the command prompt, use the **$hostname** command to identify the hostname.

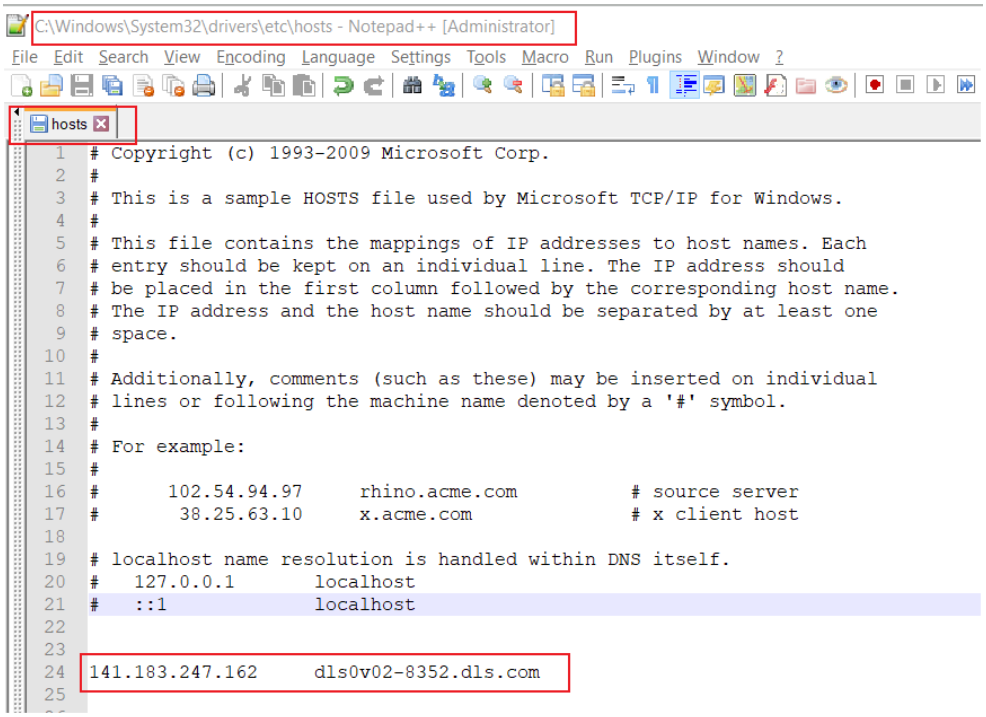


b Use the **$hostname -I** command to identify the IPv4 address and select the first one as the IPv4 address.



5 Once you have both the IPv4 address (i.e., ip address) and hostname (i.e., server url), open Notepad or Notepad++ in elevated or admin mode and add the <ip address> <server url> entry into your Windows hosts file.

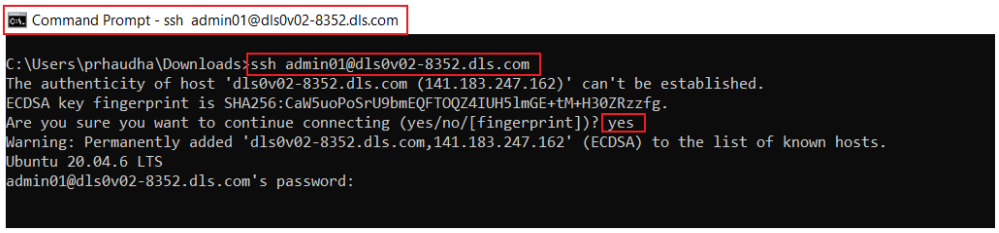
The <server url> is your Virtual Machine hostname appended by its domain name (.dls.com by default).



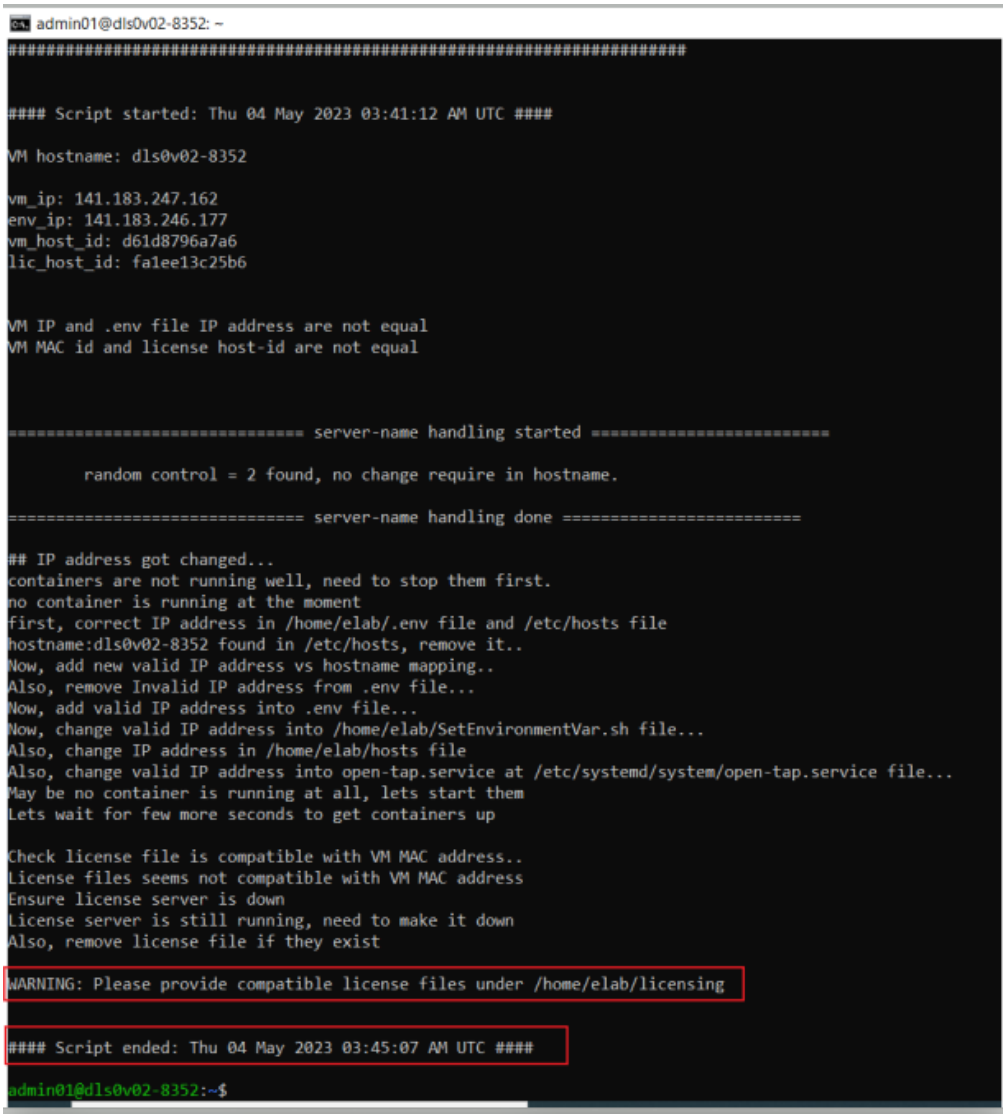
6 Use PuTTY or a Windows command line to SSH into the Virtual Machine with this command: **ssh admin01@<server url>**.

At the **Are you sure want to continue connecting (yes/no/[fingerprint])?** prompt, type **yes**.

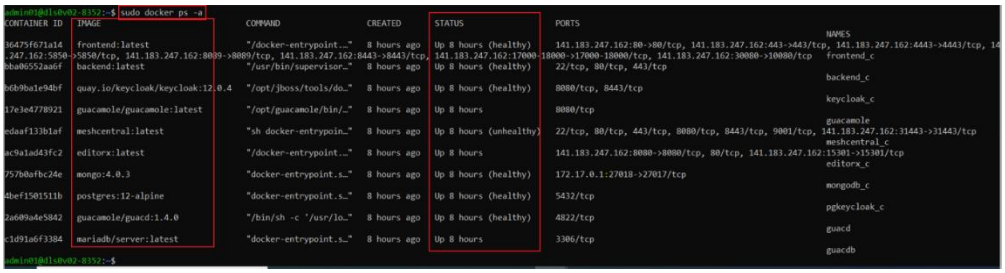
Enter the default password **KeyS1ght4u!D!s** when prompted.



7 After a successful SSH login, use this command **$ sudo cat /home/admin01/script_log.txt** to check if the DLS application is up and running. Keep running this command until you see a warning for licensing and script ended timestamp.



8 Finally, run this command **$ sudo docker ps -a** to verify that all containers are up and wait until the status is as shown in the image below.



Step 4: Customize Server Settings

NOTE This step, editing the settings config file – server_name.conf, is only applicable for users who want to use their own hostname and domain name.

---

1 Use PuTTY or a Windows command line to SSH into your Virtual Machine.

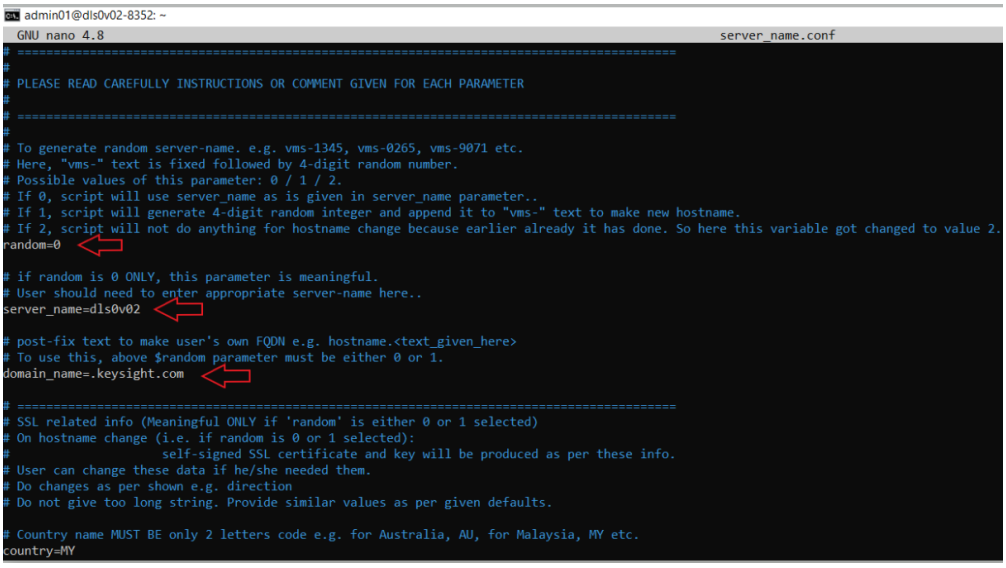
2 Use this command to go to **/home/admin01**:

```
$ cd /home/admin01
```

3 Use this command to open the server_name.conf file to edit the hostname and/or domain name:

```
$ sudo nano server_name.conf
```

4 Read the comments given after each parameter configuration. You need to set either 0 or 1 for the **random** parameter for the changes to take effect.



Step 5: Reboot Virtual Machine

NOTE This step is only applicable for users who performed Step 4: Customize Server Settings.

---

1 Run this command on the Virtual Machine command line terminal: **`$ sudo reboot`**

2 Once the reboot is complete, verify that the DLS application is up and running properly. See step 7 and step 8 under Step 3: Start and Set Up Virtual Machine for instructions.

Step 6: Ensure Resolvable Hostname

NOTE This step, verifying that the Virtual Machine <server_url> is accessible on a web browser, is only applicable for users who performed Step 4: Customize Server Settings and Step 5: Reboot Virtual Machine.

The Virtual Machine <server_url> is the hostname.domain_name as per the settings in Step 4: Customize Server Settings.

Open Notepad or Notepad++ in elevated or admin mode and add the <ip address> <server url> entry into your Windows hosts file.

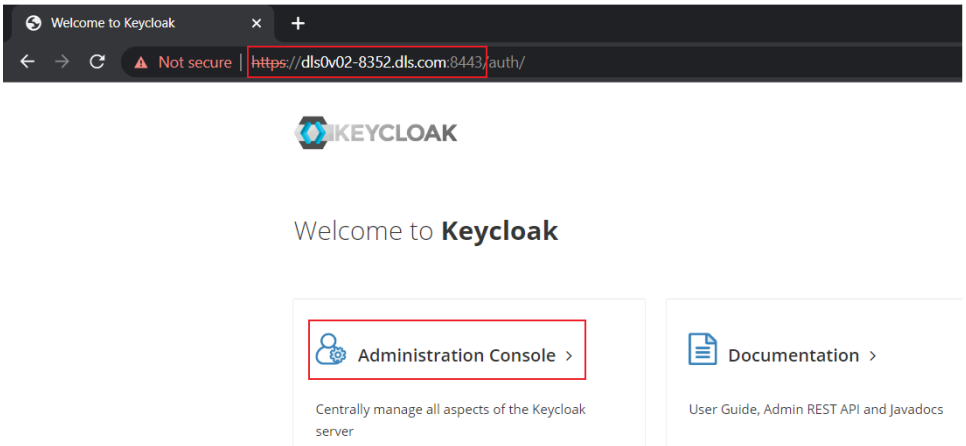
OR

Contact IT support to make it direct accessible.

Step 7: Set Up Keycloak

1 Open the URL **https:<server url>:8443** and click on **Administration Console**.

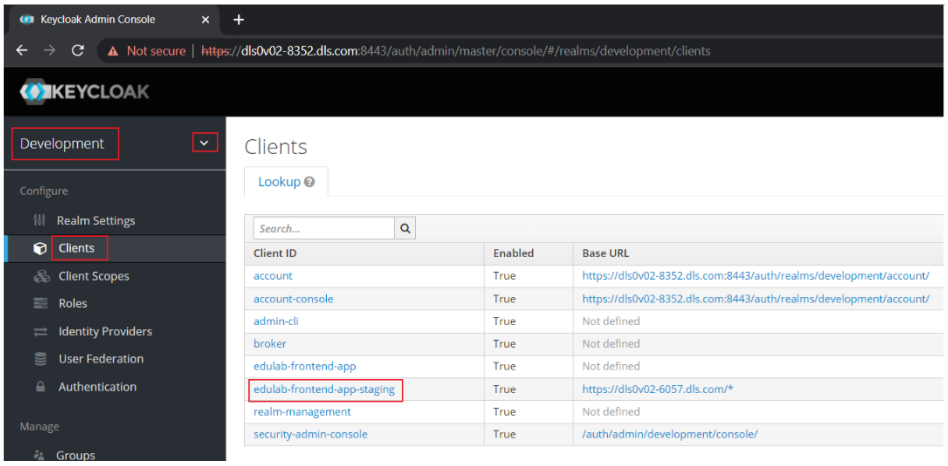
NOTE By default, your browser will not trust self-signed certificates. You will need to acknowledge the security warning during your first-time access, before proceeding with the setup.



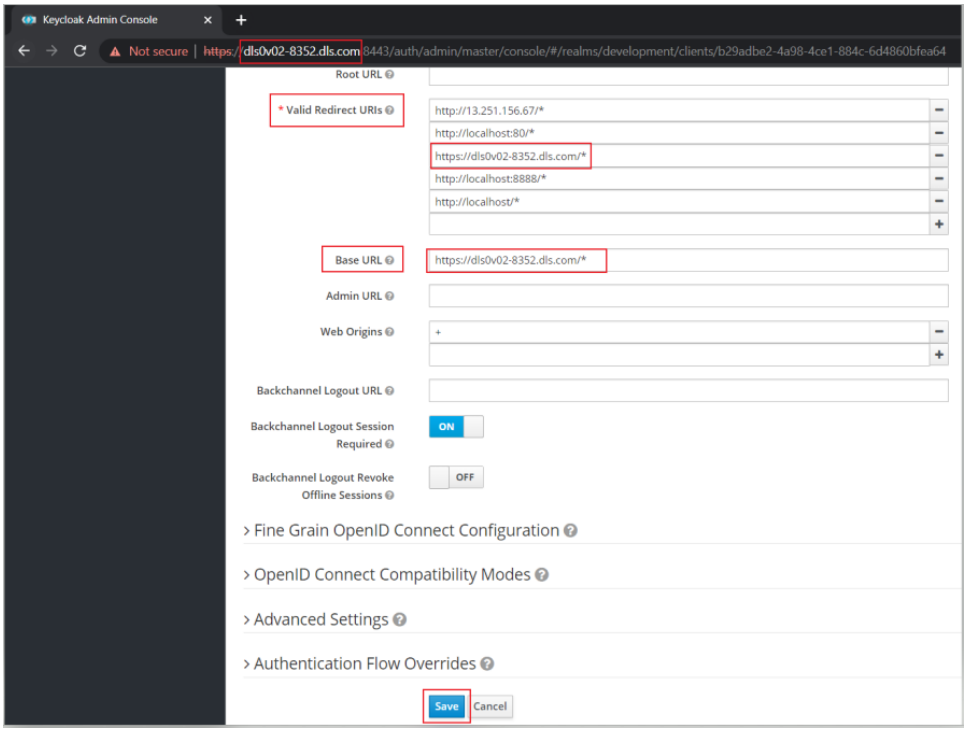
2 Log in as follows:

- Username: **admin**
- Password: **adm1n!1234**

3 Go to **Development** realm **> Clients > edulab-frontend-app-staging**



4 Scroll down to **Valid Redirect URLs** and **Base URL** and make sure they are the same as your <server url>.

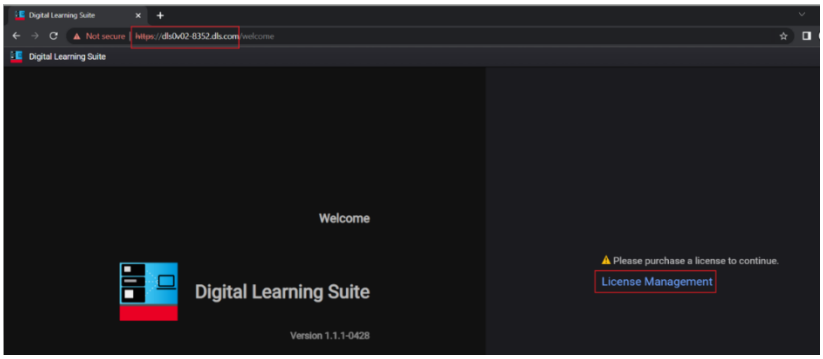


5 Click **Save**.

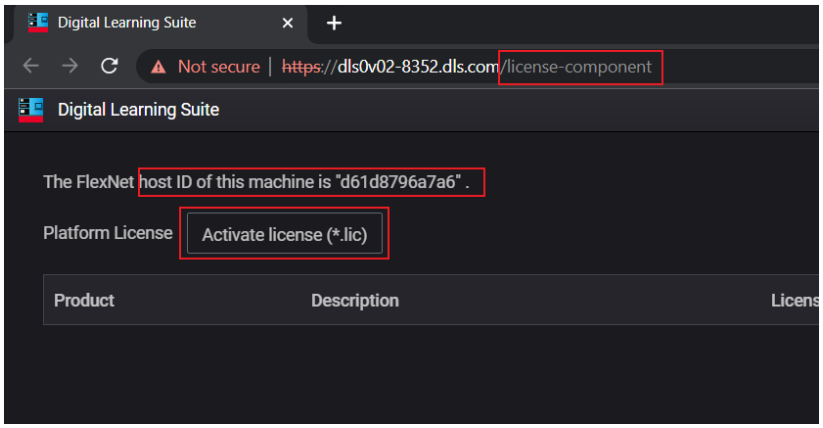
Step 8: Install License Files

1 By this point you should be able to access the DLS application welcome page. Enter your <server url> into the browser and you will see a licence request on the right pane. Click on **License Management**.

NOTE By default, your browser will not trust self-signed certificates. You will need to acknowledge the security warning during your first-time access, before proceeding with the setup.

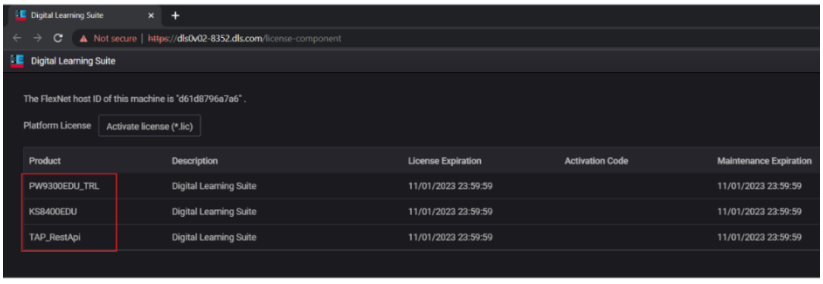


2 You will see the host ID of your machine here. Click on **Activate license (*.lic)** to upload your license files one at a time.



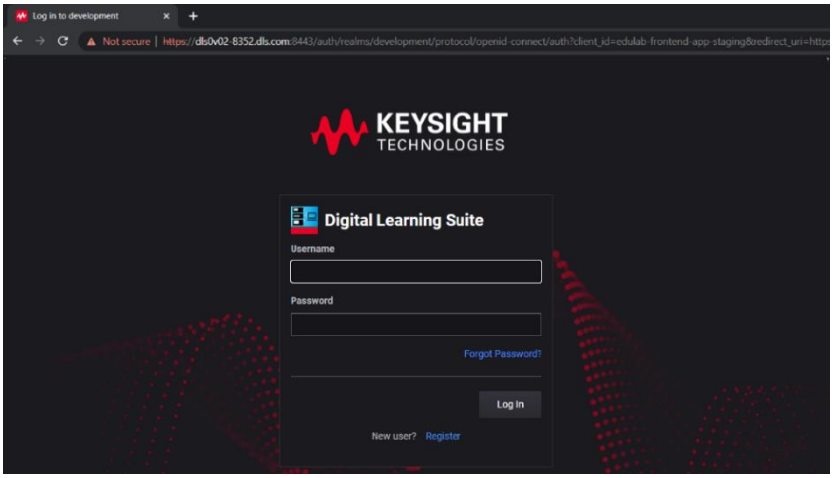
NOTE If you have not downloaded/retrieved your host ID-based license files, see Software License for the steps.

3 Once you have successfully uploaded your license files, refresh the page and the files will appear. If you do not see the license files, repeat the license upload.



Step 9: Check Client Details Settings

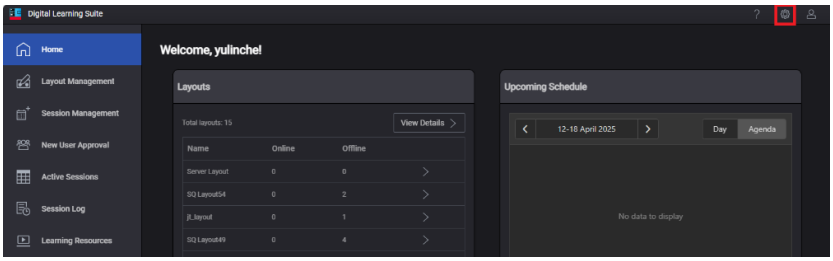
1 Enter the <server url> into the browser to go to the DLS login page.



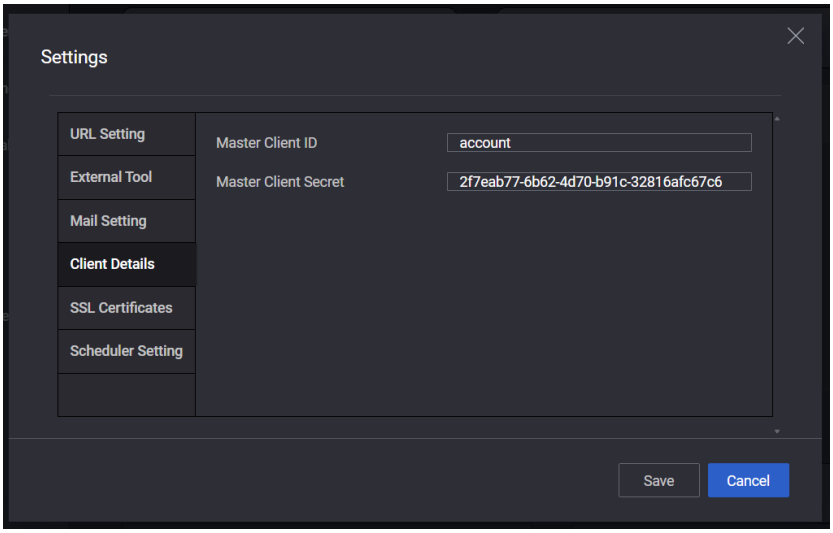
Register as a **New user**. Below is an example using **admin01**.

- Username: **admin01**
- Password: **Admin1234@**

2 At the DLS **Home** tab, click on the Settings icon > **Settings**.

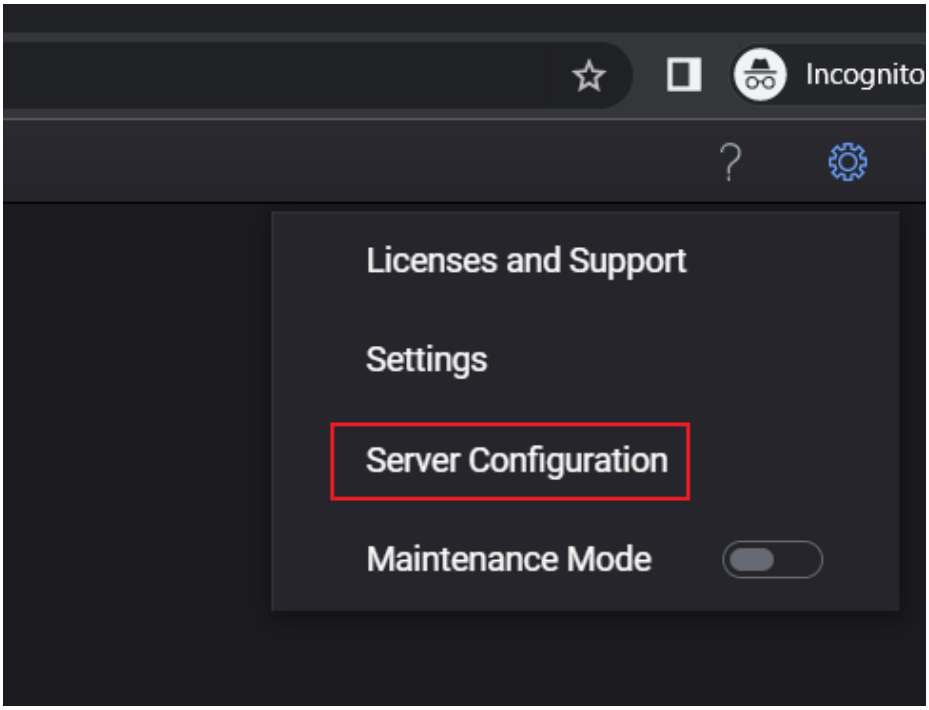


3 At **Settings**, go to **Client Details**. The fields for **Master Client ID** and **Master Client Secret** are auto generated. See *Client Details* for instructions on how to update the **Master Client Secret** field for DLS if the field information here does not match the one in Keycloak.

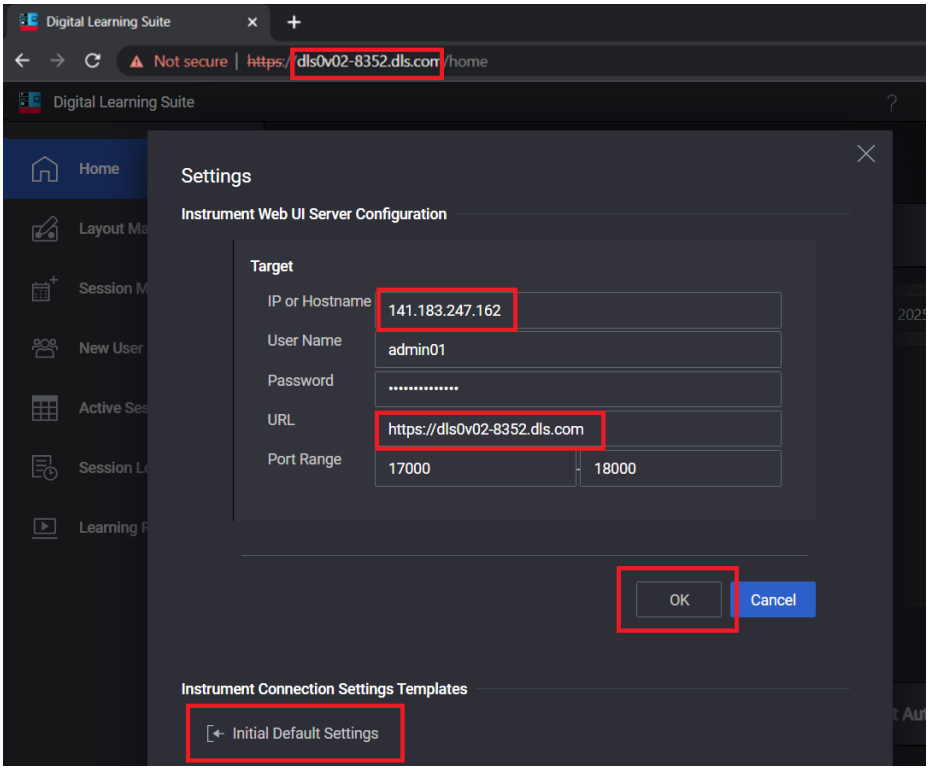


Step 10: Set Up Server Configurations

1 At the DLS **Home** tab, click on **Server Configuration**.



2 Enter your IP address and URL. Click **OK** and then **Initial Default Settings** to complete the setup.



(Optional) Upgrade from DLSv1.1.4 to DLSv1.2.1

This section will guide you through the steps to upgrade to **DLS Version 1.2.1**. Before you proceed with the upgrade process, take note of the following requirements:

- Upgrade package: **dls1v14_to_dls1v21_pkg.tar**

NOTE Go to the following link to download the file: DLS Version Upgrade Patch

---

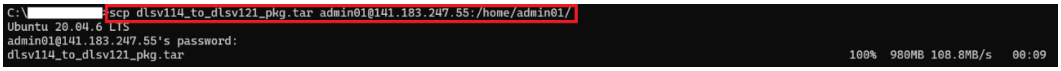
1. Make sure you have downloaded the upgrade package **dls1v14_to_dls1v21_pkg.tar** from the download link.
2. Use the following command to transfer the upgrade package to the running VM using the Windows command line,

   ```
   scp dls1v14_to_dls1v21_pkg.tar admin01@<vm_ip_address>:/home/admin01/
   ```

NOTE For this example, the VM username is **admin01**.

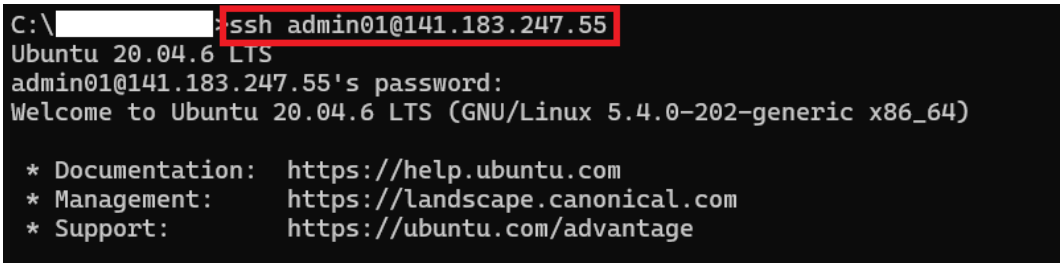
- Replace <**vm_ip_address**> with the actual IP address of your VM.
- Enter the VM's login or the default password when prompted:

  Default password: **KeyS1ght4u!D!s**



3. Log in to your VM and navigate to the folder containing the upgrade package:

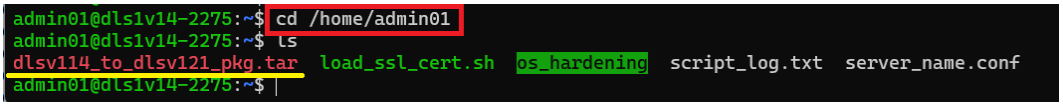
   ```
   ssh admin01@<vm_ip_address>
   ```



Perform the following commands:

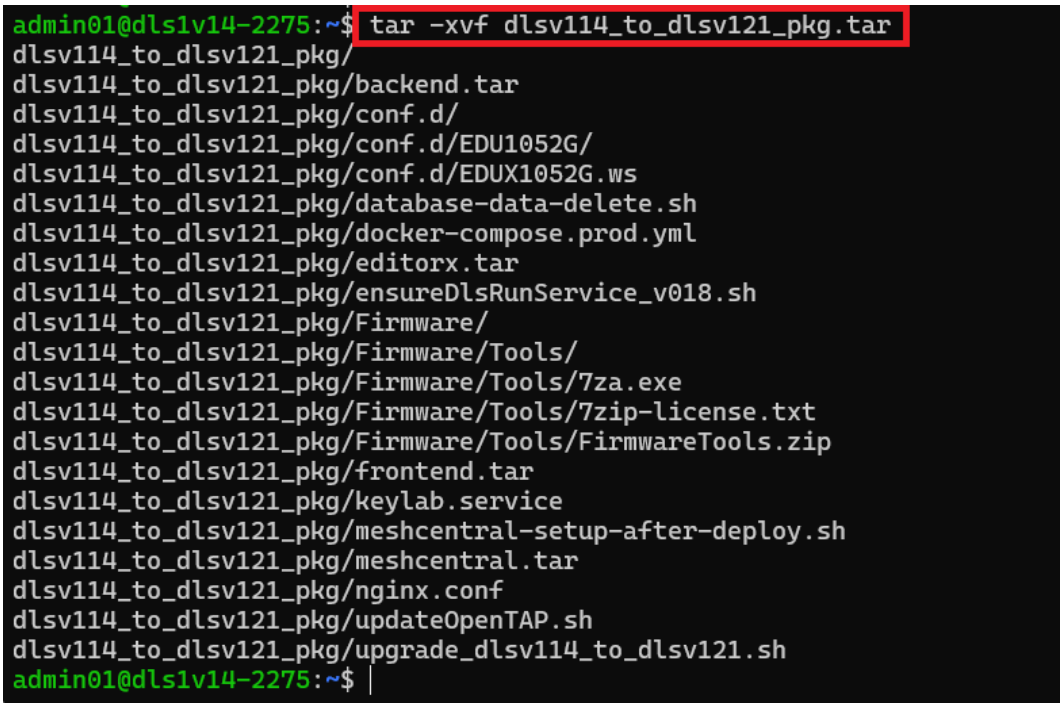
```
cd /home/admin01
```

```
ls
```



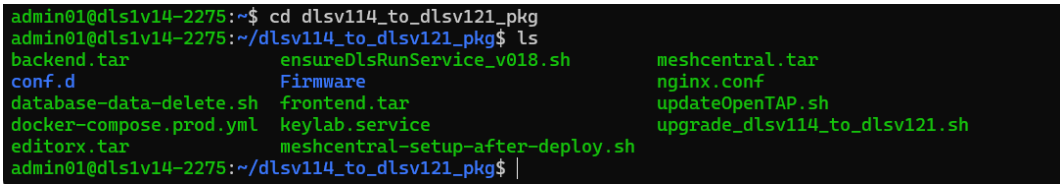
4 Use the following command to extract the contents of the upgrade package:

```
tar -xvf dls1v14_to_dls1v21_pkg.tar
```



5 Perform the following commands to check the extracted contents:

```
cd dlsv114_to_dlsv121_pkg
ls
```



6 Use the following command to ensure that the upgrade script is executable:

```
ls -la upgrade_dlsv114_to_dlsv121.sh
```

If the upgrade script is not executable, use the command below to make it executable:

```
sudo chmod +x upgrade_dlsv114_to_dlsv121.sh
```

7 Use the command below to run the upgrade script:

```
sudo sh upgrade_dlsv114_to_dlsv121.sh
```

```
admin01@dls1v14-2275:~/dlsv114_to_dlsv121_pkg$ sudo sh upgrade_dlsv114_to_dlsv121.sh
============================================================
 DLSv1.1.4 to DLSv1.2.1 upgration started
============================================================
[**Assumption: You have taken care of vm_user and vm_pswd in this script before run it.]
1. Make sure DLS app is not running
[+] Running 14/14
 ✔Container guacamole                Removed                                        0.5s
 ✔Container keycloak_c               Removed                                        1.1s
 ✔Container frontend_c               Removed                                       15.8s
 ✔Container guacdb                   Removed                                        0.6s
 ✔Container guacd                    Removed                                        0.2s
 ✔Container pgkeycloak_c             Removed                                        0.2s
 ✔Container editorx_c                Removed                                        0.2s
 ✔Container backend_c                Removed                                        2.3s
 ✔Container meshcentral_c            Removed                                       10.2s
 ✔Container mongodb_c                Removed                                        0.3s
 ✔Network edulab_network             Removed                                        0.3s
 ✔Network edulab_mongonetwork        Removed                                        0.1s
 ✔Network edulab_pgnetwork           Removed                                        0.2s
 ✔Network edulab_guacnetwork_compose Removed                                        0.4s
No stopped containers
2. Handle incompatible database
Installing mongoexport...
OK
deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/4.4 multiverse
```

```
Installing /root/.local/share/OpenTap/PackageCache/OpenTAP.9.28.0+69e2fcdd.x64.Linux.TapPackage
Starting install step 'chmod +x tap'
Succesfully ran install step  'chmod +x tap'.  [4.66 ms]
Installed OpenTAP version 9.28.0+69e2fcdd [136 ms]
Downloaded 'REST-API' to '/root/.local/share/OpenTap/PackageCache/REST-API.2.10.3+8ac067f0.Windows,Linux,Mac
os.TapPackage'. [3.68 ms]
Installing to /home/.tap
Successfully uninstalled REST-API version 2.10.3+8ac067f0. [24.7 ms]
Installing /root/.local/share/OpenTap/PackageCache/REST-API.2.10.3+8ac067f0.Windows,Linux,Macos.TapPackage
Starting install step 'tap remote configfile'
Config file at /home/.tap/Config/RPCBase.yaml already exists [111 ms]
Successfully ran install step  'tap remote configfile'.  [584 ms]
Installed REST-API version 2.10.3+8ac067f0 [831 ms]
Downloading Keysight Licensing [==============================] (100.00% | 2.75 MB of 2.75 MB)
Downloaded 'Keysight Licensing' to '/root/.local/share/OpenTap/PackageCache/Keysight Licensing.1.5.1+16a9625
a.x64.Linux.TapPackage'. [2.24 s]
Installing to /home/.tap
Successfully uninstalled Keysight Licensing version 1.4.5+2bd4be43. [13.4 ms]
Installing /root/.local/share/OpenTap/PackageCache/Keysight Licensing.1.5.1+16a9625a.x64.Linux.TapPackage
Installed Keysight Licensing version 1.5.1+16a9625a [121 ms]
Downloaded 'KeyLab Test Sequencing and Control' to '/root/.local/share/OpenTap/PackageCache/KeyLab Test Sequ
encing and Control.0.1.26-rc.1+1b51fe2f.Windows,Linux.TapPackage'. [3.67 ms]
Installing to /home/.tap
Successfully uninstalled KeyLab Test Sequencing and Control version 0.1.26-rc.1+1b51fe2f. [11.4 ms]
Installing /root/.local/share/OpenTap/PackageCache/KeyLab Test Sequencing and Control.0.1.26-rc.1+1b51fe2f.W
indows,Linux.TapPackage
Installed KeyLab Test Sequencing and Control version 0.1.26-rc.1+1b51fe2f [140 ms]
admin01@dls1v14-2275:~/dlsv114_to_dlsv121_pkg$
```

8 Once the scripts have executed successfully, run the following commands to remove the upgrade packages:

```
cd /home/admin01
```

```
admin01@dls1v14-2275:~/dlsv114_to_dlsv121_pkg$ cd /home/admin01
admin01@dls1v14-2275:~$
```

```
sudo rm -f dlsv114_to_dlsv121_pkg.tar
```

```
admin01@dls1v14-2275:~$ sudo rm -f dlsv114_to_dlsv121_pkg.tar
admin01@dls1v14-2275:~$
```

```
sudo rm -rf dlsv114_to_dlsv121_pkg
```

```
admin01@dls1v14-2275:~$ sudo rm -rf dlsv114_to_dlsv121_pkg
admin01@dls1v14-2275:~$
```

9 Use the following command to initiate a reboot of the VM to conclude the upgrade process:

```
sudo reboot
```

```
admin01@dls1v14-2275:~$ sudo reboot
Connection to 141.183.247.55 closed by remote host.
Connection to 141.183.247.55 closed.
```

10 Once the reboot is complete, use PuTTY or a Windows command line to SSH into the Virtual Machine with this command:

```
ssh admin01@<vm_ip_address>
```

```
C:\              >ssh admin01@141.183.247.55
Ubuntu 20.04.6 LTS
admin01@141.183.247.55's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-202-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

11 After a successful SSH login, use the command below to check if the DLS application is up and running. Repeat this command until you see license server message and script ended timestamp.

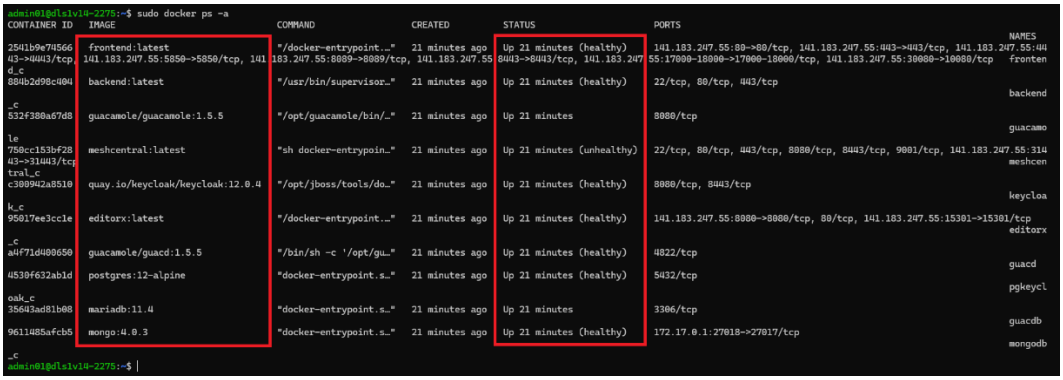
```
sudo cat /home/admin01/script_log.txt
```

```
admin01@dls1v14-2275:~$ sudo cat /home/admin01/script_log.txt


#########################################################################
#### Scrpit to ensure Keylab app and license server up and running ####
####                    Script Version:0.1.8                       ####
####                    PreConfig Version:1.2.1                    ####
#########################################################################


#### Script started: Sat 12 Apr 2025 10:08:28 AM UTC ####

VM hostname: dls1v14-2275

vm_ip: 141.183.247.55
env_ip: 141.183.247.55
vm_host_id: bc24118298bd
lic_host_id: bc24118298bd
License file exists


Both IP address are equal..



============================== server-name handling started ========================

        random control = 2 found, no change require in hostname.

============================== server-name handling done ========================

May be no container is running at all, lets start them
Lets wait for few more seconds to get containers up

Check license file is compatible with VM MAC address..
license files seems available, make sure license server is up
License server is already up and running

#### Script ended: Sat 12 Apr 2025 10:10:56 AM UTC ####

admin01@dls1v14-2275:~$
```

12 Execute the following command to verify that all the containers are up:

```
sudo docker ps -a
```

Ensure that the status is as shown in the image below:



(Optional) Upload New Valid SSL or Self-Signed Certificate and Private Key

NOTE

If you wish to use your own certificate and private key, follow the steps below to replace the default self-signed certificate and private key provided with the pre-configured Virtual Machine.

To reduce security risk, avoid using the default self-signed certificate. Please adhere to your IT security guidelines on SSL certificate usage.

---

1. Make sure you have a valid SSL certificate (.crt file) and private key (.key file) readily available in your Windows directory.
2. Open a text editor of your choice (e.g., Notepad, Sublime Text, or Visual Studio Code).
3. Create a new file and save it with the filename: **load_ssl_cert.sh**
4. Copy and paste the following content into your script, i.e., text editor, file:

   ----------Start---------- (Do not copy this line)

```
#!/bin/sh


echo "1. First, remove existing crt and key files from all places"
sudo rm /home/elab/e-lab.crt /home/elab/e-lab.key
sudo rm /home/elab/ssl/e-lab.crt /home/elab/ssl/e-lab.key
sudo rm /home/elab/meshcentral-data/webserver-cert-public.crt
/home/elab/meshcentral-data/webserver-cert-private.key
sudo rm /etc/ssl/private/request.csr /etc/ssl/private/certificate.crt
/etc/ssl/private/private.key


echo "2. Now, rename new added crt and key file with e-lab.crt and e-
lab.key file"
sudo mv /home/admin01/*.crt /home/admin01/e-lab.crt
sudo mv /home/admin01/*.key /home/admin01/e-lab.key


echo "3. Now, first, copy new added crt file at all required places"
sudo cp /home/admin01/e-lab.crt /home/elab/
sudo cp /home/admin01/e-lab.crt /home/elab/ssl
sudo cp /home/admin01/e-lab.crt /home/elab/meshcentral-data/webserver-
cert-public.crt
sudo cp /home/admin01/e-lab.crt /etc/ssl/private/certificate.crt


echo "4. Also, copy new added key file at all required places"
sudo cp /home/admin01/e-lab.key /home/elab/
sudo cp /home/admin01/e-lab.key /home/elab/ssl
sudo cp /home/admin01/e-lab.key /home/elab/meshcentral-data/webserver-
cert-private.key
```

```
sudo cp /home/admin01/e-lab.key /etc/ssl/private/private.key


echo "5. Also, now, delete new added crt and key files from
/home/admin01/"
sudo rm /home/admin01/e-lab.crt /home/admin01/e-lab.key


echo "6. At the end, just reboot the VM..."
sleep 2
sudo reboot
```

----------End---------- (Do not copy this line)

5 Save the script file in the same directory as your<.crt> and <.key> files.

6 Use a Windows command line and run the following commands:

```
# cd <Directory path where the .crt, .key, and load_ssl_cert.sh files are
stored>
# scp <.crt file> <.key file> load_ssl_cert.sh
admin01@<server_url>:/home/admin01
```

7 Enter the SSH password of your Virtual Machine to start the transfer.

8 SSH into your Virtual Machine using same windows command line terminal and perform subsequent commands:

```
# ssh admin01@<server_url>
# Enter your SSH password
# cd /home/admin01
# sudo chmod +x load_ssl_cert.sh
# sudo ./load_ssl_cert.sh
```

9 Run this command on the Virtual Machine command line terminal: **`$ sudo reboot`**

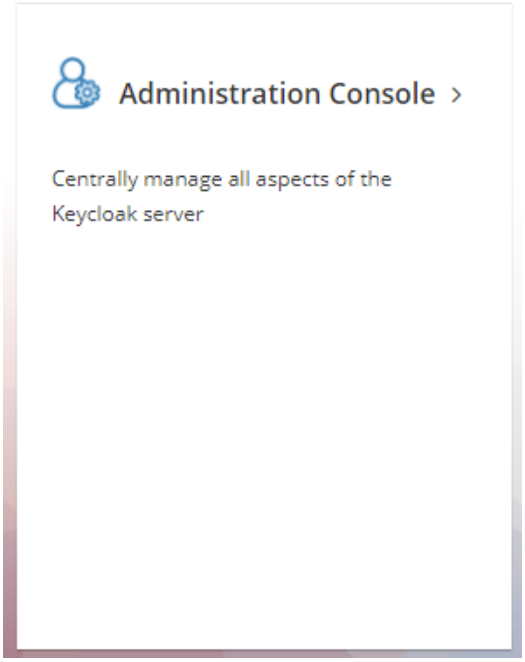
10 Once the reboot is complete, verify that the DLS application is up and running properly. See step 7 and step 8 under Step 3: Start and Set Up Virtual Machine for instructions.

Keycloak Settings

NOTE It is highly recommended that you change the password before using the application.

Change the Keycloak Default Admin Password

1. In a web browser, open the Error! Reference source not found. **https://<URL>:8443** to go to t he Keycloak page welcome page.
2. Click on **Administration Console**.



3. Log in with the following:

   Username: admin

   Password: adm1n!1234
4. Go to **Users** on the left panel and click **View all users**.
5. Click **Edit** on the row for the account **admin**.
6. Go to the **Credentials** tab. Under **Manage Password**, enter a new secure password and disable **Temporary**.
7. Click **Reset Password**.

Create Super-Admin Accounts

NOTE

Super-Admins have full authorization to carry out user management tasks such as adding/removing Digital Learning Suite users, resetting passwords, and changing the role (Student, Lecturer, or LabAdmin) of Digital Learning Suite users - these tasks can be offloaded to the system administrator(s) on the customer's side.

Super-Admins login via the **https://<URL>:8443** link instead of the regular **https://<URL>** link.

1. Go to the **Master** realm by hovering over **Development** on the left side and clicking **Master**.
1. Click on **Users** on the left panel.
2. Click **Add user** at the end of the table's header.
3. Fill in the **Username**, **Email**, **First Name**, and **Last Name** of the user. Click **Save**.
4. You will be redirected to the user's profile page. Go to the **Role Mappings** tab.
5. Under **Available Roles**, click on **admin** and click **Add selected >** below it. This assigns the **admin** role to the newly created account.
6. Go to the **Credentials** tab, and under **Manage Password**, enter a new memorable password. Ensure **Temporary** is ON. Click **Reset Password**.
7. Go back to the **Details** tab and take note of the **Username**.
8. Provide the **Username** and **Password** to the system administrator. When they login, they will be prompted to enter a new password.
9. Repeat from Step 1 to create more accounts.

Keycloak Administration Console

Use the default credentials below to access the Keycloak Administration Console:

Username: **admin**

Password: **adm1n!1234**

NOTE

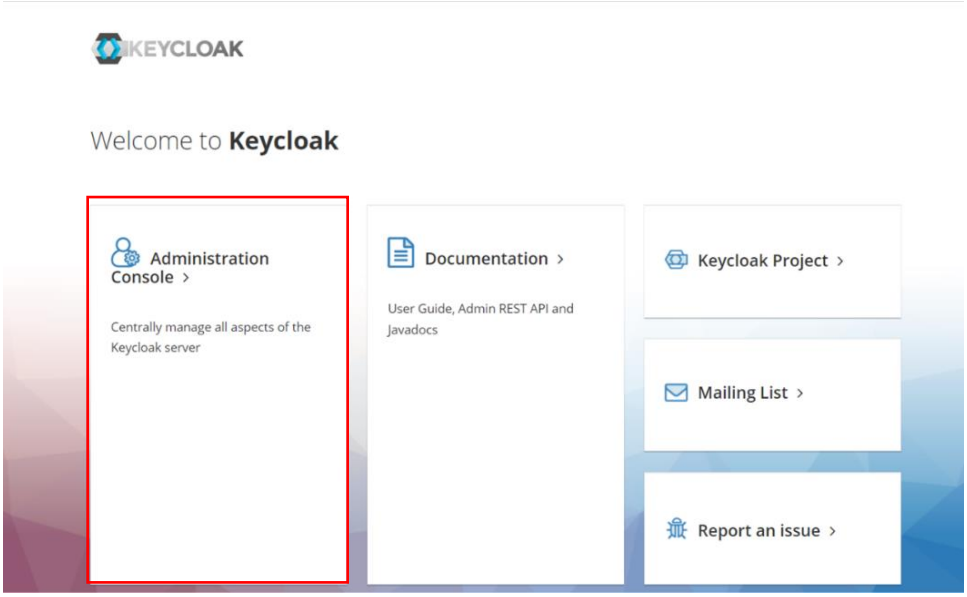
It is highly recommended that you **change the password** before using the application. See Change the Keycloak Default Admin Password for instructions.

See Keycloak Settings for instructions to create Super-Admin Accounts.

---

1 In a web browser, open the **Error! Reference source not found. https://<URL>:8443** to go to the K eycloak page welcome page.

Click on **Administration Console** and log in.



2 You can perform the following tasks in the **Development** realm:

- **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.

- **Enable Email Settings**

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

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

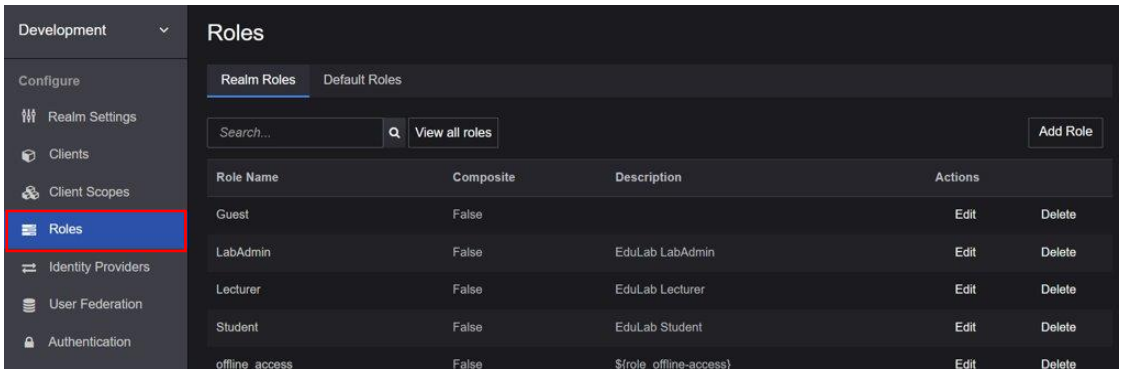
  This is an optional step to set up the social sign in for your application.

Configuration and Settings

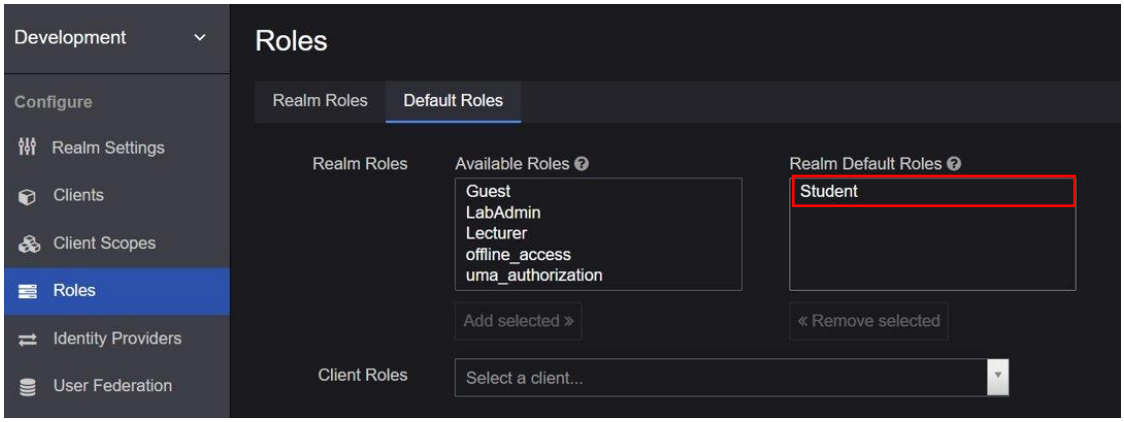
Configure Roles

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.

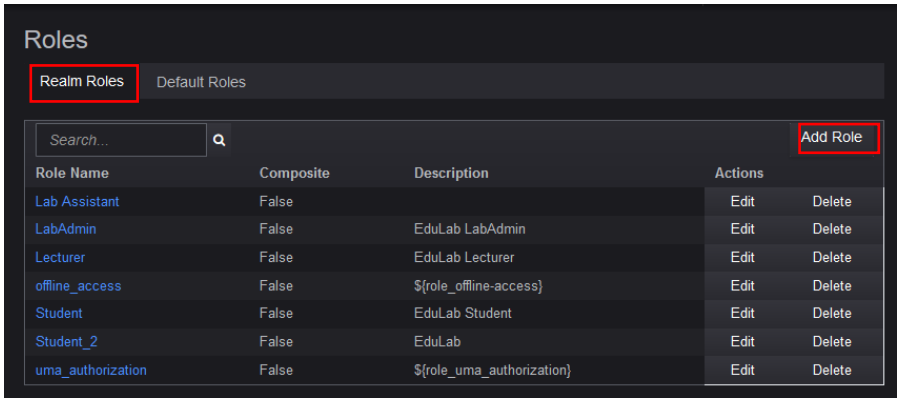


2 Go to the **Default Roles** tab to view or modify the default roles assigned to new accounts. By default, new accounts are assigned with **Guest** role during registration.

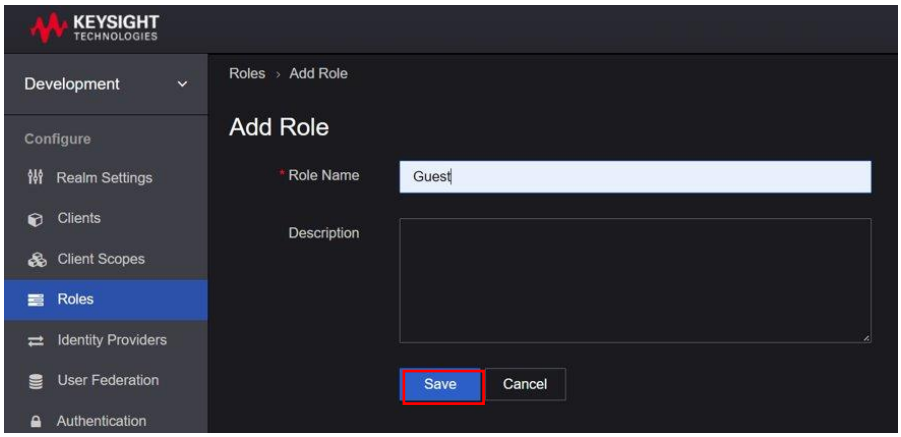


NOTE You can only add or remove one role at a time. To change the default role, you must first select the Guest role and click **Remove Selected** button. Then, select the desired role and click **Add Selected** to set it as the Realm Default Role.

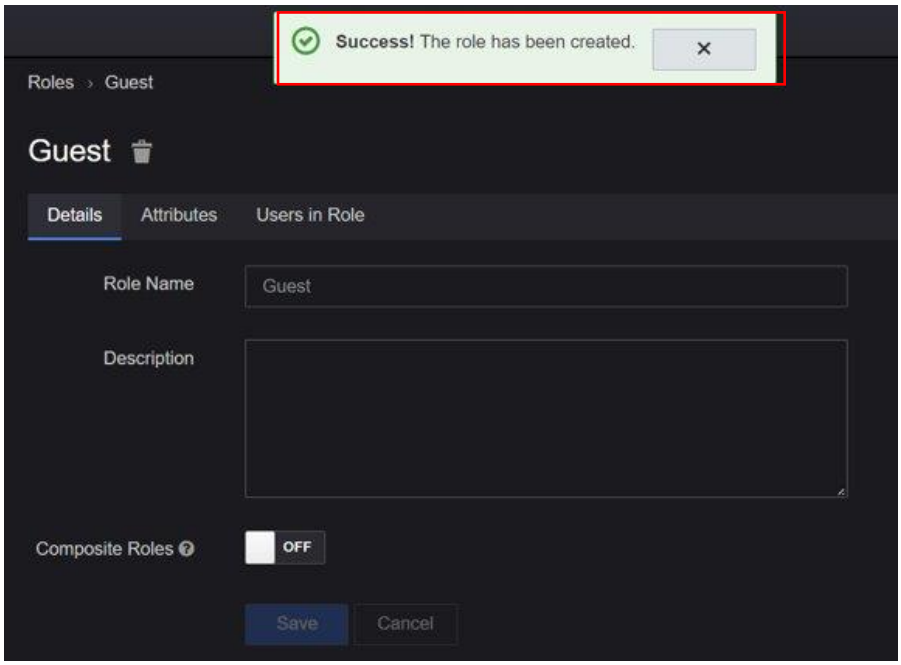
3 To add a new role, return to **Realm Roles** tab and click the **Add Role** button.



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.

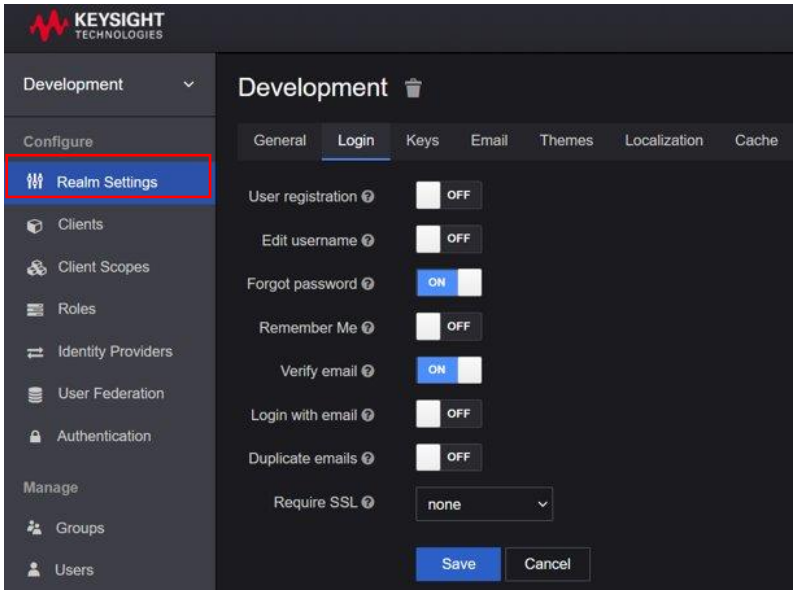


Add User

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.

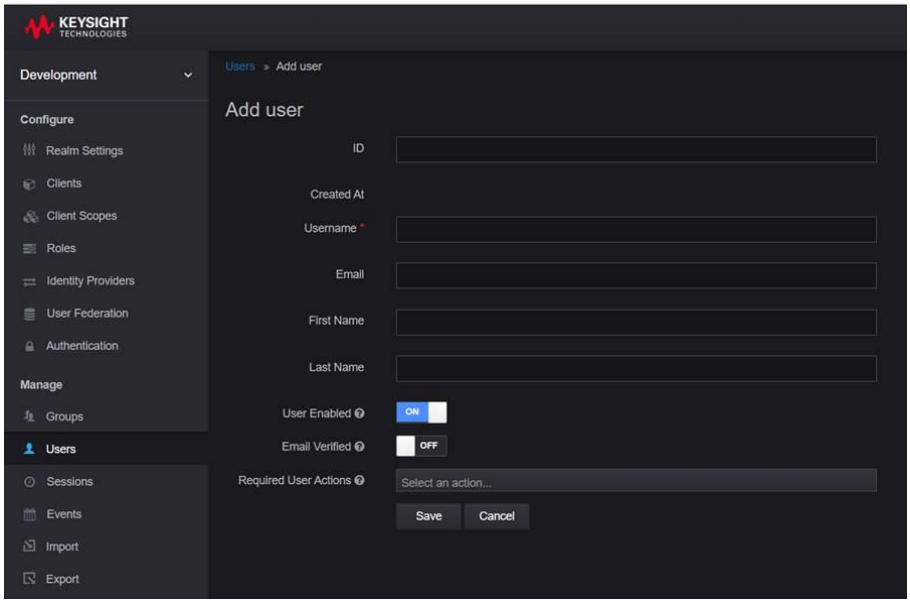
Go to **Realm settings > Login** to view this setting.



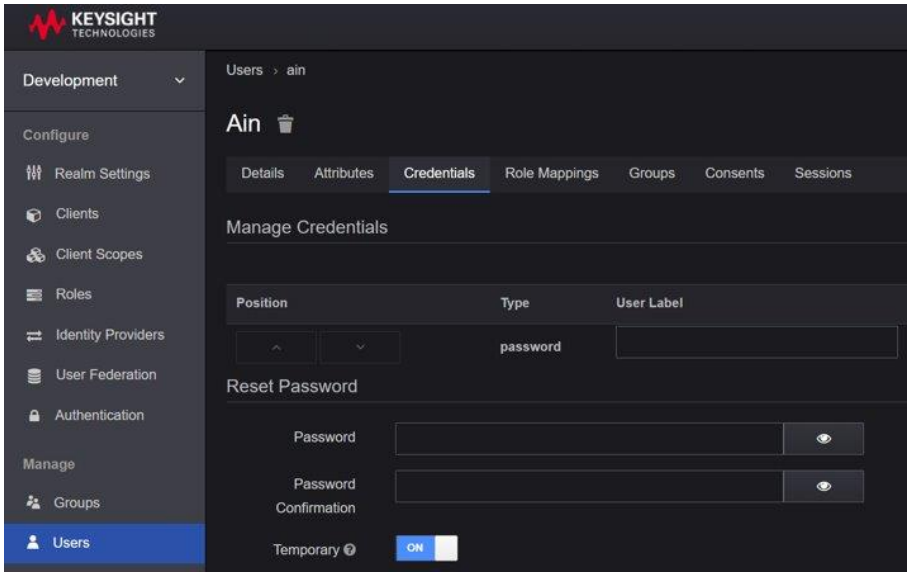
- When the User registration setting is set as **OFF**, only accounts with administrator roles assigned will be able to register new users and set the appropriate roles and access.
- When the User Registration is set to **ON**, any users with the link to the application will be able to register on their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

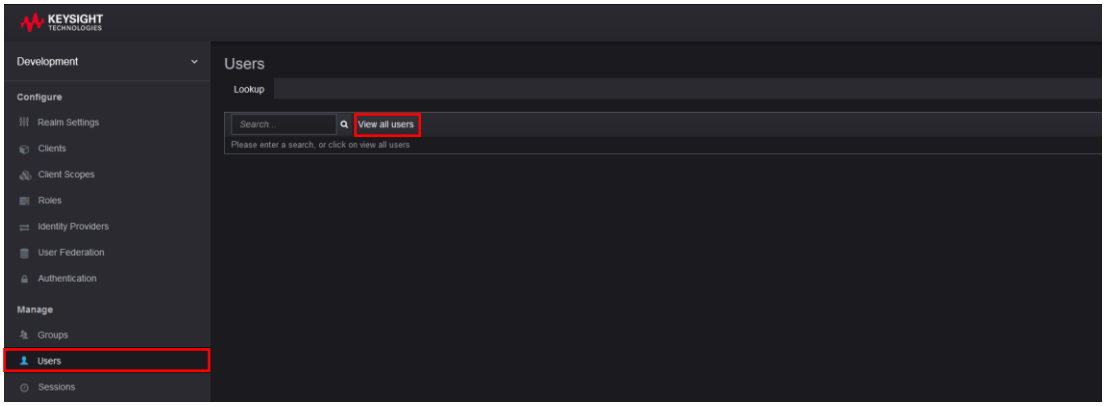
3 Click **Change Password** to update the password to the newly created account. Click **Reset Password** to activate the new password.

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**.

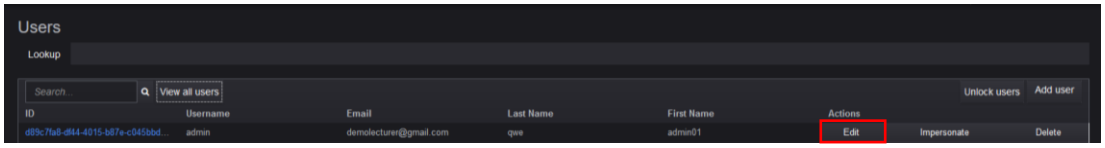
Manage User

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

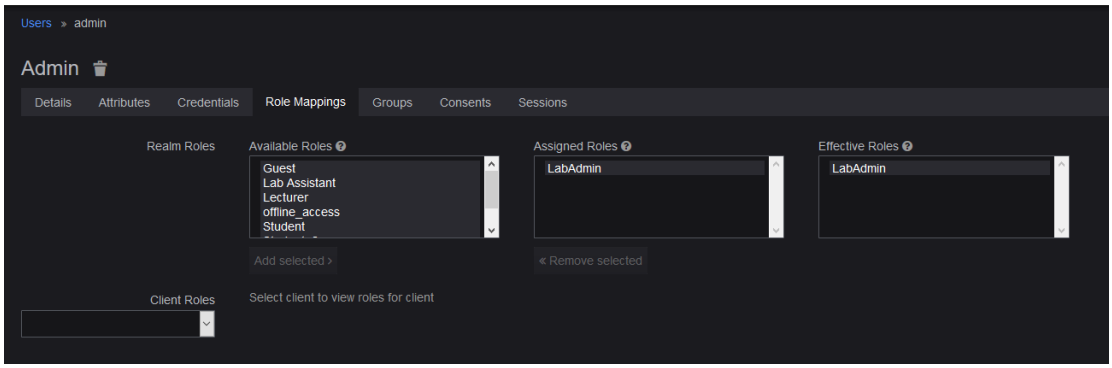
1 To modify the assigned roles for an account, go to **Manage > Users** and click **View all users**.



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.



Enable Email Settings

NOTE

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 Digital Learning Suite Solution.

Once you have set up an identity provider, you may sign in to the Digital Learning Suite Solution application using any of the social providers such as Facebook, Google, or Twitter.

Refer to 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 the Keycloak solution, which is designed following standard security protocols to provide dynamic single sign-on solution.

The University IT can configure the Digital Learning Suite Solution to access the university's active directory. This addresses security concerns, helps eliminate tedious registration process, and streamlines the authentication and authorization process.

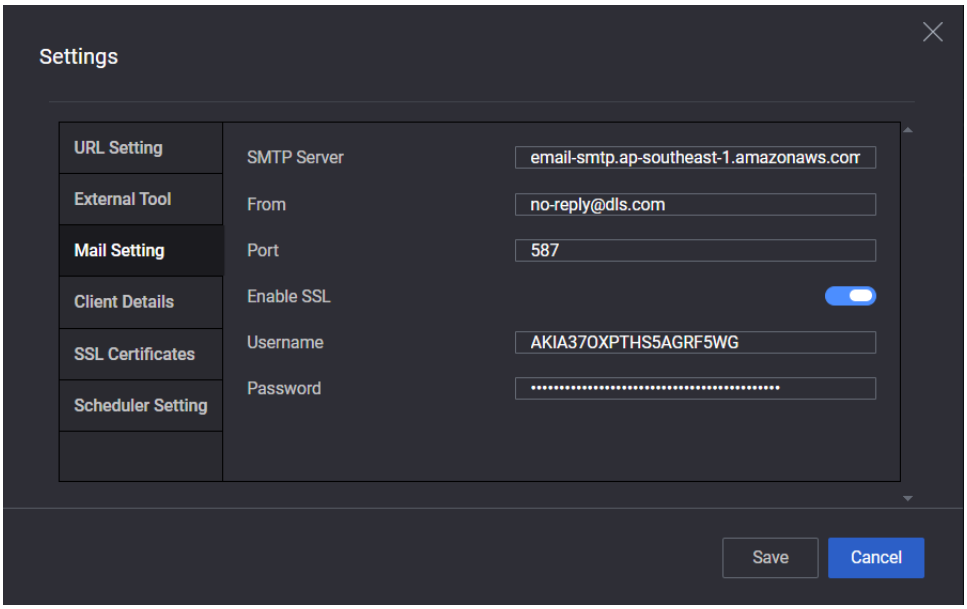
Keycloak's documentation: https://www.keycloak.org/docs/latest/server_admin/

Configure Email Settings

This feature will send a confirmation email to the users to inform them of the status of the sessions in Digital Learning Suite Solution. The setup will depend on the SMTP server setup in the university.

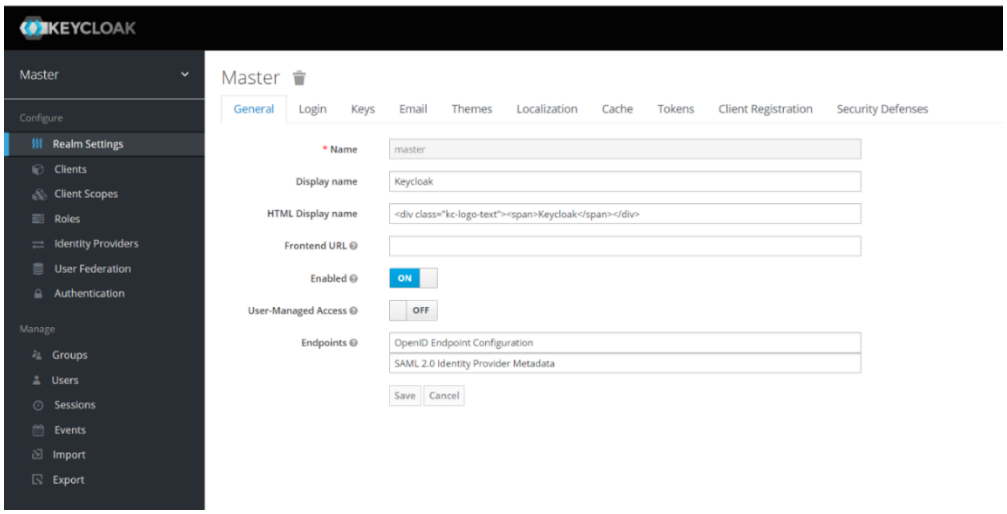
Mail Setting

Enter the information regarding your server.

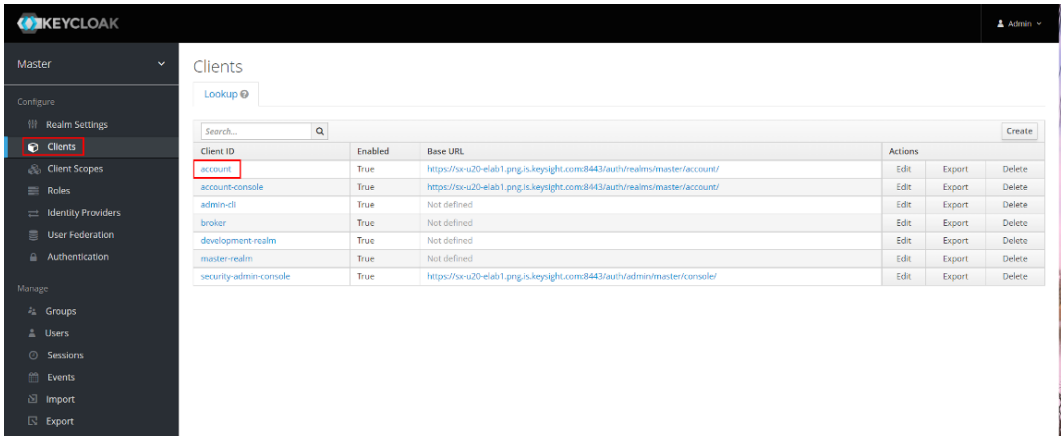


Client Details

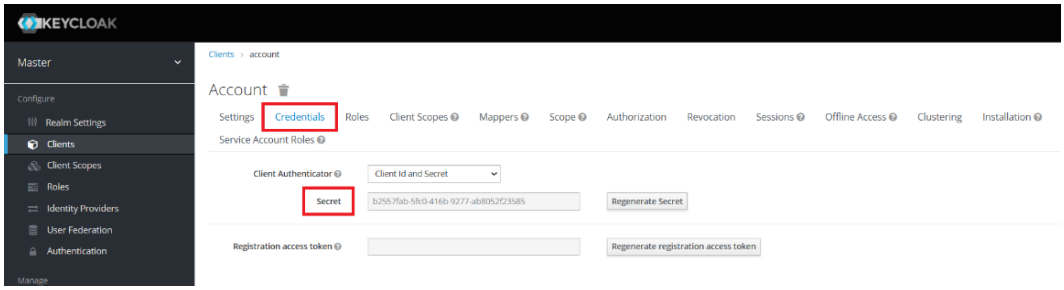
1 Go to **Realm > Master Realm**.



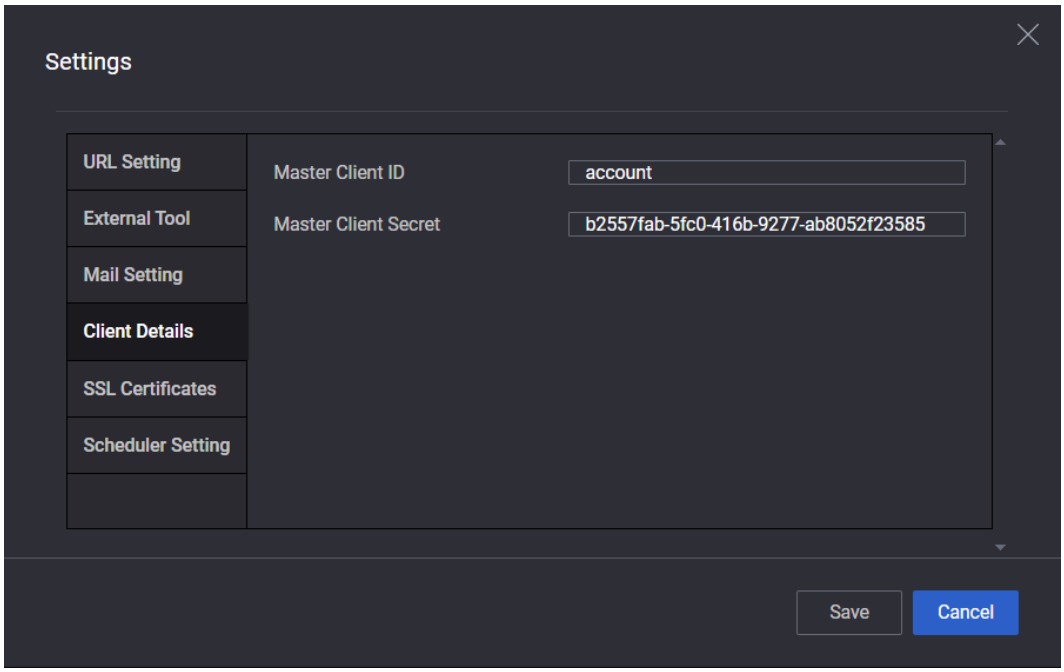
2 In the Clients tab, select **account**.



3 Click the **Credentials** tab and you will see the information in the **Secret** field.



4 The information in the **Master Client ID** and **Master Client Secret** fields in **Digital Learning Suite Home Page > Settings > Client Details** are auto generated. However, if the information in DLS is not a match, copy the information in the **Secret** field and update and save the settings in DLS under **Digital Learning Suite Home Page > Settings > Client Details > Master Client Secret**.



(Optional) Learning Tools Interoperability (LTI) Features

CANVAS

Generate the Developer Key for LTI Implementation

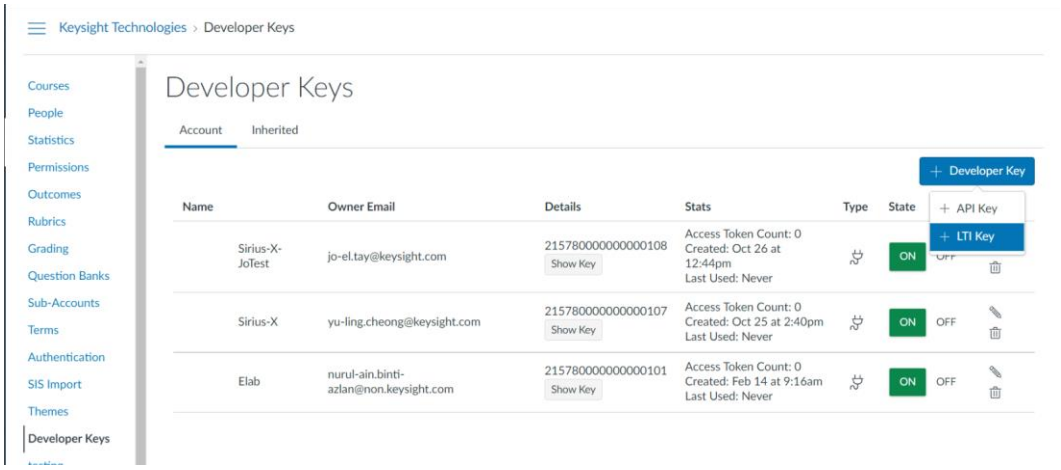
A developer key is used to create custom integrations with Canvas and allow third-party applications.

1 Log into your Canvas account.

2 In **Global Navigation**, click on the **Admin** link and select the name of your account.

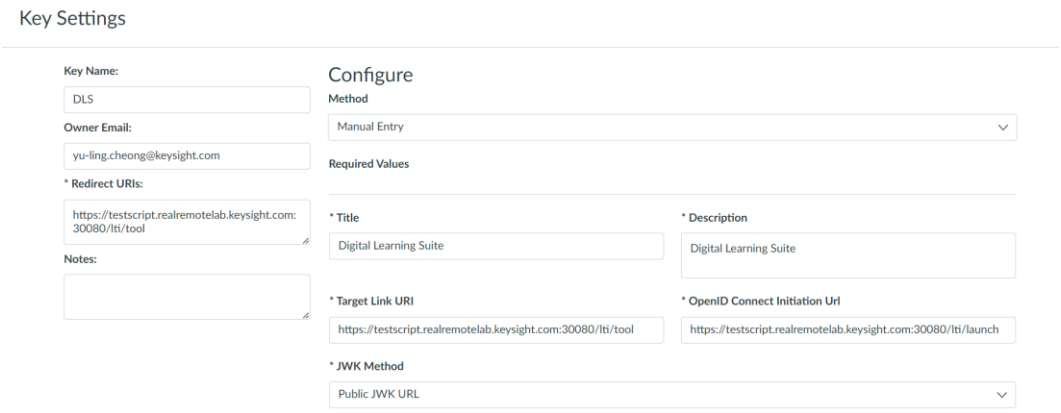
3 From your **Account Navigation**, select the **Developer Keys** option from the left-side menu.

4 Click **+ Developer Key** and select the **+API Key** option.



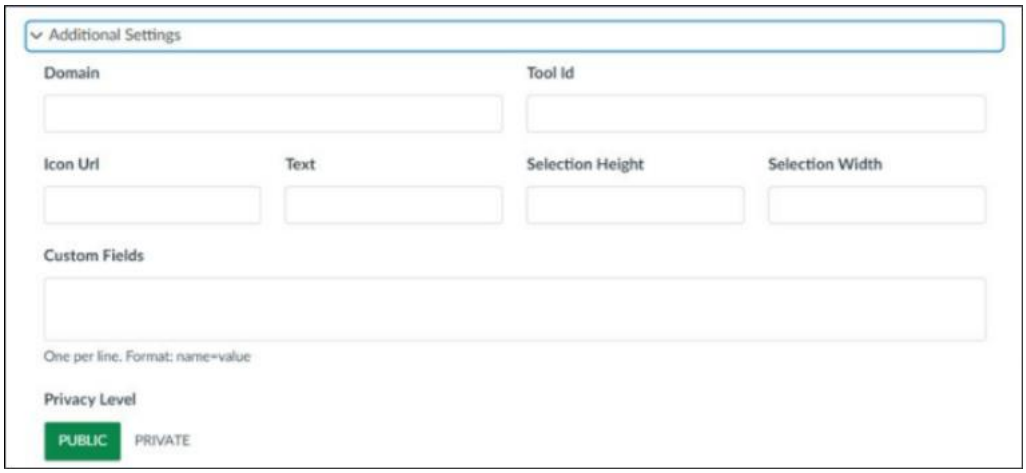
5 Complete the following for **Key Settings**:

- Key Name: The key name can be created according to your school's standard naming conventions
- Owner Email
- Redirect URIs (Legacy)



NOTE

For Additional Settings, change the Privacy Level to PUBLIC so that Canvas is able to pass the relevant information to the tool.

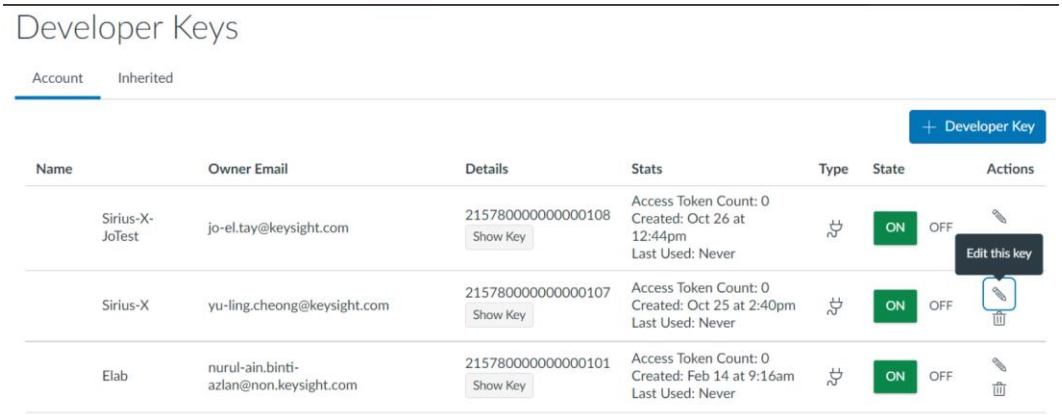


You will see the following error if this is not set.

```
{"messages":["claim is missing []."]."error":null}
```

6 Once you have completed the necessary fields, click **Save Key**.

7 On the **Developer Keys** summary page, set the **State** of the key to **ON**.



Set the Digital Learning Suite Settings

Issuer: https://canvas.instructure.com

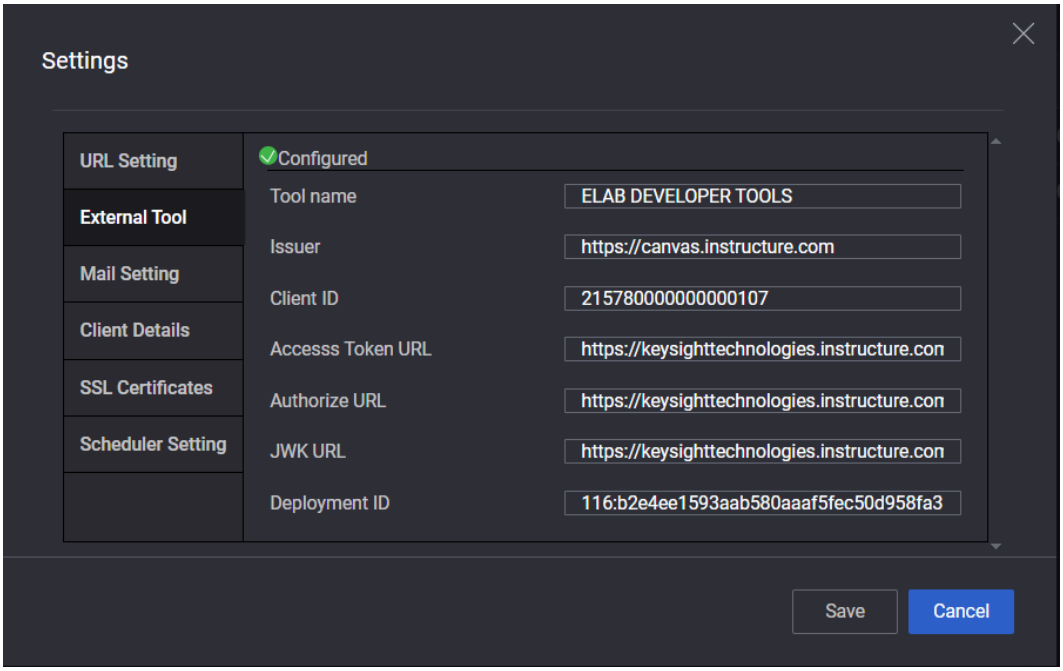
Client ID: Get this from your CANVAS **Developer Key > Details** column

Access Token: https://keysighttechnologies.instructure.com/login/oauth2/token

Authorize URL: https://keysighttechnologies.instructure.com/api/lti/authorize_redirect

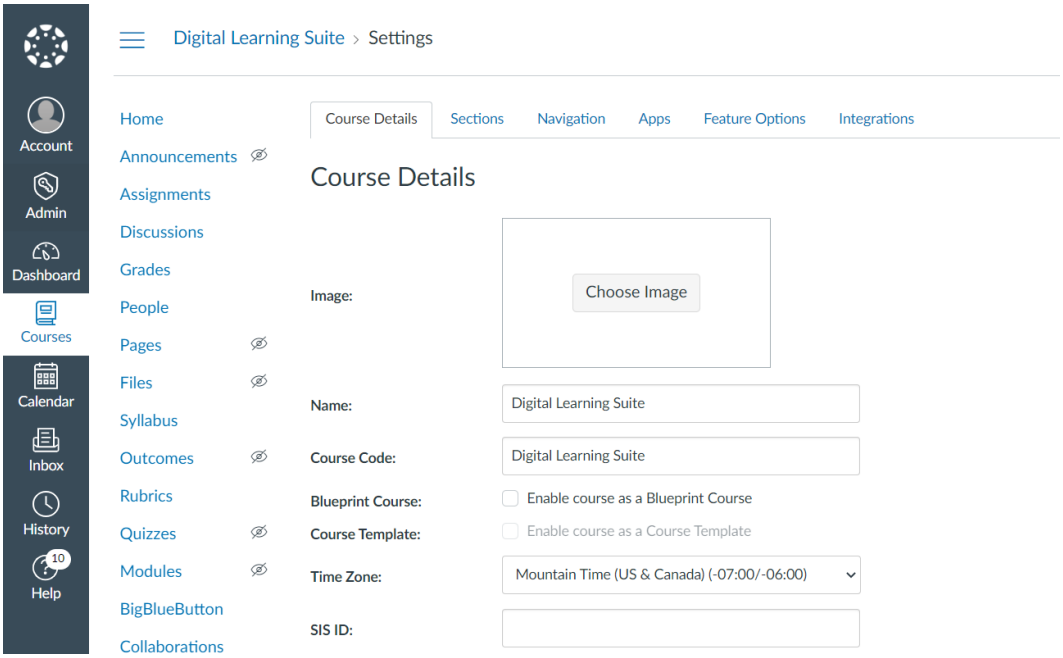
JWK URL: https://keysighttechnologies.instructure.com/api/lti/security/jwks

Deployment ID: Get this from your CANVAS **Developer Key > Show Key**

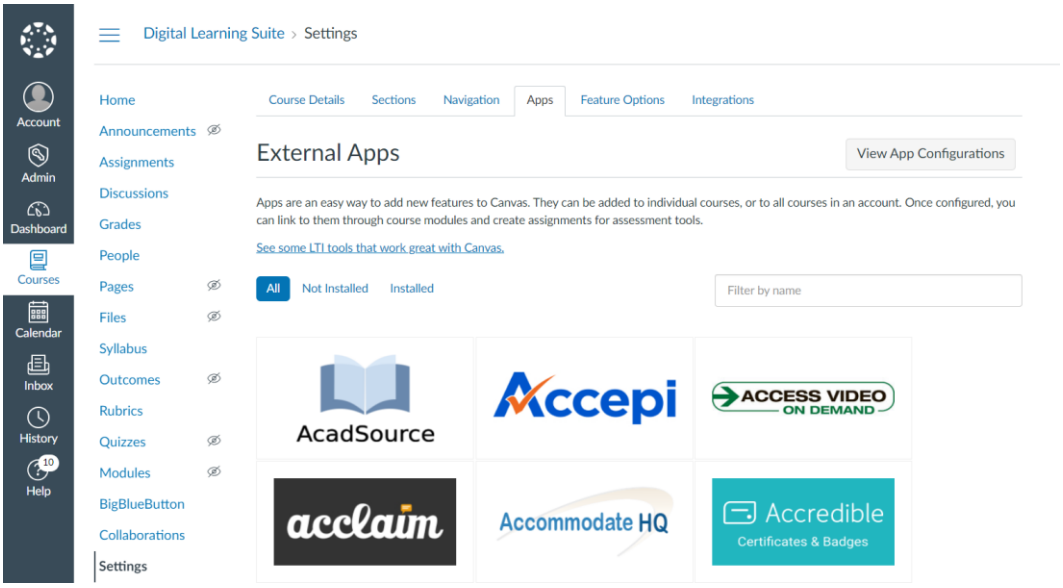


Create the Deep Linking App in Canvas

1 Click on the **Courses** panel and navigate to **Settings**.

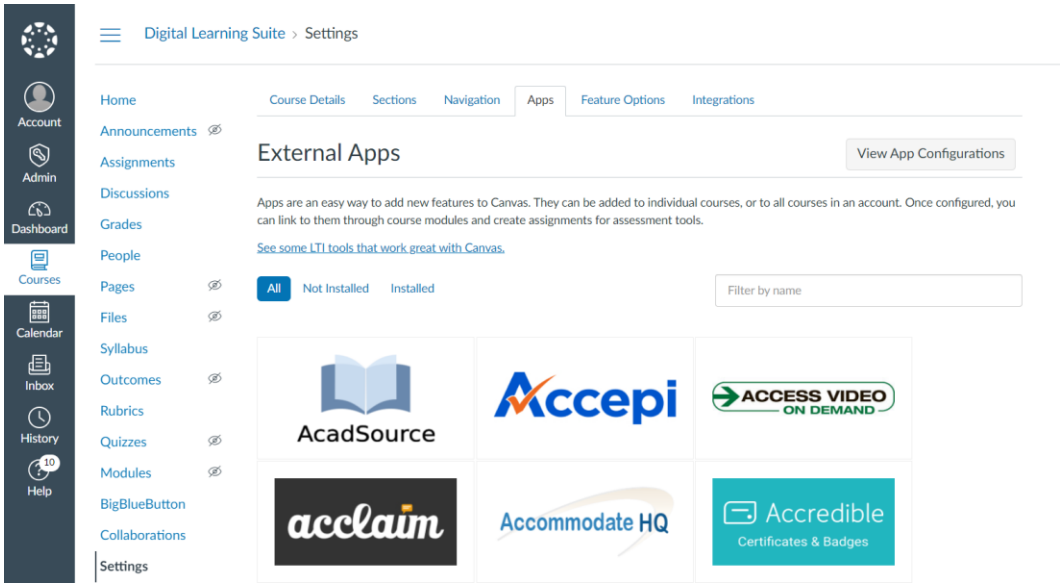


2 On the **Settings** page, select the **Apps** tab.

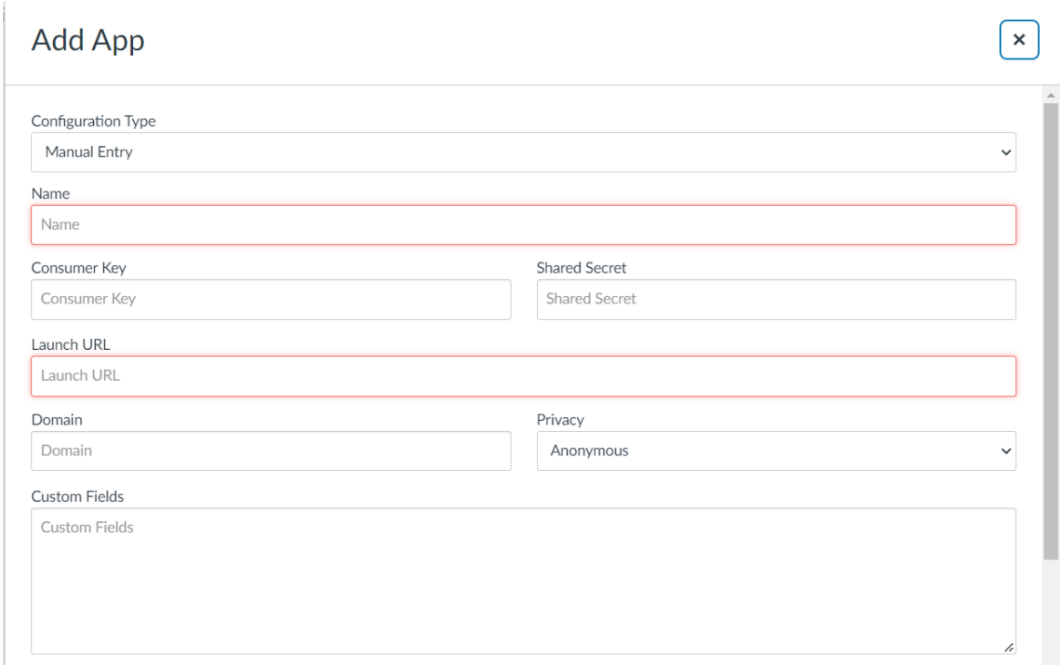


3 At the **Apps** page, click the **+ App** button to create an external link for the LTI integration from your school's Canvas environment to the Digital Learning Suite environment.

If you do not see the **+ App** button, click **View App Configurations** and go to **Add App**.

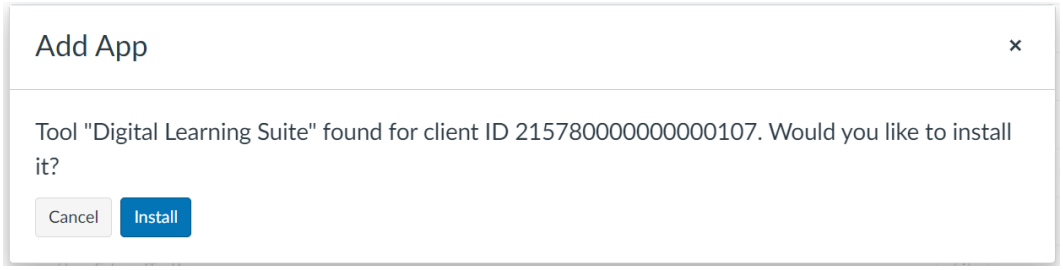


4 Complete the following fields in the **Add App** window.



5 Select **By Client ID** for the **Configuration Type** field and enter the Client ID. Click **Submit**.

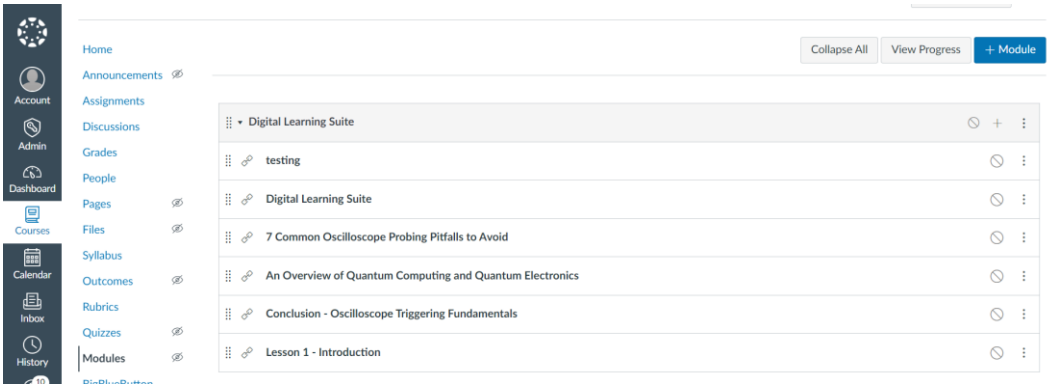
6 Click **Install**.



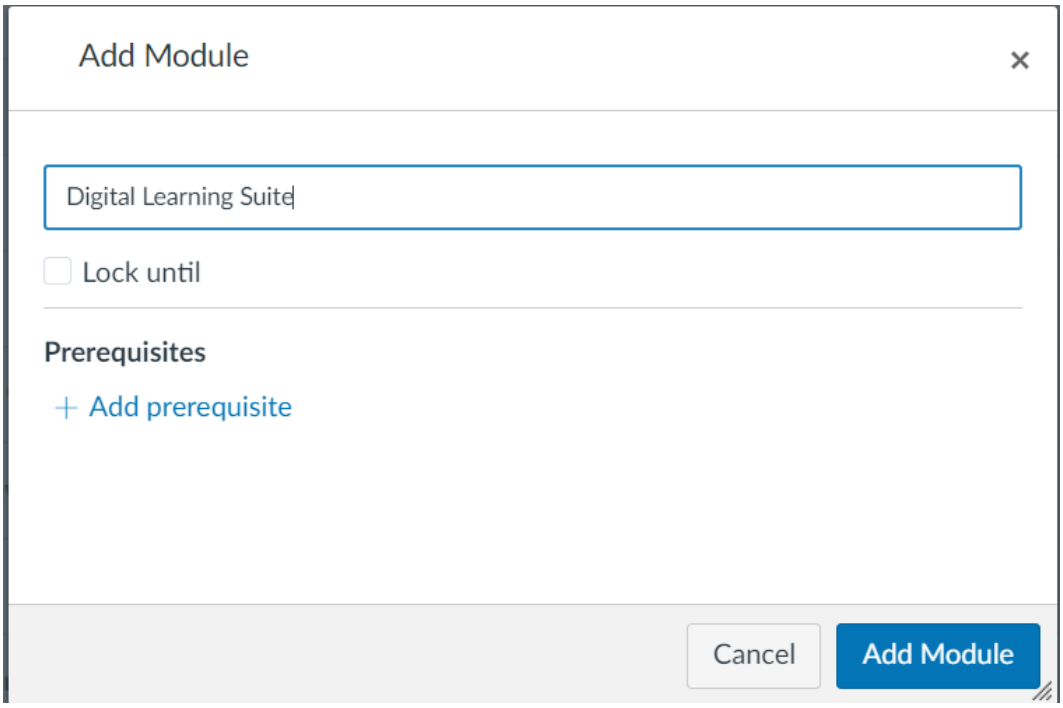
Import Your Course Content

1 Click on the **Courses** panel and navigate to **Modules**.

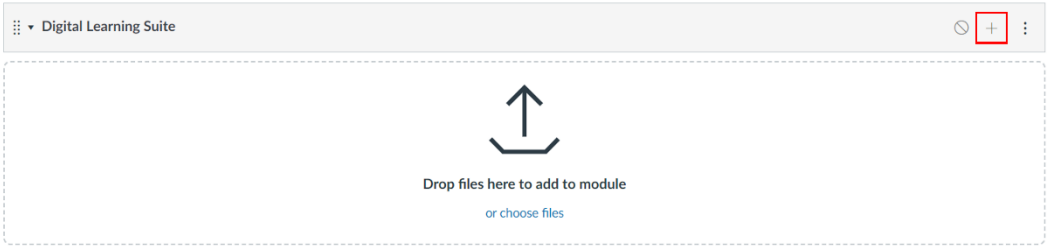
2 On the **Modules** page, click **+ Module** to add a new module to the course.



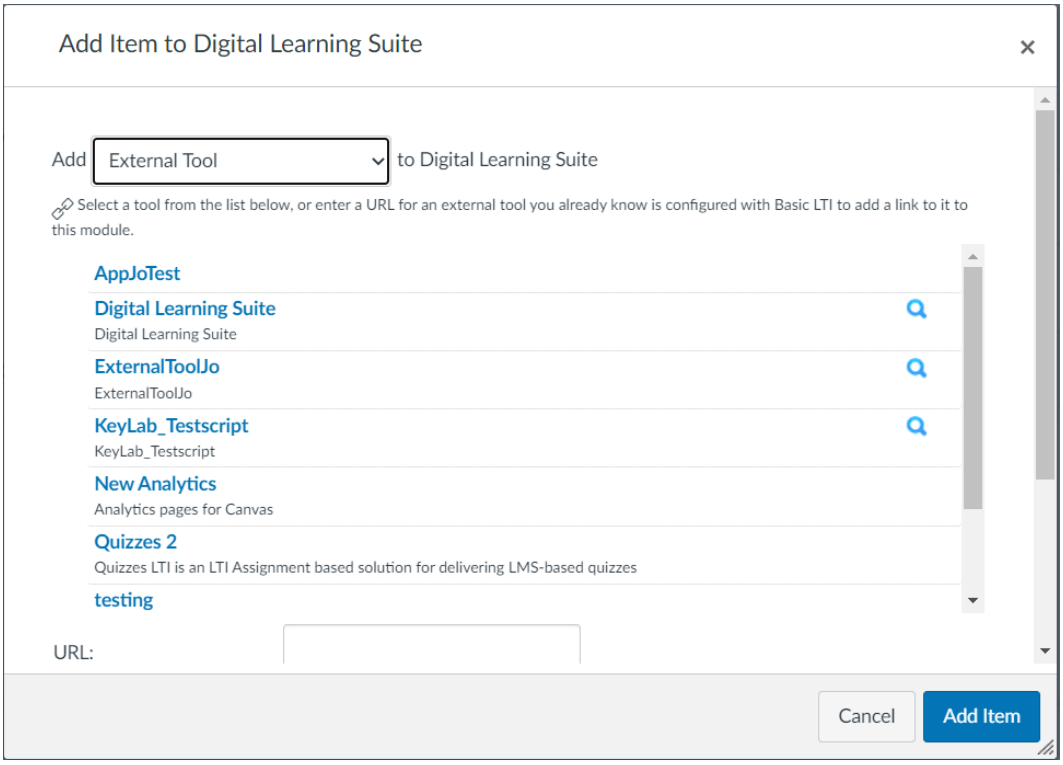
3 Enter **Digital Learning Suite** for the module name and click **Add Module**.



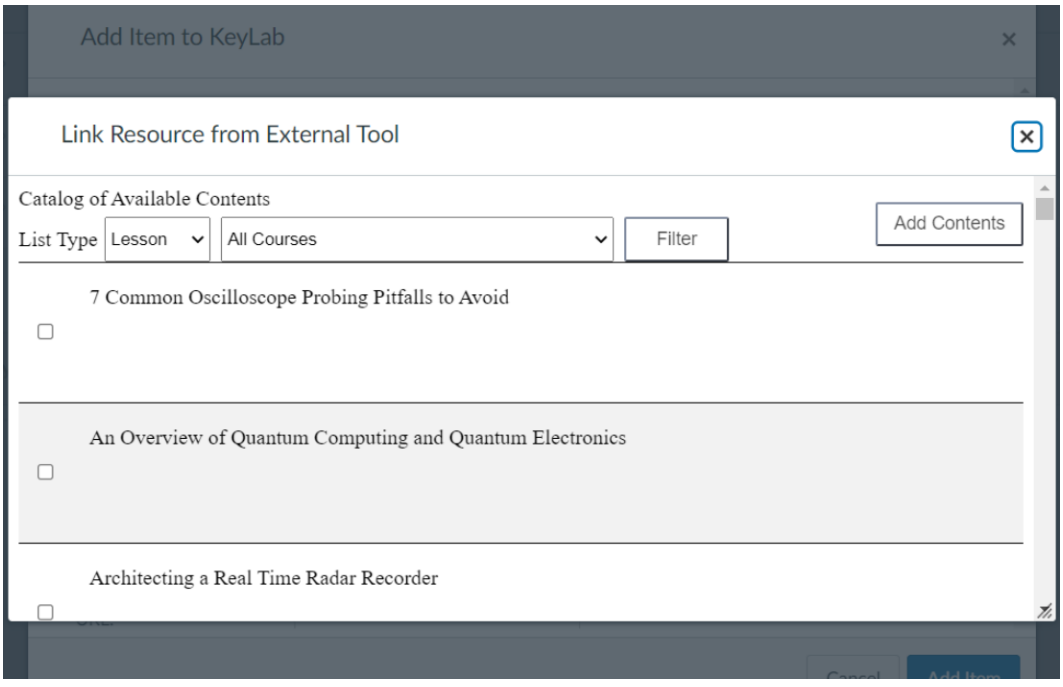
4 Click the **+** icon to add to the module.



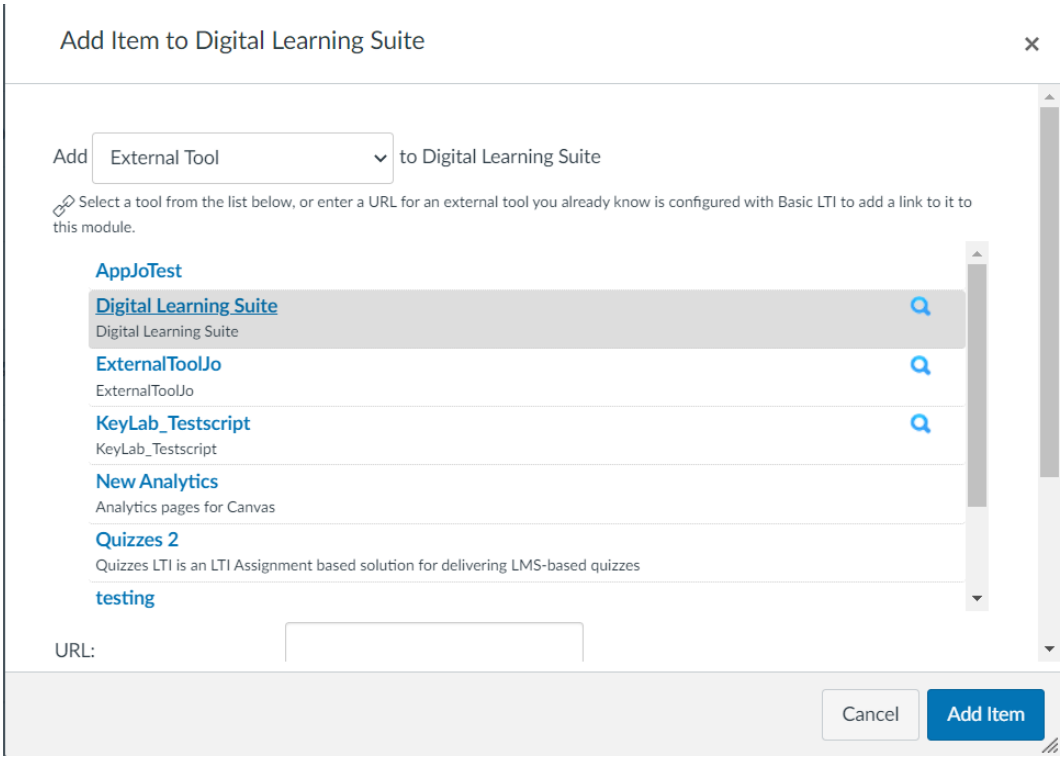
5 Select **External Tool** and click on the blue hyperlink for the newly created tool.



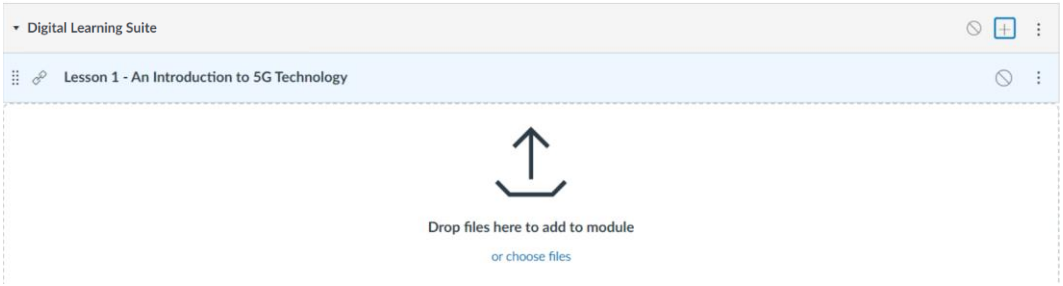
6 Select your topic and click **Add Contents**.



7 Click **Add Item**.



8 You will see the content added to your module.



Moodle

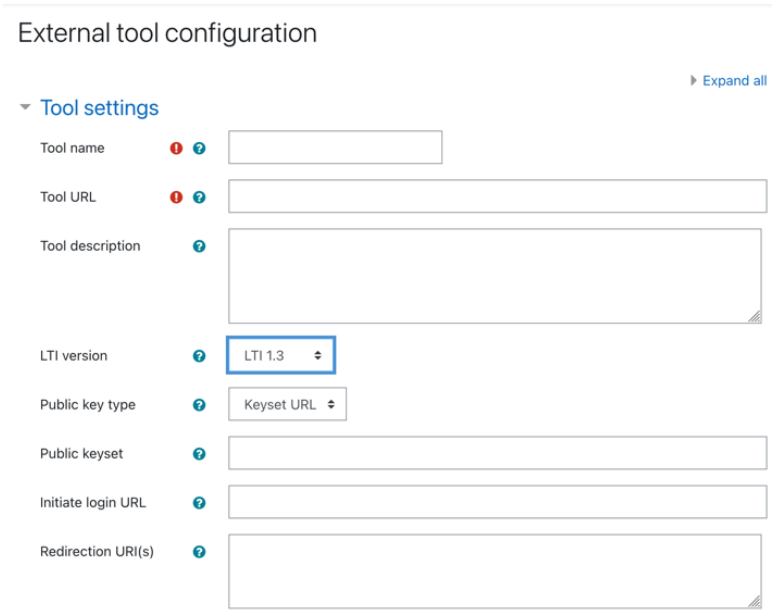
Integrate Moodle and Digital Learning Suite into LTI 1.3

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

Register the LTI 1.3 Tool

1. Navigate to **Site Administration > Plugins > Activity Modules > External Tool > Manage Tools**.
2. Under Manage Tools, select the **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 Digital Learning Suite 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: https://<DLS server URL>:30080
   - **c** LTI version: **LTI 1.3**
   - **d** Public Key Type: Keyset URL
   - **e** Public keyset: https://<DLS server URL>:30080/lti/settingJwkUrl
   - **f** Initiate login URL: https://<DLS server URL>:30080/lti/launch
   - **g** Redirection URL(s): https://<DLS server URL>: 30080/lti/tool
   - **h** Icon URL: https://<DLS server URL>/assets/favicon.png
   - **i** Secure icon URL: https://<DLS server URL>/assets/favicon.png

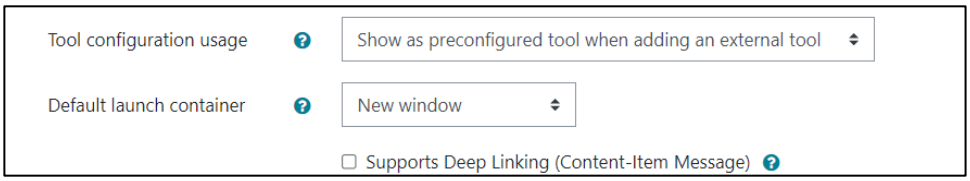
The completed form should appear as below.



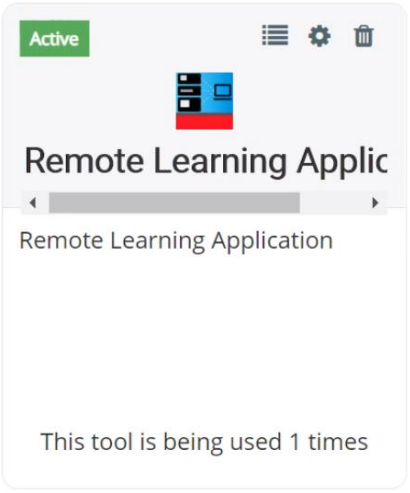
4 Set the following:

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

Default launch container: New window



5 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'.



Use the following information to set up the Digital Learning Suite application.

6 Log in to your Digital Learning Suite application as an administrator and click **Setting External Tool**.

7 Enter the details from Moodle to set it up as an External Tool:

a Tool name: Enter the desired name for Digital Learning Suite 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

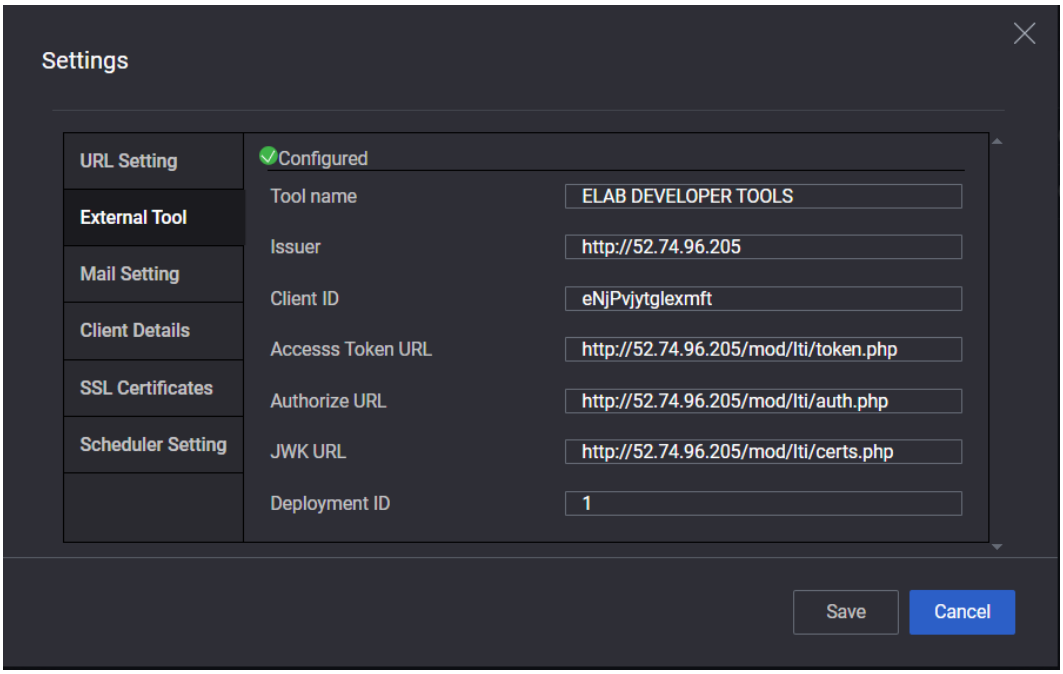
c Client ID: This will use the Application ID for the Moodle application

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.



General Troubleshooting Guide

1. Backend container cannot resolve hostname
2. Virtual Machine unable to update, e.g., cannot find source file
3. Bad Request with two IP addresses at host file
4. 400 Bad Request at Lab Management
5. Session Manager not running
6. Access blocked when accessing a self-signed-cert site using Mozilla Firefox
7. Virtual Machine is not able to connect to FileZilla or PuTTY

Steps and Solutions

1 Backend container cannot resolve hostname

Enter the following commands and add your Virtual Machine IP address and hostname:

```
user@ubuntuserver:/home/elab$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntuserver
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.74.79.25 ubuntuserver (Example)
```

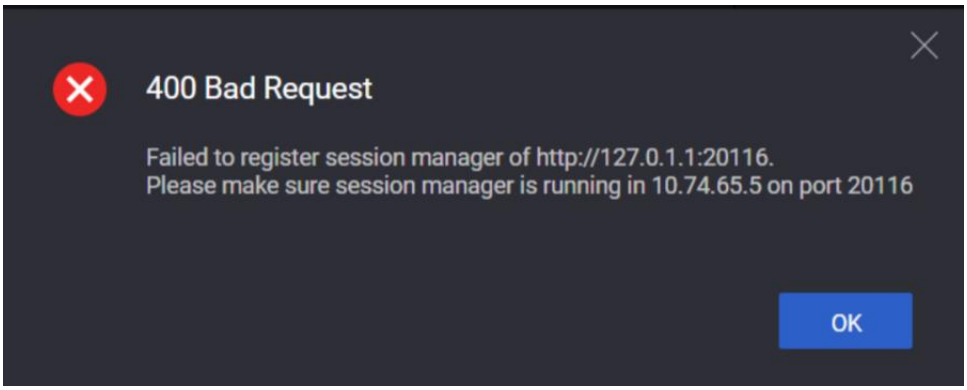
2 Virtual Machine unable to update, e.g., cannot find source file

Apt repo URL is being blocked by IT:

```
sudo nano /etc/apt/sources.list
```

Change to https://mirror.kku.ac.th/ubuntu or to any URL on this list.

3 Bad Request with two IP addresses at host file

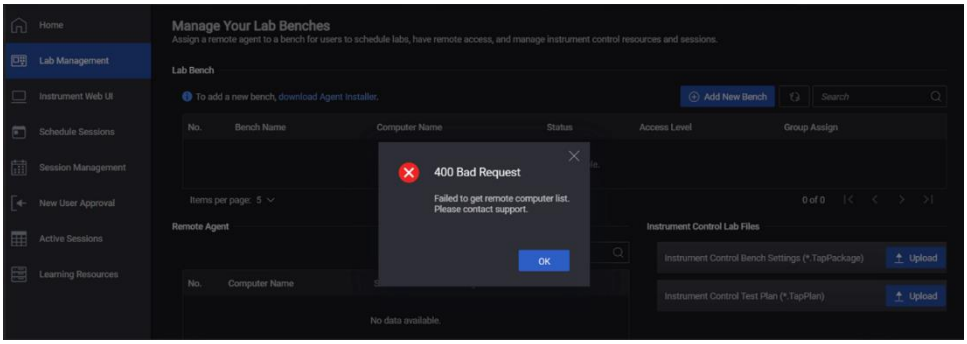


Go to `sudo nano /etc/hosts` and remove the extra IP address 127.0.1.1.

```
  GNU nano 4.8
127.0.0.1 localhost
#127.0.1.1 ubuntuserver

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.74.65.5 ubuntuserver
```

4 400 Bad Request at Lab Management

Meshcentral may down after a restart and sometimes crontab services is not able to run the auto restart for this service.

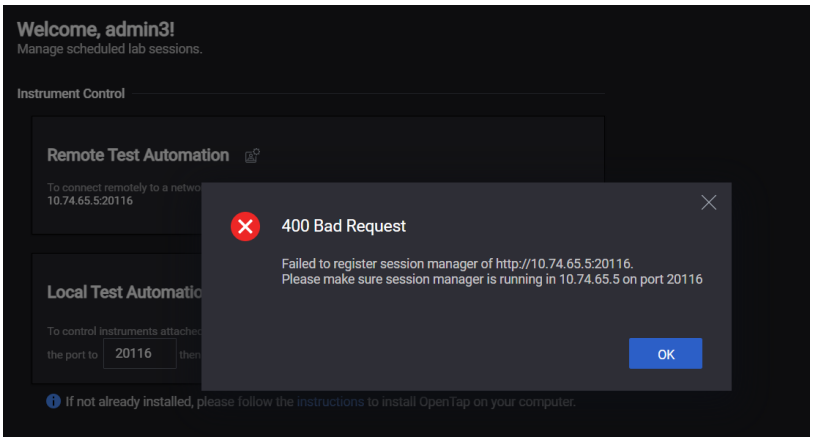


Go to PuTTY and run the following command:

`sudo sh /home/elab/meshcentral-setup-after-deploy.sh`

5 Session Manager not running

Sometimes the session manager service might not be able to start.



Run the following commands:

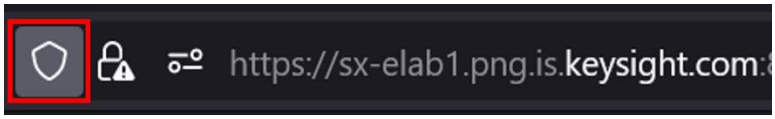
```
sudo -S systemctl enable open-tap
sudo -S systemctl start open-tap
sudo -S systemctl status open-tap
```

6 Access blocked when accessing a self-signed-cert site using Mozilla Firefox

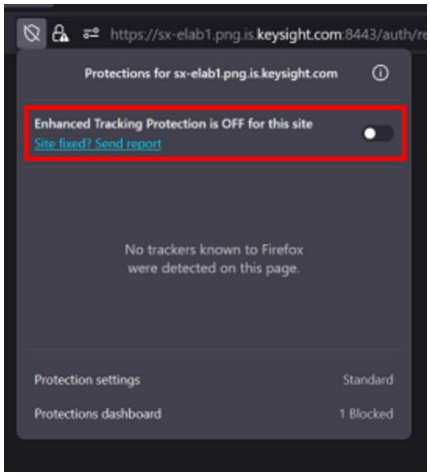
Firefox may block access to a site that uses a self-signed-cert and the user is stopped at the welcome page.

Disable the tracking protection. For example, if the site is **sx-elab1.png.is.keysight.com**:

i Go to sx-elab1.png.is.keysight.com and click the shield icon.



ii Disable the **Enhanced Tracking Protection is ON for this site** feature.



iii Go to **sx-elab1.png.is.keysight.com:30080** and repeat the steps.

7 Virtual Machine is not able to connect to FileZilla or PuTTY

This is because the SSH terminal is not installed in the Virtual Machine.

Run the following commands:

```
sudo apt-get install openssh-server
sudo systemctl enable ssh
sudo systemctl enable ssh --now
sudo systemctl start ssh
```

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 cracked easily.

- Do not write passwords down, anywhere

  Memorize them or use a password management application to keep track of your passwords.

- 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.

Printed in Malaysia
Edition 6, April 2025

SR101-90000
www.keysight.com