
SR101EDUA Digital Learning Suite

Notices

Copyright Notice

© Keysight Technologies 2023–2024

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

SR101-90000

Edition

Edition 3, March 2024

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 DFARS 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, INCLUDING 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 CONTAINED 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

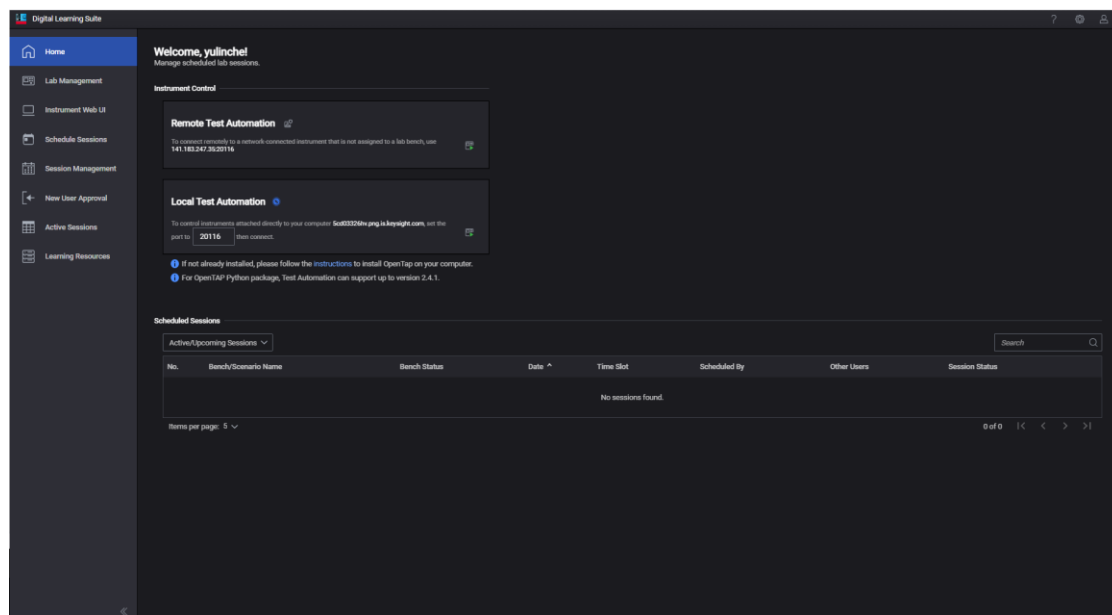
Table of Contents

Notices.....	1
Sales and Technical Support	2
Overview	5
Intended Use of the Installation Guide.....	6
Introduction	6
System Requirements	7
Software Requirements.....	7
Get Started	8
Software License.....	8
Trial License	8
Full License	8
Overview: Installation Flow	9
Step 1: Download Preconfigured Virtual Machine Image File	10
Step 2: Import and Restore Preconfigured Virtual Machine.....	10
VirtualBox.....	10
Proxmox Virtual Environment (VE)	14
Step 3: Start and Set Up Virtual Machine.....	18
Step 4: Customize Server Settings	22
Step 5: Reboot Virtual Machine	22
Step 6: Ensure Resolvable Hostname.....	23
Step 7: Set Up Keycloak.....	23
Step 8: Install License Files	25
Step 9: Check Client Details Settings	26
Step 10: Set Up Server Configurations.....	27
(Optional) Upload New Valid SSL or Self-Signed Certificate and Private Key.....	28
Keycloak Settings.....	30
Change the Keycloak Default Admin Password	30
Create Super-Admin Accounts.....	31

Keycloak Administration Console.....	32
Configuration and Settings	33
Configure Roles	33
Add User	35
Manage User.....	37
Enable Email Settings.....	38
Set up Single Sign-On (SSO)	38
Configure Email Settings.....	39
Mail Setting.....	39
Client Details.....	39
(Optional) Learning Tools Interoperability (LTI) Features	41
CANVAS.....	41
Generate the Developer Key for LTI Implementation	41
Set the Digital Learning Suite Settings.....	42
Create the Deep Linking App in Canvas	43
Import Your Course Content	46
Blackboard.....	49
Integrate Digital Learning Suite into LTI 1.3 Blackboard	49
Add External Tools in the Blackboard Platform	52
Obtain the Deployment ID.....	56
Add Detail to Application.....	57
Launch the Application in Blackboard	58
Moodle.....	59
Integrate Moodle and Digital Learning Suite into LTI 1.3.....	59
Register the LTI 1.3 Tool.....	59
General Troubleshooting Guide	62
Recommended Password Practices	66

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

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	
NOTE: See Introduction to get a basic overview of VirtualBox and Proxmox .		
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	<p>For Windows 10</p> <ol style="list-style-type: none"> 1 VirtualBox – https://www.virtualbox.org/ 2 FileZilla – https://filezilla-project.org/download.php?type=client 3 PuTTY – Latest release (0.78) <p>For Proxmox Virtual Environment</p> <ol style="list-style-type: none"> 1 FileZilla – https://filezilla-project.org/download.php?type=client 2 PuTTY – Latest release (0.78)
Supported LTI Compliant LMS Integration	<p>Moodle v3.9 and above Blackboard Canvas</p> <p>For other LTI compliant LMS platforms, please contact Keysight Technologies for further information.</p>
Supported Web Browsers	<p>Microsoft Edge v107.0.1418.62 and above Google Chrome v108.0.5359.94 and above Mozilla Firefox v107.0.1 and above</p>

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**.

Go to the links below to obtain a trial license:

- PW9300EDU-TRL
<https://ksm.software.keysight.com/ASM/External/TrialLicense.aspx?ProdNum=PW9300EDU-TRL>.
- KS8400EDU-TRL
<https://ksm.software.keysight.com/ASM/External/TrialLicense.aspx?ProdNum=KS8400EDU-TRL>

Full License

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

NOTE

Save the license files to a folder on the Windows PC. These **license files** are required when accessing the DLS application.

Overview: Installation Flow

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

NOTE

You can skip **Step 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: *dls0v02_03052023.ova*
- Proxmox Image File: *vzdump-qemu-103-03052023.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

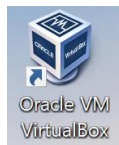
VirtualBox

NOTE

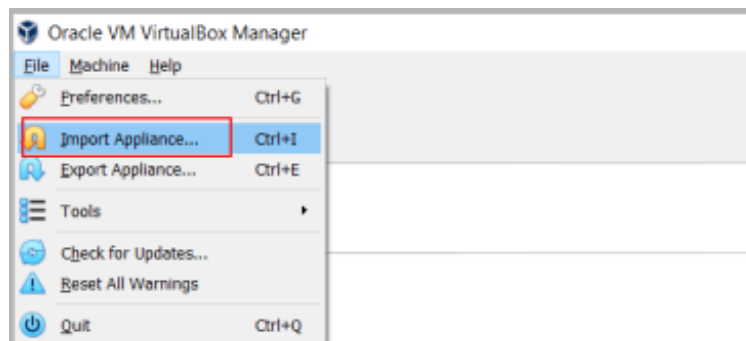
If VirtualBox is not installed/running on your Windows 10, follow the steps below to set up the Oracle VirtualBox on your PC before proceeding with **Step 2: Import and Restore Preconfigured Virtual Machine**.

- 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.

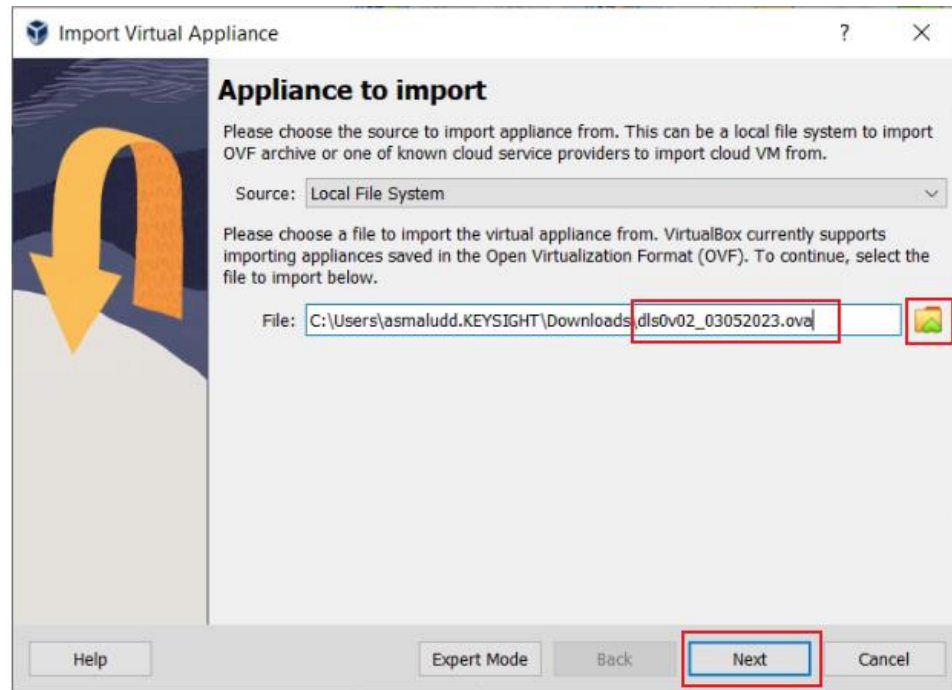
-
- 1 Click on the **Oracle VM VirtualBox** icon to launch the application.



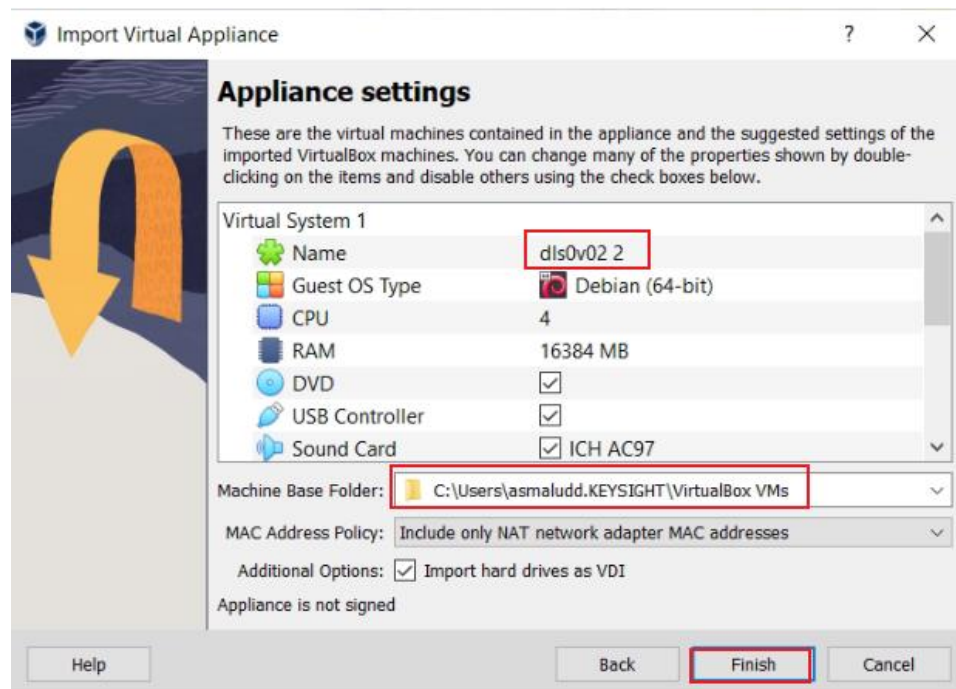
- 2 Go to **File** and click on **Import Appliance...**



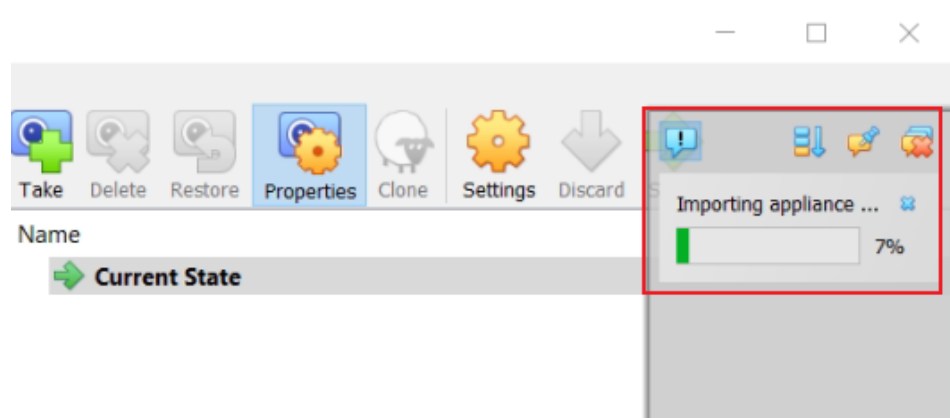
- 3 Browse to the folder where you have downloaded the VirtualBox image file and select *dls0v02_03052023.ova*. Click **Next** to proceed.



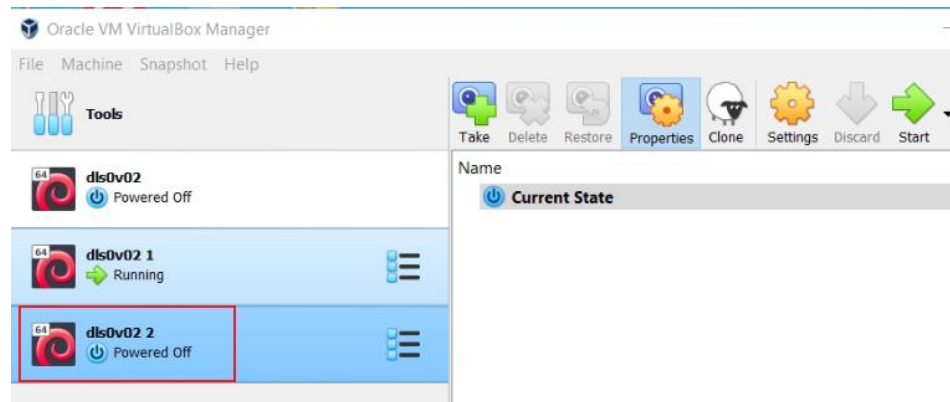
- 4 If required, change the name and default path of the Virtual Machine (VM) as shown below and click **Finish**.



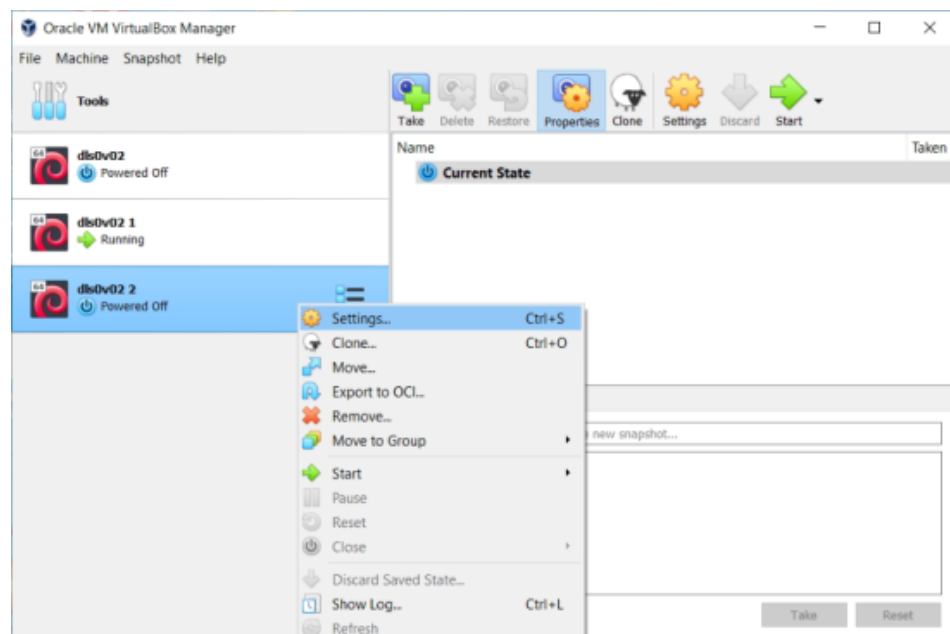
- 5 The application will now create a new Virtual Machine. Wait until the process is complete.



- 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**.



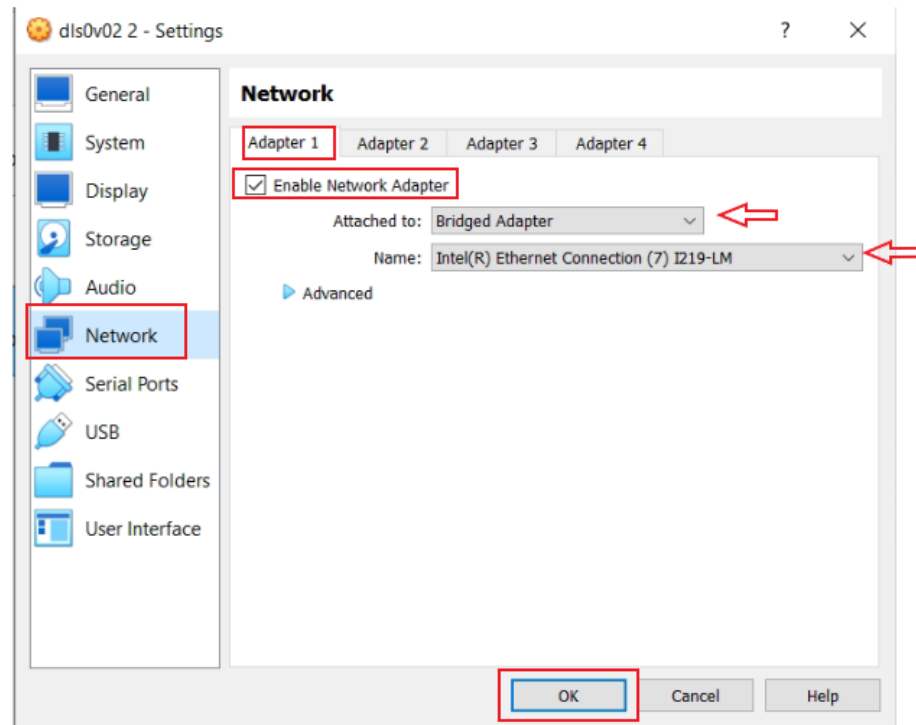
Click on **Network** and select the tab for **Adapter 1**. Set the following:

- 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.

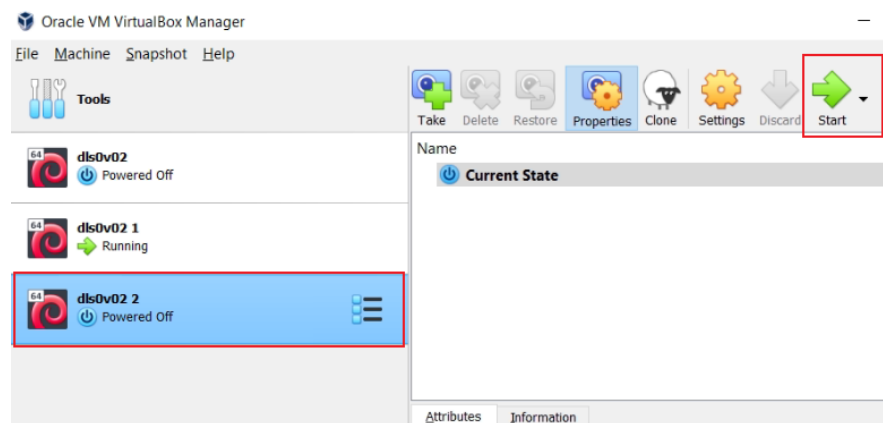
NOTE

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.

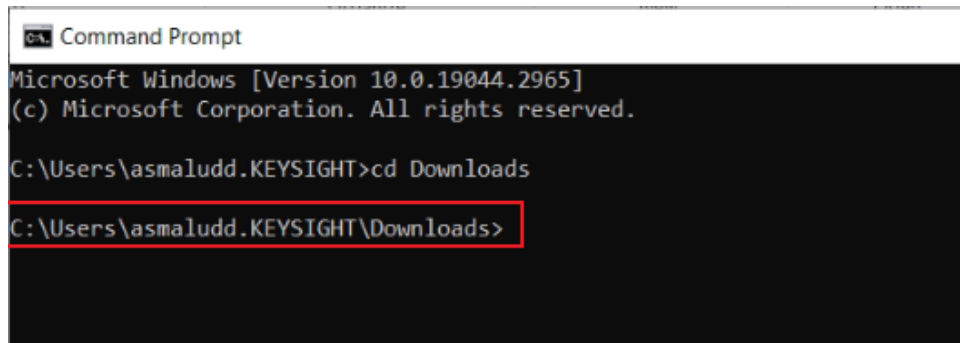


- 8 Select the new Virtual Machine in the left-pane of the Oracle VM VirtualBox Manager and click on **Start** to start the Virtual Machine.

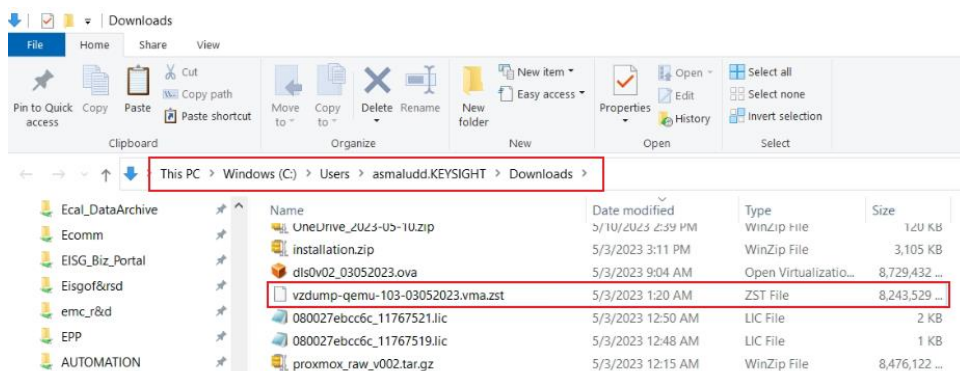


Proxmox Virtual Environment (VE)

- 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.

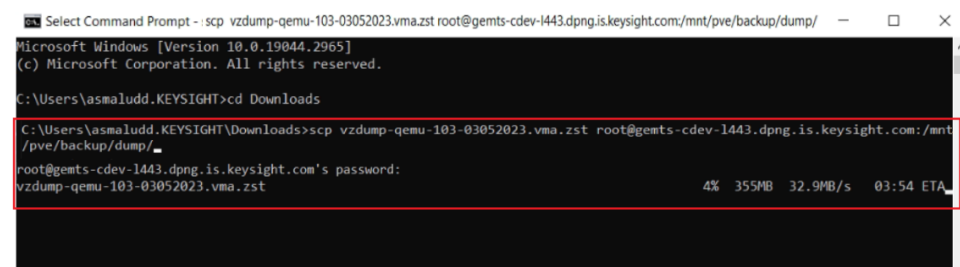


In this example, the Proxmox image file is stored in the **Downloads** folder.

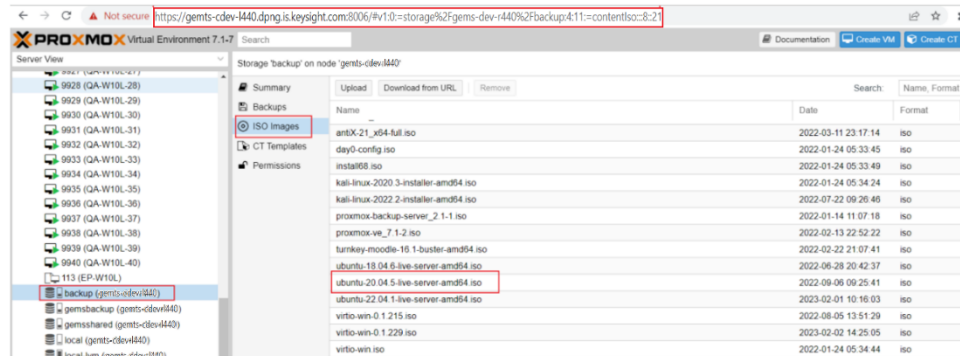


- b Run this command, replacing `gemts-cdev-l440.dpng.is.keysight.com` seen in the image below with your Proxmox server URL: `scp vzdump-qemu-103-03052023.vma.zst <your username>@<your proxmox server url>:/mnt/pve/backup/dump/`

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:

- Open the Windows command terminal.
- Run the command `#ssh <username>@<proxmox server url>` and log in with your password.
- Run the following commands:

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

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

```
root@gems-cdev-1440:/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@gems-cdev-1440:/mnt/pve/backup/template/iso# ls -la | grep ubuntu-20.04.5-live-server-amd64.iso
root@gems-cdev-1440:/mnt/pve/backup/template/iso#
```

If this happens, go to the Ubuntu [webpage](https://ubuntu.com/download/server#downloads) to download the image file.



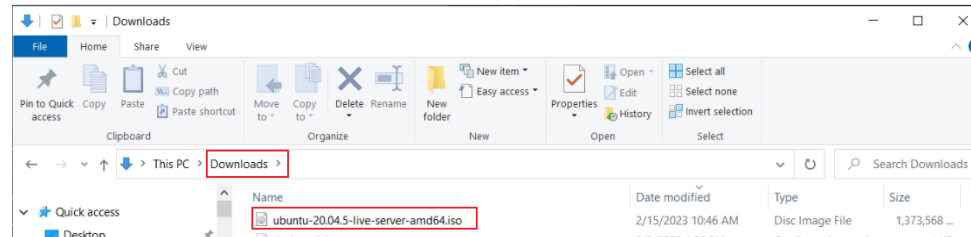
Use the **cd** command at windows command line to go to where the downloaded Ubuntu server image file, *ubuntu-20.04.5-live-server-amd64.iso*, is stored.

```

Command Prompt
Microsoft Windows [Version 10.0.19044.2965]
(c) Microsoft Corporation. All rights reserved.

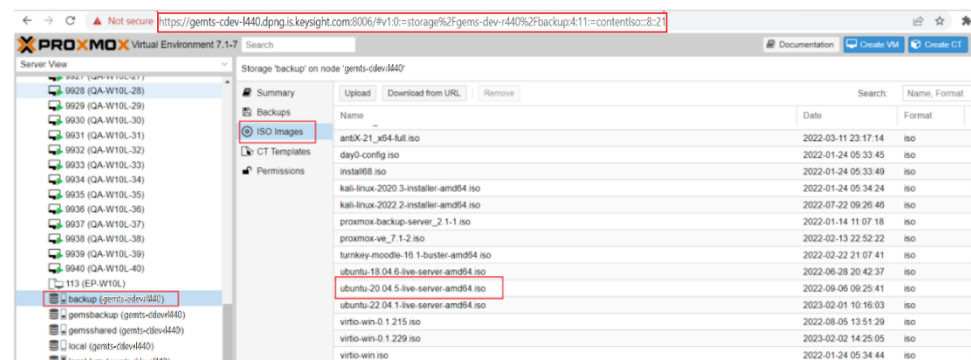
C:\Users\asmaludd\KEYSIGHT>cd Downloads
C:\Users\asmaludd\KEYSIGHT\Downloads>scp ubuntu-20.04.5-live-server-amd64.iso root@gemts-cdv-1440.dpng.is.keysight.com:/mnt/pve/backup/template/iso

```

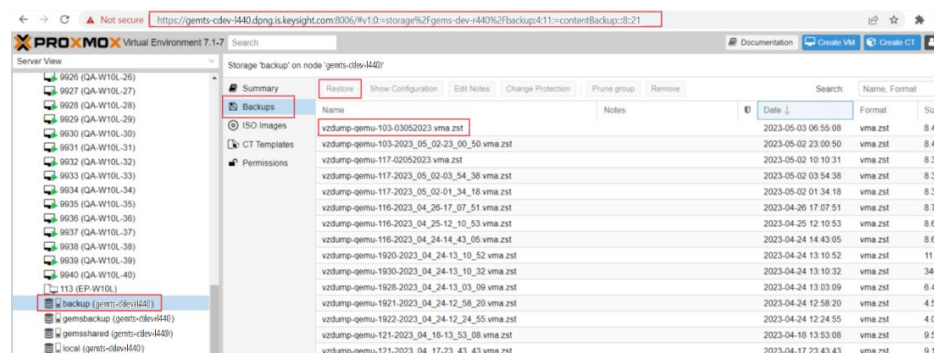


Use this command to transfer the Ubuntu server image to your Proxmox server: `scp ubuntu-20.04.5-live-server-amd64.iso <your username>@<your proxmox server url>:/mnt/pve/backup/template/iso`

- ✓ 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>.



- 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**.

Restore: VM

Source: vzdump-qemu-103-03052023.vma.zst

Storage: From backup configuration

VM ID: 102

Bandwidth Limit: Defaults to target storage restore limit MiB/s

Unique: ☒ Start after restore: ☐

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.

Task viewer: VM 102 - Restore

Output Status

Stop

progress 87% (read 46707769344 bytes, duration 60 sec)
progress 88% (read 47244640256 bytes, duration 60 sec)
progress 89% (read 47781511168 bytes, duration 60 sec)
progress 90% (read 48318382080 bytes, duration 60 sec)
progress 91% (read 48855252992 bytes, duration 60 sec)
progress 92% (read 49392123904 bytes, duration 60 sec)
progress 93% (read 49928994816 bytes, duration 60 sec)
progress 94% (read 50465865728 bytes, duration 60 sec)
progress 95% (read 51002736640 bytes, duration 60 sec)
progress 96% (read 51539607552 bytes, duration 60 sec)
progress 97% (read 52076478464 bytes, duration 60 sec)
progress 98% (read 52613349376 bytes, duration 60 sec)
progress 99% (read 53150220288 bytes, duration 60 sec)
progress 100% (read 53687091200 bytes, duration 60 sec)
total bytes read 53687091200, sparse bytes 31973744640 (59.6%)
space reduction due to 4K zero blocks 1.19%
rescan volumes...
TASK OK

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.

PROXMOX Virtual Environment 7.1-7

Server View

Virtual Machine 102 (ds0v02-pc) on node 'gems-dev1440'

Summary Edit Revert

Name ds0v02-pc

Start at boot No

Start/Shutdown order order=any

OS Type Linux 5.x - 2.6 Kernel

Boot Order scsi0, ide2, net0

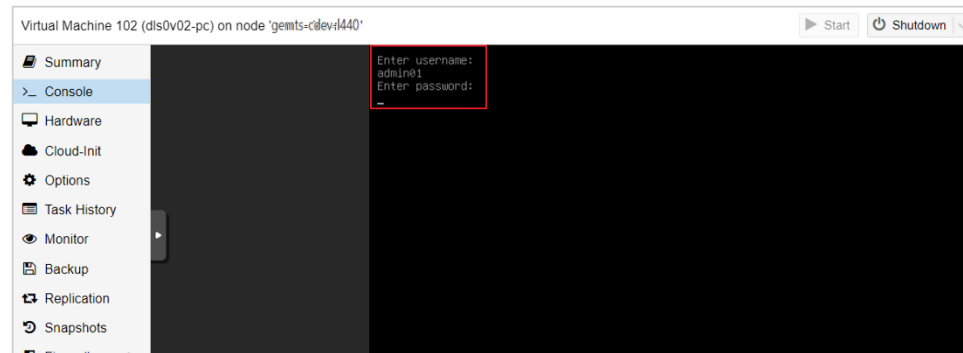
Use tablet for pointer Yes

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



Step 3: Start and Set Up Virtual Machine

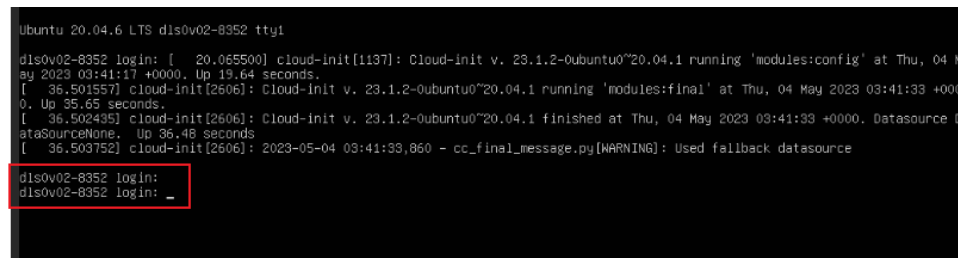
- Pressing **Start** will take you to the bootup login screen. Enter the following to start bootup:
 - Username: **admin01**
 - Default password: **KeyS1ght4u!D!s**



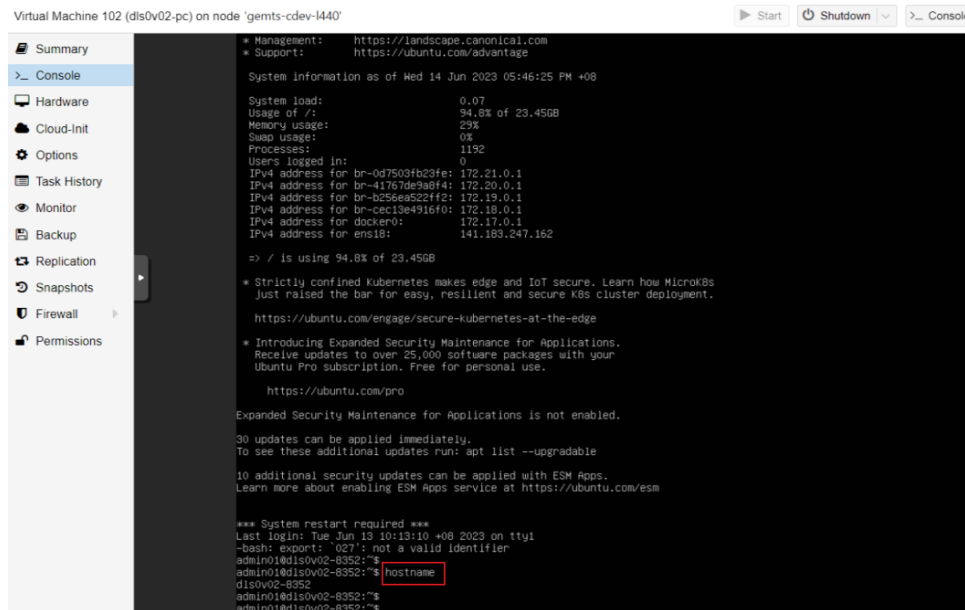
NOTE

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.

- If this is the first bootup, the Virtual Machine will immediately auto reboot and return you to the bootup login screen. Again, enter the username and default password to start bootup.
- After bootup is complete, enter the username **admin01** and default password **KeyS1ght4u!D!s** at the user login prompt.



- 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.



```
Virtual Machine 102 (disov02-pc) on node 'gemts-cdev-l440'
```

```
Summary
> Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
```

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

System Information as of Wed 14 Jun 2023 05:46:25 PM +08

System load: 0.07
Usage of /: 94.8% of 23.45GB
Memory usage: 23%
Swap usage: 0%
Processes: 1192
Users logged in: 0
IPv4 address for br-0d7503fb23fe: 172.21.0.1
IPv4 address for br-41767de9a8f4: 172.20.0.1
IPv4 address for br-b256ea522ff2: 172.19.0.1
IPv4 address for br-ccc13e4916f0: 172.18.0.1
IPv4 address for docker0: 172.17.0.1
IPv4 address for ens18: 141.183.247.162

=> / is using 94.8% of 23.45GB

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  Just raised the bar for easy, resilient and secure K8s cluster deployment.
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.
  https://ubuntu.com/pro

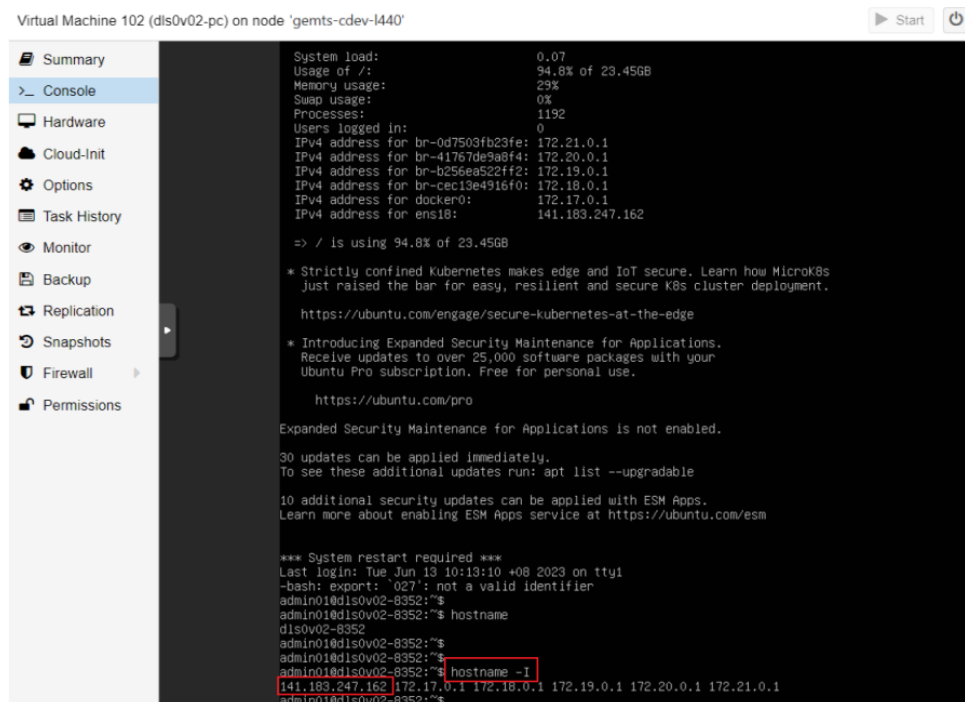
Expanded Security Maintenance for Applications is not enabled.

30 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

10 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

*** System restart required ***
Last login: Tue Jun 13 10:13:10 +08 2023 on tty1
-bash: export: `027': not a valid identifier
admin01@disov02-8352:~$ hostname
disov02-8352
admin01@disov02-8352:~$
```

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



```
Virtual Machine 102 (disov02-pc) on node 'gemts-cdev-l440'
```

```
Summary
> Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
```

```
System load: 0.07
Usage of /: 94.8% of 23.45GB
Memory usage: 23%
Swap usage: 0%
Processes: 1192
Users logged in: 0
IPv4 address for br-0d7503fb23fe: 172.21.0.1
IPv4 address for br-41767de9a8f4: 172.20.0.1
IPv4 address for br-b256ea522ff2: 172.19.0.1
IPv4 address for br-ccc13e4916f0: 172.18.0.1
IPv4 address for docker0: 172.17.0.1
IPv4 address for ens18: 141.183.247.162

=> / is using 94.8% of 23.45GB

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  Just raised the bar for easy, resilient and secure K8s cluster deployment.
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.
  https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

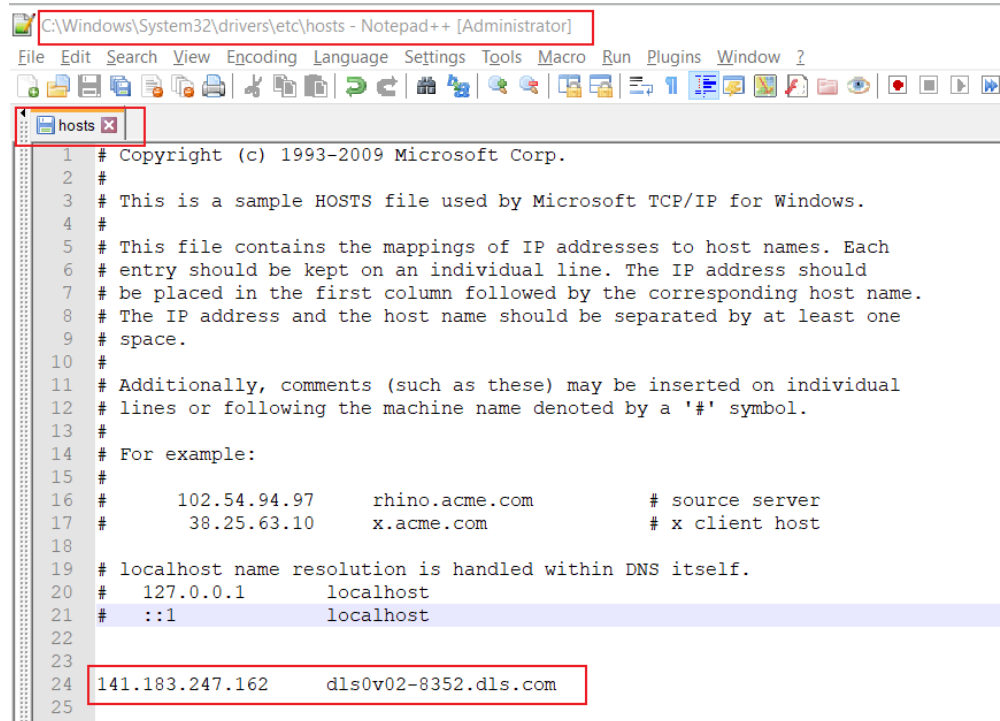
30 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

10 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

*** System restart required ***
Last login: Tue Jun 13 10:13:10 +08 2023 on tty1
-bash: export: `027': not a valid identifier
admin01@disov02-8352:~$ hostname
disov02-8352
admin01@disov02-8352:~$ hostname -I
141.183.247.162
admin01@disov02-8352:~$
```

- 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).

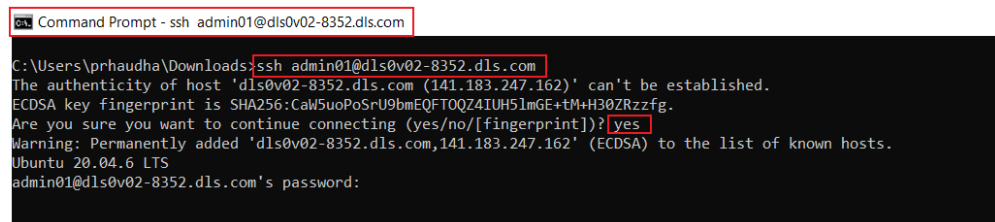


```
C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts x
1 # Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #       102.54.94.97       rhino.acme.com           # source server
17 #       38.25.63.10       x.acme.com               # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 #   127.0.0.1       localhost
21 #   ::1             localhost
22
23
24 141.183.247.162       dls0v02-8352.dls.com
25
```

- 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.



```
Command Prompt - ssh admin01@dls0v02-8352.dls.com
C:\Users\praudha\Downloads>ssh admin01@dls0v02-8352.dls.com
The authenticity of host 'dls0v02-8352.dls.com (141.183.247.162)' can't be established.
ECDSA key fingerprint is SHA256:CaW5uoPoSrU9bmEQFTQZ4IUH51mGE+tM+H30ZRzzfg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'dls0v02-8352.dls.com,141.183.247.162' (ECDSA) to the list of known hosts.
Ubuntu 20.04.6 LTS
admin01@dls0v02-8352.dls.com's password:
```

- 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.

```

admin01@dls0v02-8352: ~
#####

### Script started: Thu 04 May 2023 03:41:12 AM UTC ###

VM hostname: dls0v02-8352

vm_ip: 141.183.247.162
env_ip: 141.183.246.177
vm_host_id: d61d8796a7a6
lic_host_id: fa1ee13c25b6

VM IP and .env file IP address are not equal
VM MAC id and license host-id are not equal

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

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

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

## IP address got changed...
containers are not running well, need to stop them first.
no container is running at the moment
first, correct IP address in /home/elab/.env file and /etc/hosts file
hostname:dls0v02-8352 found in /etc/hosts, remove it..
Now, add new valid IP address vs hostname mapping..
Also, remove Invalid IP address from .env file...
Now, add valid IP address into .env file...
Now, change valid IP address into /home/elab/SetEnvironmentVar.sh file...
Also, change IP address in /home/elab/hosts file
Also, change valid IP address into open-tap.service at /etc/systemd/system/open-tap.service file...
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 not compatible with VM MAC address
Ensure license server is down
License server is still running, need to make it down
Also, remove license file if they exist

WARNING: Please provide compatible license files under /home/elab/licensing

### Script ended: Thu 04 May 2023 03:45:07 AM UTC ###

admin01@dls0v02-8352:~$

```

- 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.

```

admin01@dls0v02-8352:~$ sudo docker ps -a
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS                               NAMES
36d75f671a16   frontend:latest                    "/docker-entrypoint..." 8 hours ago    Up 8 hours (healthy)   141.183.247.162:80->80/tcp, 141.183.247.162:443->443/tcp, 141.183.247.162:443->443/tcp, 141.183.247.162:8080->8080/tcp, 141.183.247.162:30000->30000/tcp   frontend_c
bb0e552a6f     backend:latest                     "/usr/bin/supervisor..." 8 hours ago    Up 8 hours (healthy)   22/tcp, 80/tcp, 443/tcp            backend_c
8db9a1e94bf    quay.io/keycloak/keycloak:12.0.4   "/opt/jboss/tools/de..." 8 hours ago    Up 8 hours (healthy)   8080/tcp, 8443/tcp                keycloak_c
17e1e4778921   guacamole/guacamole:latest        "/opt/guacamole/bin/..." 8 hours ago    Up 8 hours            8080/tcp                          guacamole
edaaf11b1af    meshcentral:latest                "sh docker-entrypoint..." 8 hours ago    Up 8 hours (unhealthy)  22/tcp, 80/tcp, 443/tcp, 8080/tcp, 8443/tcp, 9001/tcp, 141.183.247.162:31443->31443/tcp   meshcentral_c
ac9a1d43fc2    editorx:latest                    "/docker-entrypoint..." 8 hours ago    Up 8 hours            141.183.247.162:8080->8080/tcp, 80/tcp, 141.183.247.162:15301->15301/tcp   editorx_c
757b0bfc2de    mongo:4.0.3                       "docker-entrypoint.s..." 8 hours ago    Up 8 hours (healthy)   172.17.0.1:27018->27017/tcp        mongodb_c
d1ef1501511b   postgres:12-alpine               "docker-entrypoint.s..." 8 hours ago    Up 8 hours (healthy)   5432/tcp                          pgkeycloak_c
2a609a4e3842   guacamole/guacd:1.4.0             "/bin/sh -c './usr/lo..." 8 hours ago    Up 8 hours (healthy)   4222/tcp                          guacd
c1091a6f3384   mariadb/server:latest             "docker-entrypoint.s..." 8 hours ago    Up 8 hours            3306/tcp                          guacdb

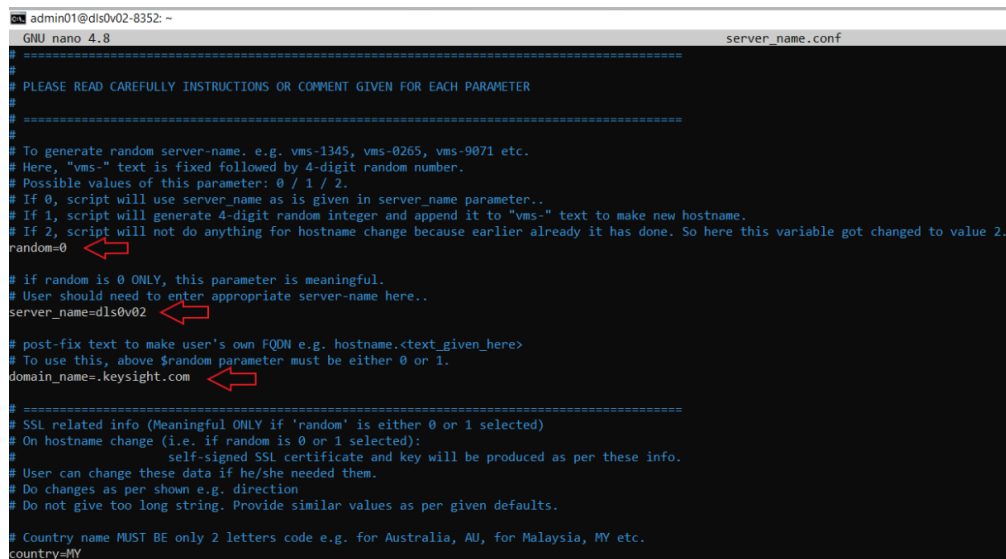
```

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.



```
admin01@dls0v02-8352: ~
GNU nano 4.8 server_name.conf
#
# PLEASE READ CAREFULLY INSTRUCTIONS OR COMMENT GIVEN FOR EACH PARAMETER
#
# =====
# To generate random server-name. e.g. vms-1345, vms-0265, vms-9071 etc.
# Here, "vms-" text is fixed followed by 4-digit random number.
# Possible values of this parameter: 0 / 1 / 2.
# If 0, script will use server_name as is given in server_name parameter..
# If 1, script will generate 4-digit random integer and append it to "vms-" text to make new hostname.
# If 2, script will not do anything for hostname change because earlier already it has done. So here this variable got changed to value 2.
random=0
# if random is 0 ONLY, this parameter is meaningful.
# User should need to enter appropriate server-name here..
server_name=dls0v02
# post-fix text to make user's own FQDN e.g. hostname.<text_given_here>
# To use this, above $random parameter must be either 0 or 1.
domain_name=keysight.com
# =====
# SSL related info (Meaningful ONLY if 'random' is either 0 or 1 selected)
# On hostname change (i.e. if random is 0 or 1 selected):
#     self-signed SSL certificate and key will be produced as per these info.
# User can change these data if he/she needed them.
# Do changes as per shown e.g. direction
# Do not give too long string. Provide similar values as per given defaults.
# Country name MUST BE only 2 letters code e.g. for Australia, AU, for Malaysia, MY etc.
country=MY
```

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

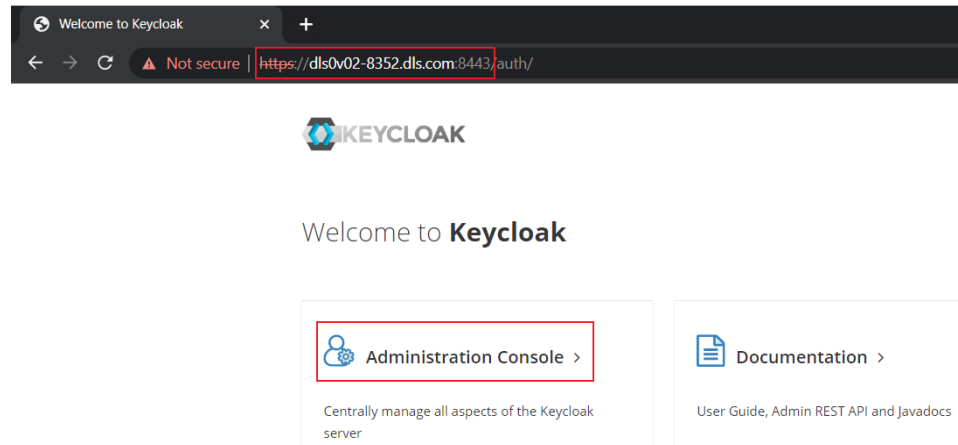
Contact IT support to make it direct accessible.

Step 7: Set Up Keycloak

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

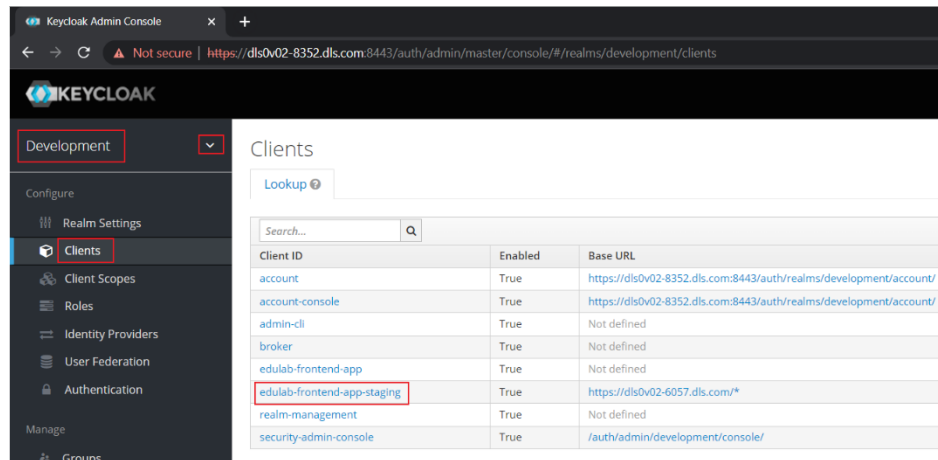
NOTE

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.

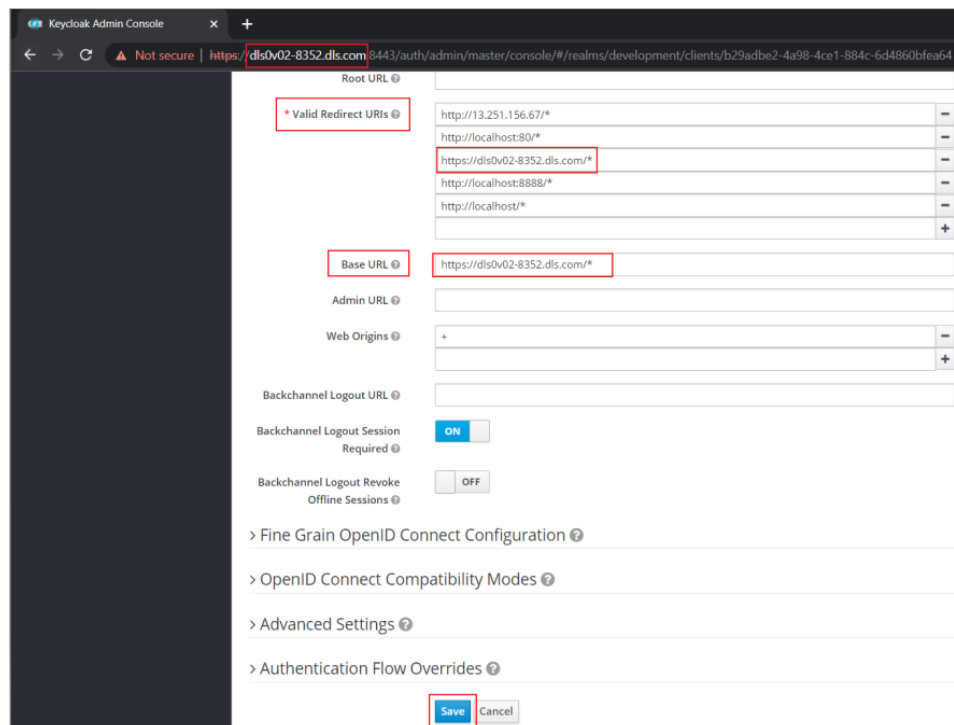


- 2 Log in as follows:
 - Username: **admin**
 - Password: **adm1n!1234**

- 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>.



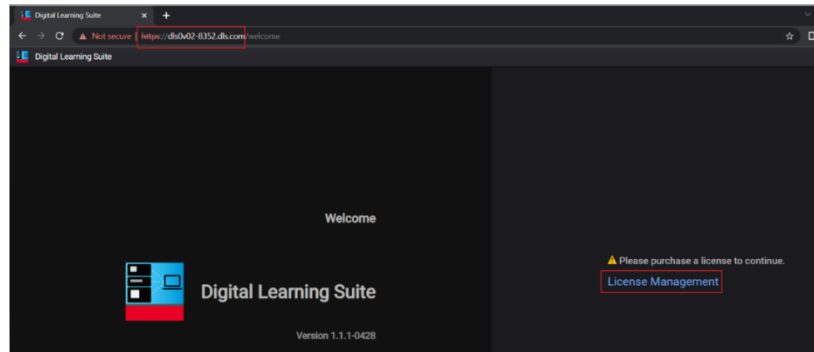
- 5 Click **Save**.

Step 8: Install License Files

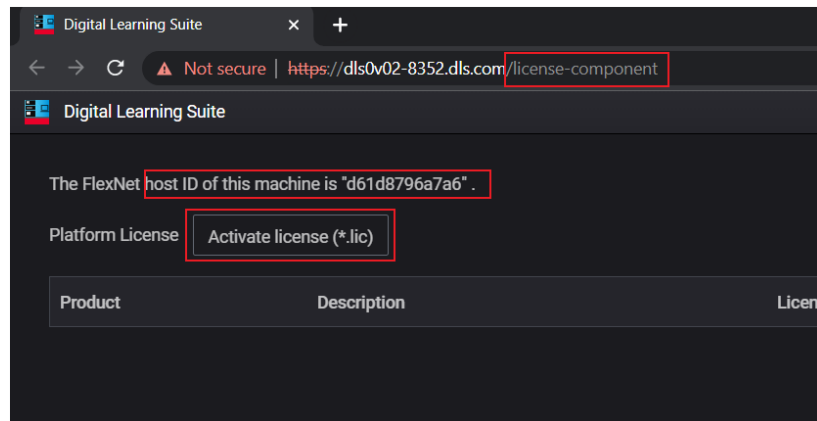
- 1 By this point you should be able to access the DLS application welcome page. Enter your <server url> into the browser and you will see a licence request on the right pane. Click on **License Management**.

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.



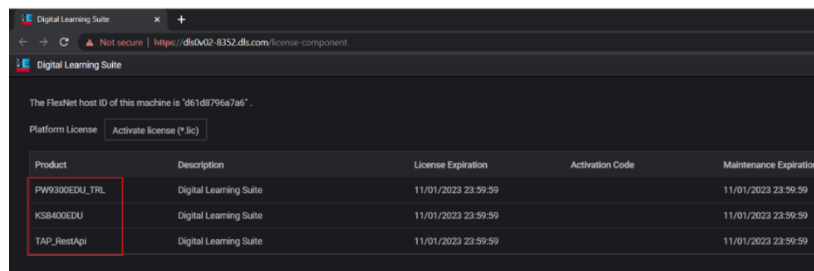
- 2 You will see the **host ID** of your machine here. Click on **Activate license (*.lic)** to upload your license files one at a time.



NOTE

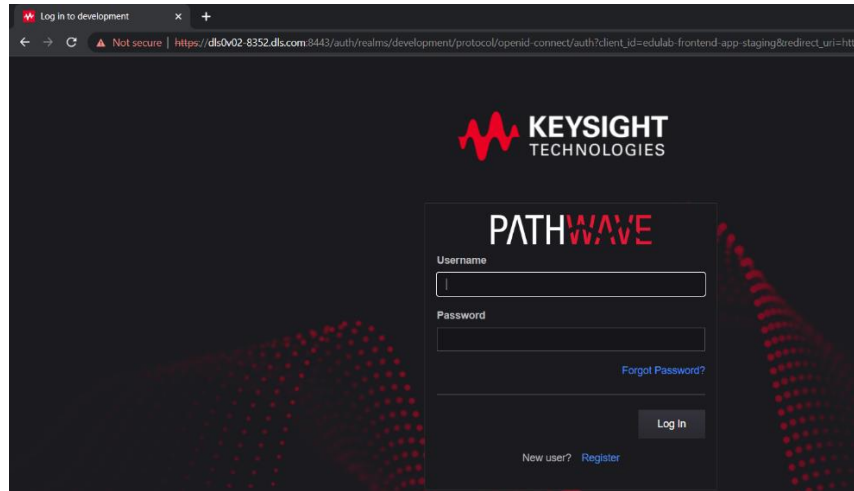
If you have not downloaded/retrieved your **host ID**-based license files, see [Software License](#) for the steps.

- 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

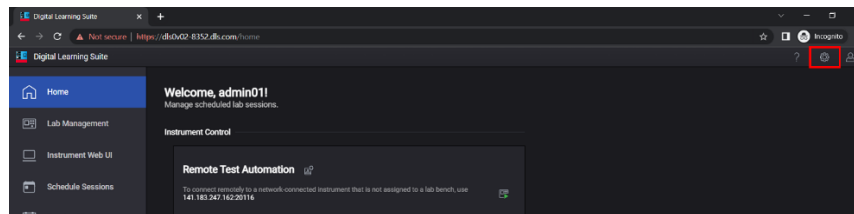
- 1 Enter the <server url> into the browser to go to the DLS login page.



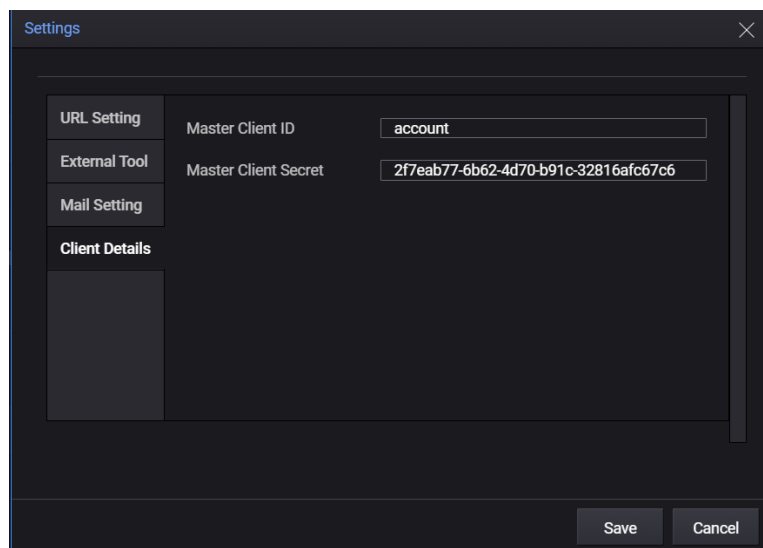
You can register as a **new user** or sign into the default account with the following:

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

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

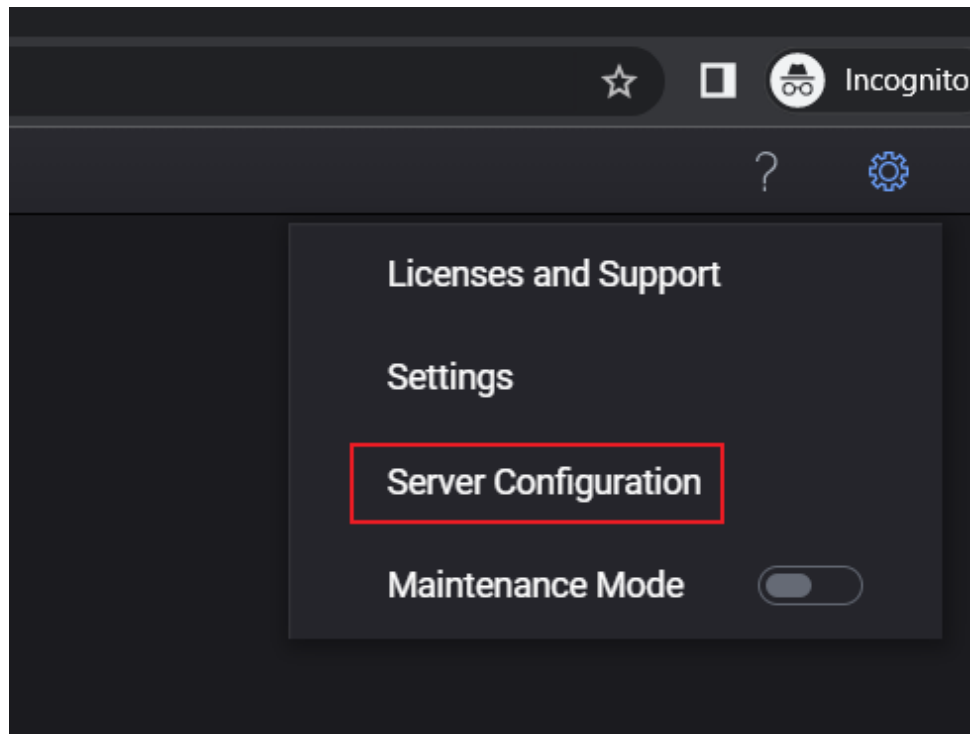


- 3 At **Settings**, go to **Client Details**. The fields for **Master Client ID** and **Master Client Secret** are auto generated. See *Client Details* for instructions on how to update the **Master Client Secret** field for DLS if the field information here does not match the one in Keycloak.

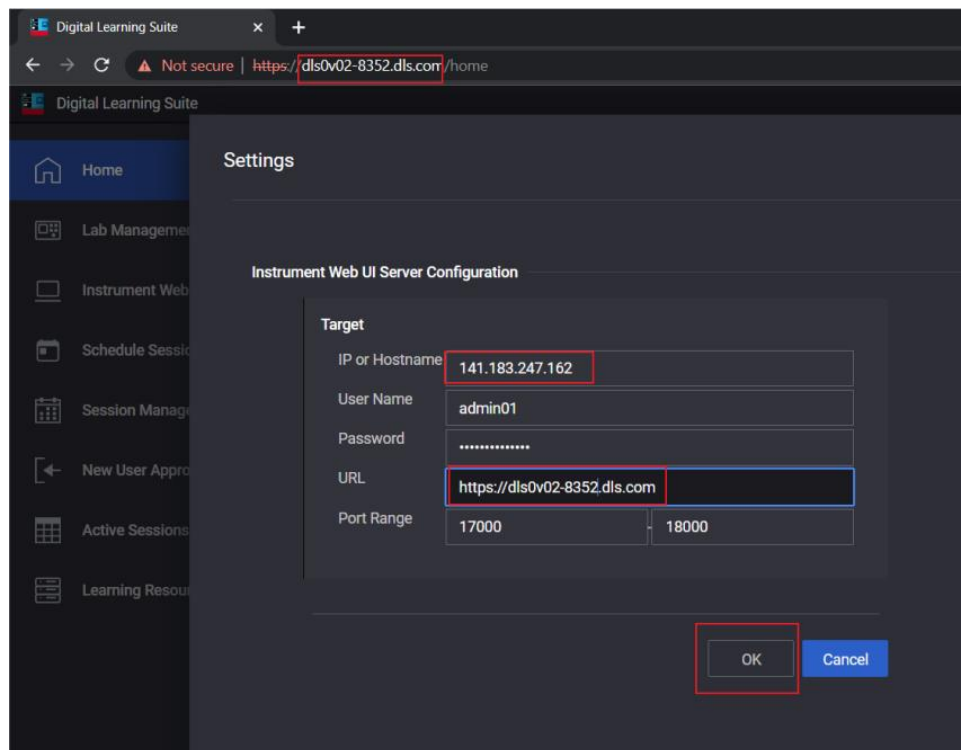


Step 10: Set Up Server Configurations

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



- 2 Enter your IP address and URL and click **OK** to complete the setup.



(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.

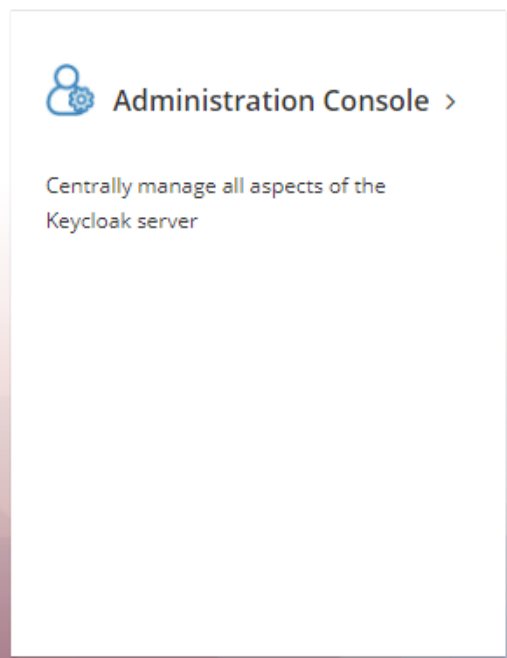
Keycloak Settings

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 the 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**

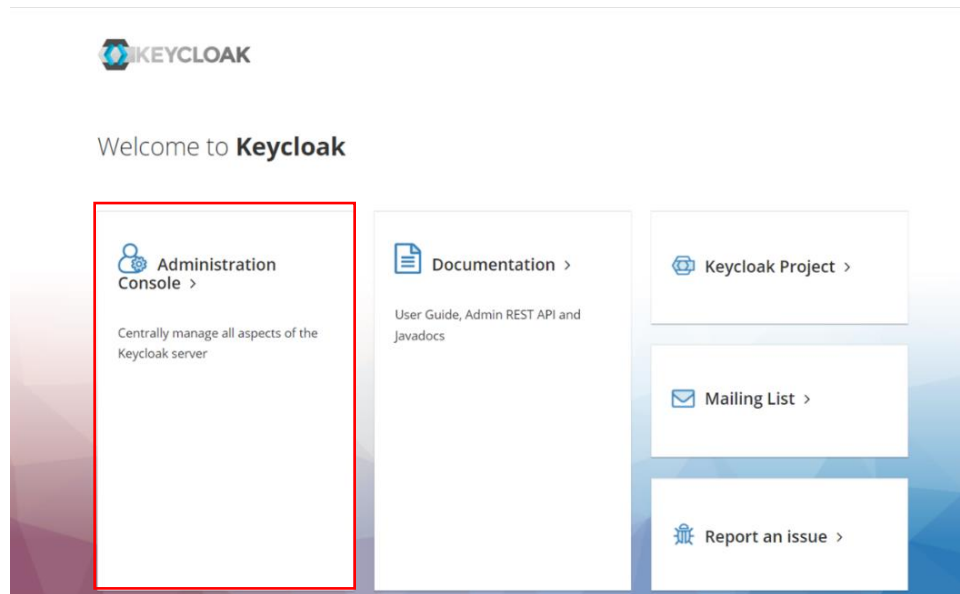
NOTE

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 Keycloak 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.

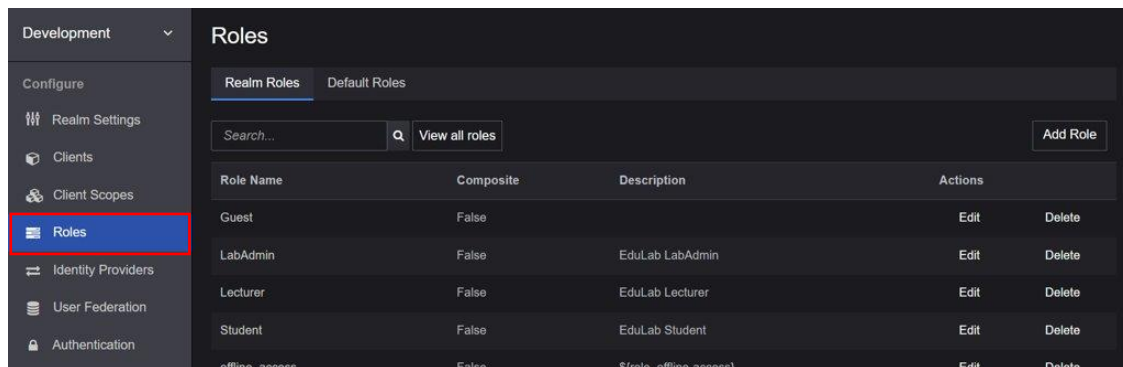
- **Enable Email Settings**
Perform the steps in this section to turn on the **Forgot Password** feature.
- **Set Up Single Sign-On (SSO)**
This is an optional step to set up the social sign in for your application.

Configuration and Settings

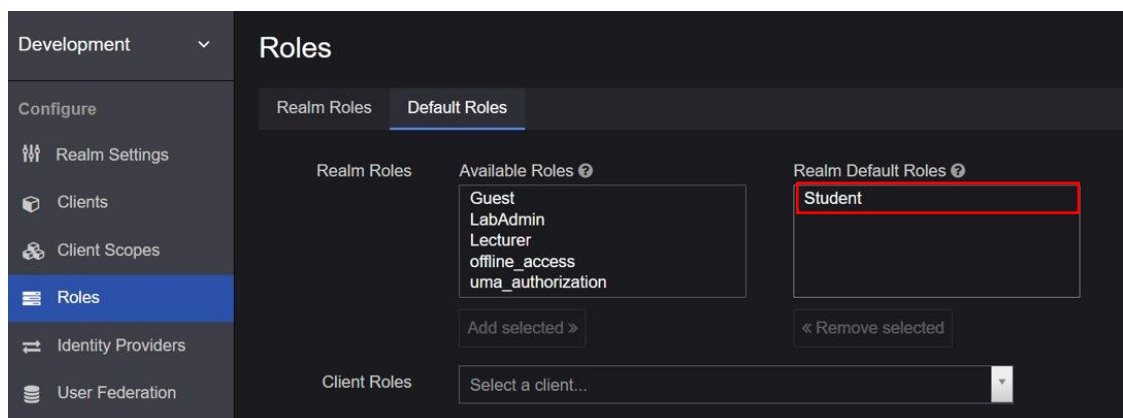
Configure Roles

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.



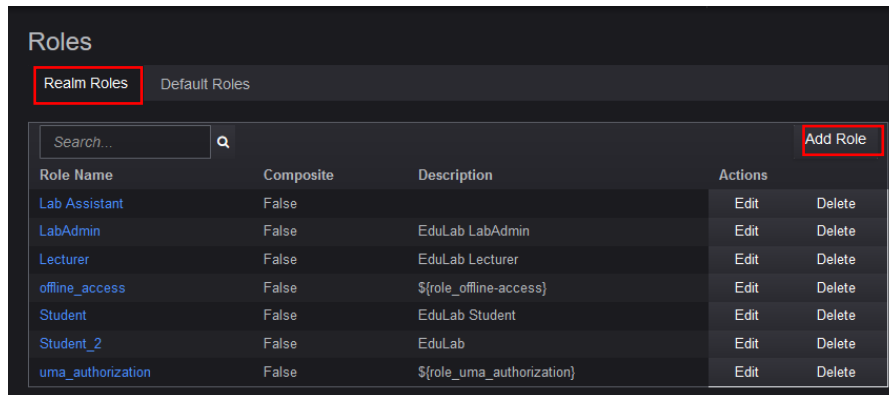
- 2 Go to the **Default Roles** tab to view or modify the default roles assigned to new accounts. By default, new accounts are assigned with **Guest** role during registration.



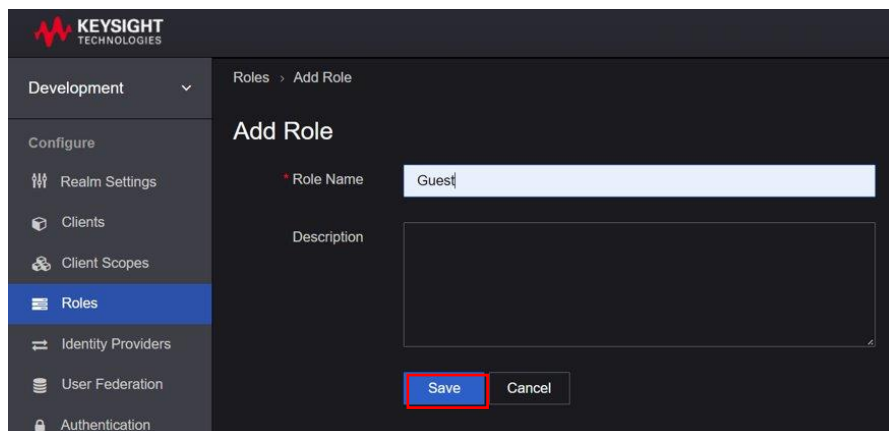
NOTE

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.

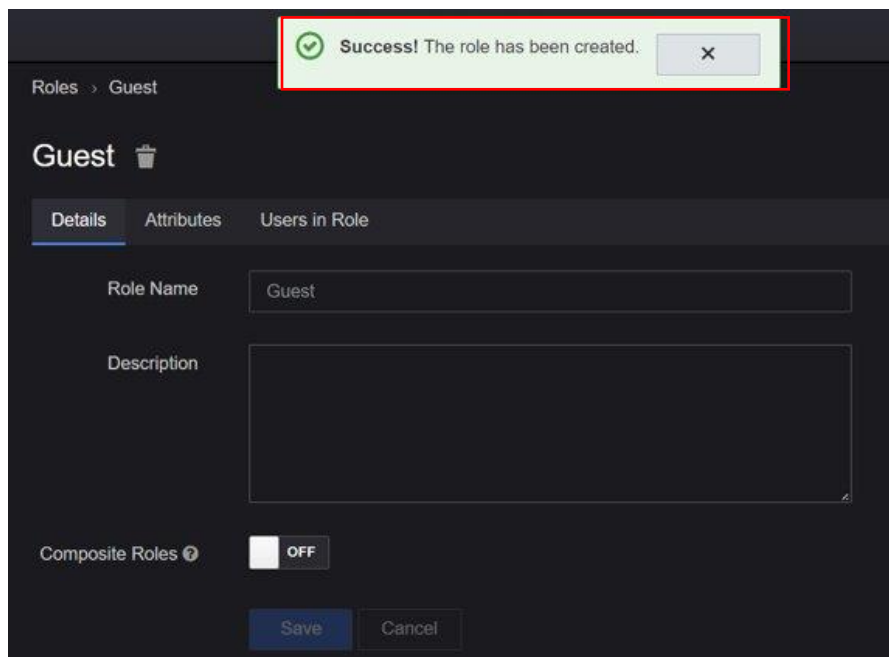
- 3 To add a new role, return to **Realm Roles** tab and click the **Add Role** button.



- 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.

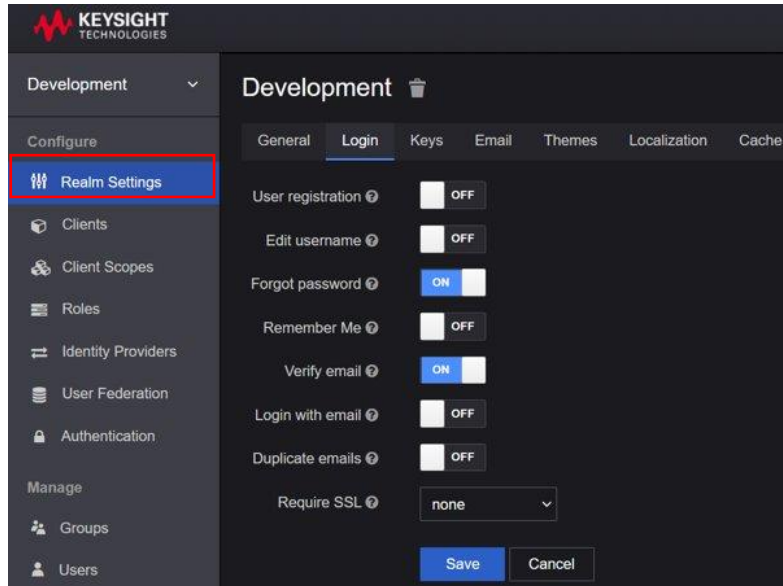


Add User

NOTE

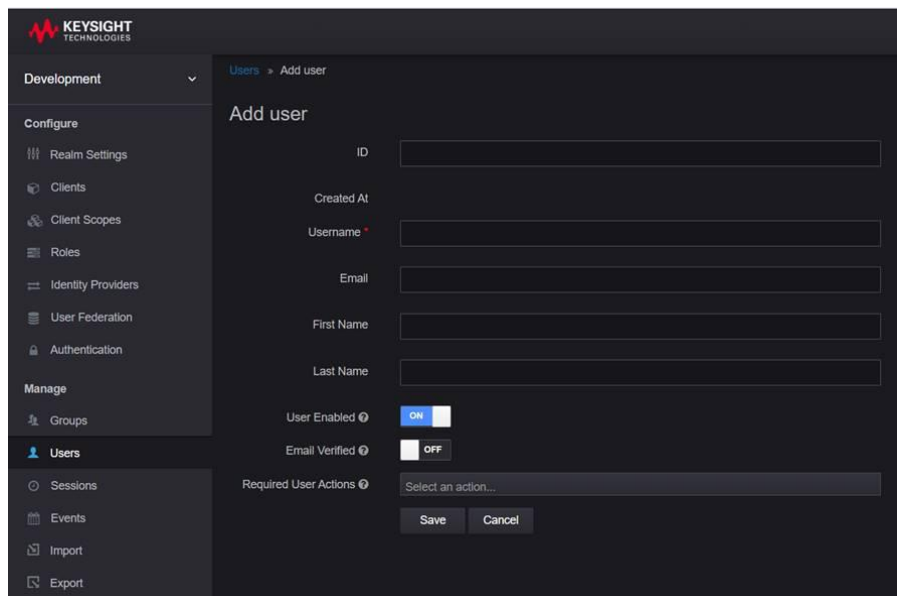
By default, the **User registration** setting is set as **OFF**. This is the recommended setting to prevent other users from registering an account using the link to the application.

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:

The screenshot shows the Keysight Technologies user management interface. On the left is a sidebar with a 'Development' dropdown and a 'Configure' section containing links for Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, and Authentication. Below this is a 'Manage' section with links for Groups and Users. The 'Users' link is selected. The main content area shows the 'Users > ain' path. Under the user name 'Ain' is a trash icon and a tabbed interface with 'Details', 'Attributes', 'Credentials' (selected), 'Role Mappings', 'Groups', 'Consents', and 'Sessions'. The 'Manage Credentials' section has a table with columns 'Position', 'Type', and 'User Label'. The 'Type' column has a dropdown menu with 'password' selected. Below this is a 'Reset Password' section with two password input fields labeled 'Password' and 'Password Confirmation', each with a toggle icon. At the bottom, there is a 'Temporary' checkbox which is currently checked and labeled 'ON'.

- a In the Manage Password section, enter the desired password as shown above.
- b Enable the **Temporary** option to create a temporary password.

NOTE

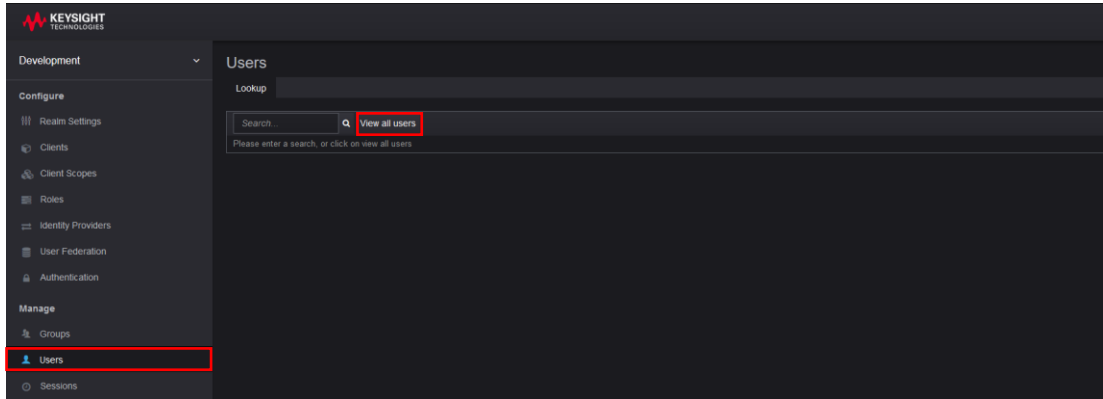
When the **Temporary** option is enabled, users are required to change the password when they first log in to the application. You may turn off the **Temporary** option if you prefer to create a permanent password for the user.

- 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**.

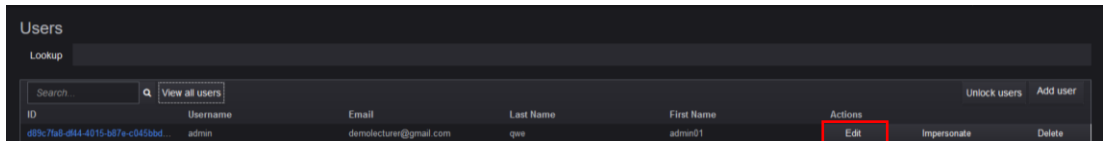
Manage User

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

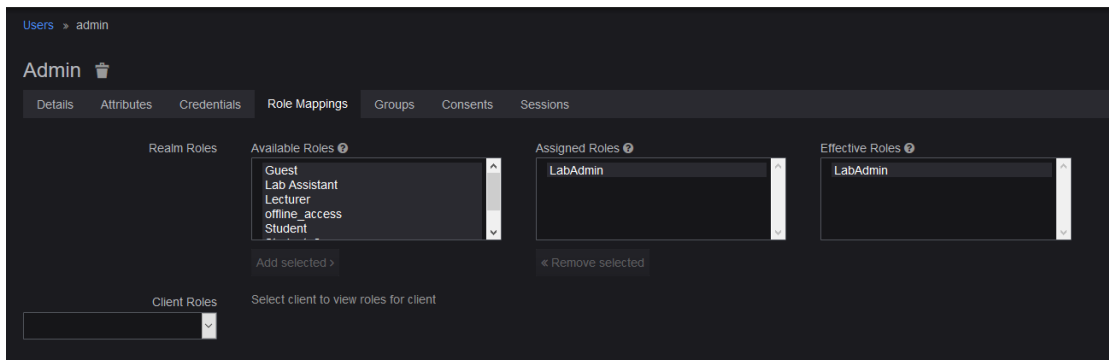
- 1 To modify the assigned roles for an account, go to **Manage > Users** and click **View all users**.



- 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.

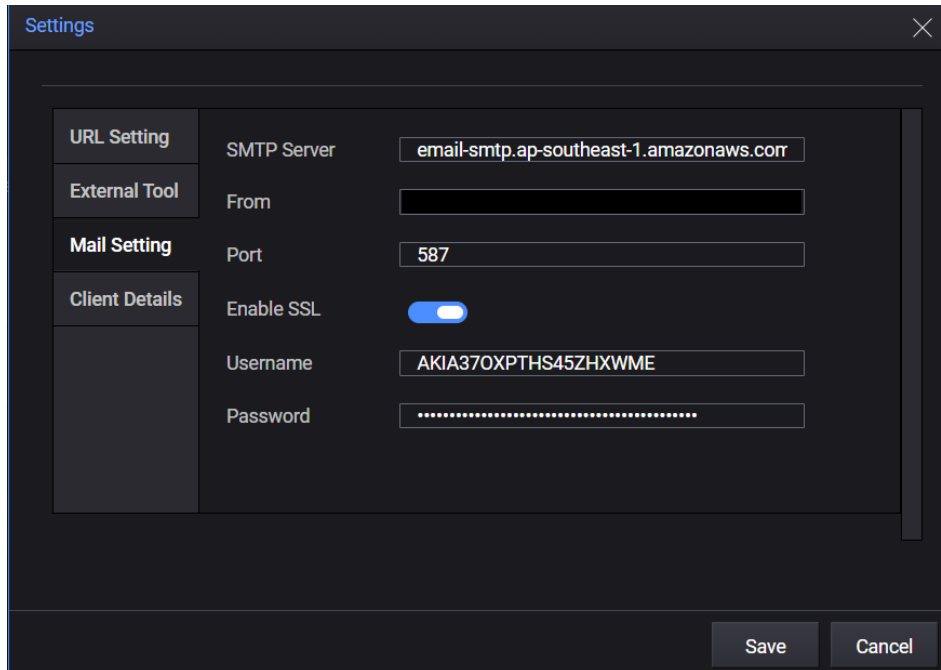
Keycloak's documentation: https://www.keycloak.org/docs/latest/server_admin/

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

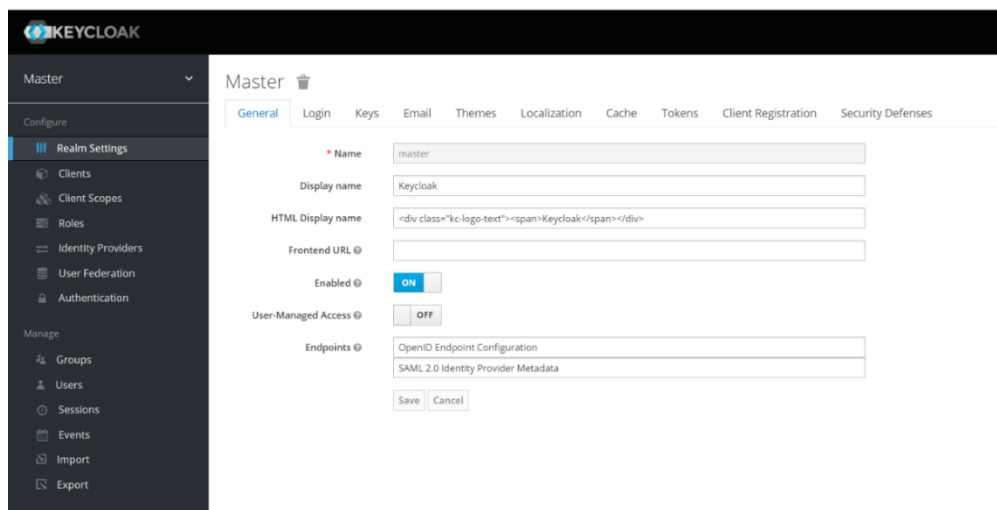
Enter the information regarding your server.



Category	Field	Value
URL Setting	SMTP Server	email-smtp.ap-southeast-1.amazonaws.com
External Tool	From	
Mail Setting	Port	587
Client Details	Enable SSL	<input checked="" type="checkbox"/>
	Username	AKIA37OXP...
	Password

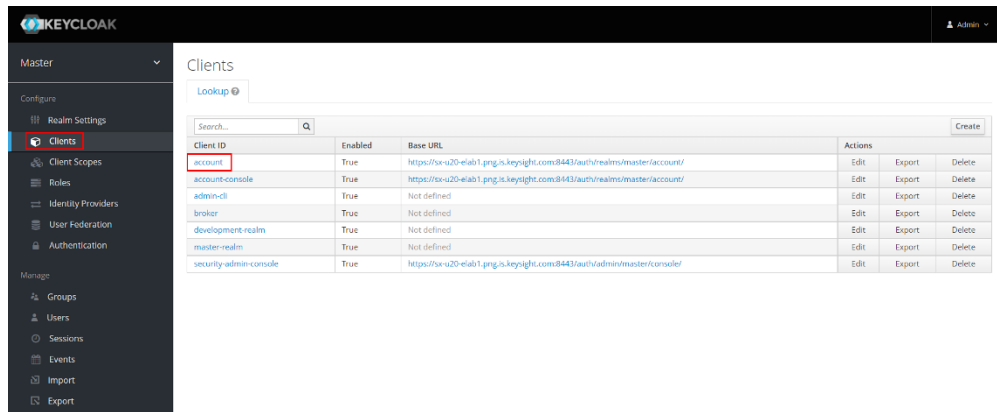
Client Details

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

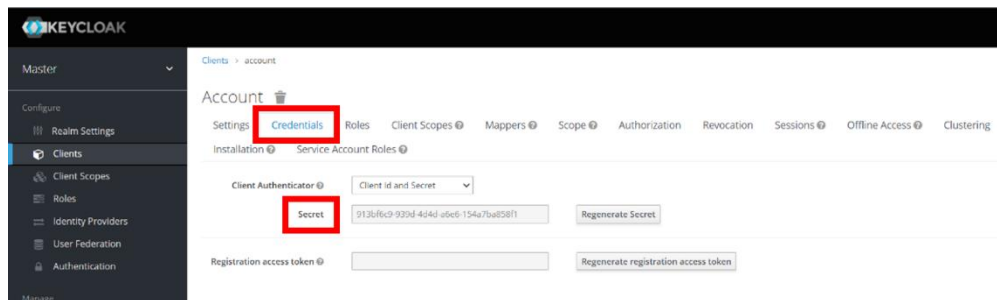


Field	Value
Name	master
Display name	Keycloak
HTML Display name	<div class="kc-logo-text">Keycloak</div>
Frontend URL	
Enabled	ON
User-Managed Access	OFF
Endpoints	OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata

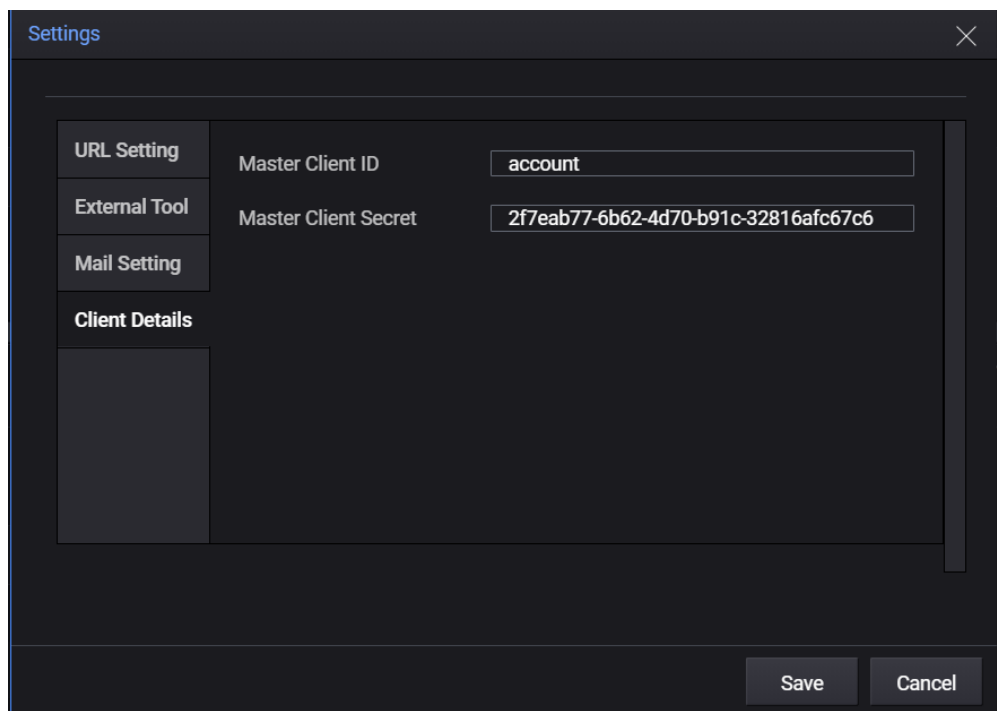
- 2 In the Clients tab, select **account**.



- 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**.



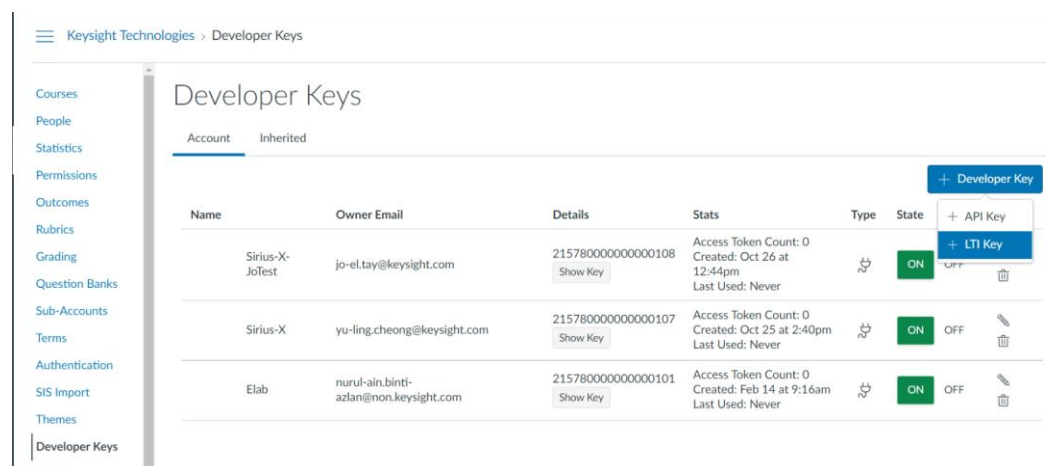
(Optional) Learning Tools Interoperability (LTI) Features

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)

Key Settings

Key Name:
DLS

Owner Email:
yu-ling.cheong@keysight.com

* Redirect URIs:
https://testscript.realmotolab.keysight.com:30080/lti/tool

Notes:

Configure

Method
Manual Entry

Required Values

* Title
Digital Learning Suite

* Description
Digital Learning Suite

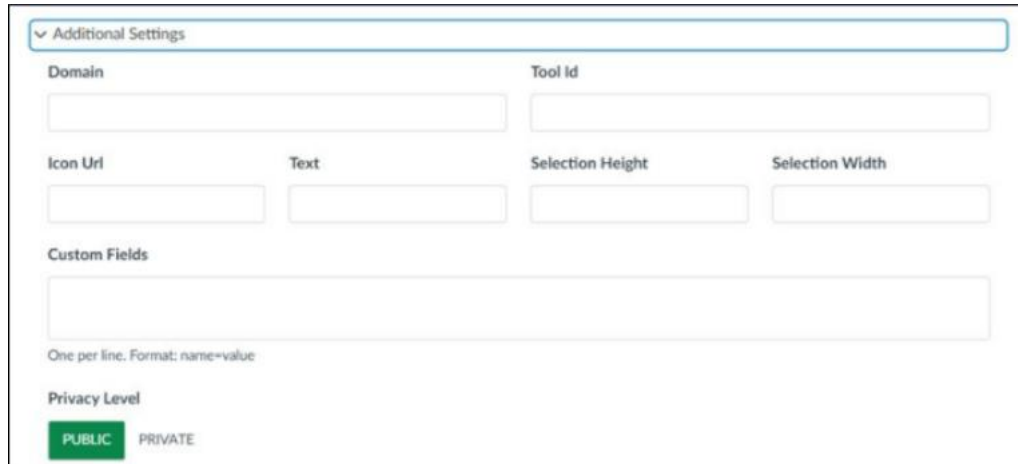
* Target Link URI
https://testscript.realmotolab.keysight.com:30080/lti/tool

* OpenID Connect Initiation Url
https://testscript.realmotolab.keysight.com:30080/lti/launch

* JWK Method
Public JWK URL

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**.

Developer Keys

Account		Inherited					
Name	Owner Email	Details	Stats	Type	State	Actions	
Sirius-X-JoTest	jo-el.tay@keysight.com	21578000000000108 Show Key	Access Token Count: 0 Created: Oct 26 at 12:44pm Last Used: Never	~\$	ON OFF	Edit this key	
Sirius-X	yu-ling.cheong@keysight.com	21578000000000107 Show Key	Access Token Count: 0 Created: Oct 25 at 2:40pm Last Used: Never	~\$	ON OFF	Edit this key	
Elab	nurul-ain.binti-azlan@non.keysight.com	21578000000000101 Show Key	Access Token Count: 0 Created: Feb 14 at 9:16am Last Used: Never	~\$	ON OFF	Edit this key	

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**

Settings

URL Setting

External Tool

Mail Setting

Client Details

SSL Certificates

Tool name

Issuer

Client ID

Access Token URL

Authorize URL

JWK URL

Deployment ID

ELAB DEVELOPER TOOLS

https://canvas.instructure.com

21578000000000107

https://keysighttechnologies.instructure.com

https://keysighttechnologies.instructure.com

https://keysighttechnologies.instructure.com

116:b2e4ee1593aab580aaaf5fec50d958fa3

Save

Cancel

Create the Deep Linking App in Canvas

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

Account

Admin

Dashboard

Courses

Calendar

Inbox

History

Help

Digital Learning Suite > Settings

Home

Announcements

Assignments

Discussions

Grades

People

Pages

Files

Syllabus

Outcomes

Rubrics

Quizzes

Modules

BigBlueButton

Collaborations

Course Details

Sections

Navigation

Apps

Feature Options

Integrations

Image:

Choose Image

Name:

Digital Learning Suite

Course Code:

Digital Learning Suite

Blueprint Course:

☐ Enable course as a Blueprint Course

Course Template:

☐ Enable course as a Course Template

Time Zone:

Mountain Time (US & Canada) (-07:00/-06:00)

SIS ID:

Keysight SR101EDUA Digital Learning Suite Installation Guide

43

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

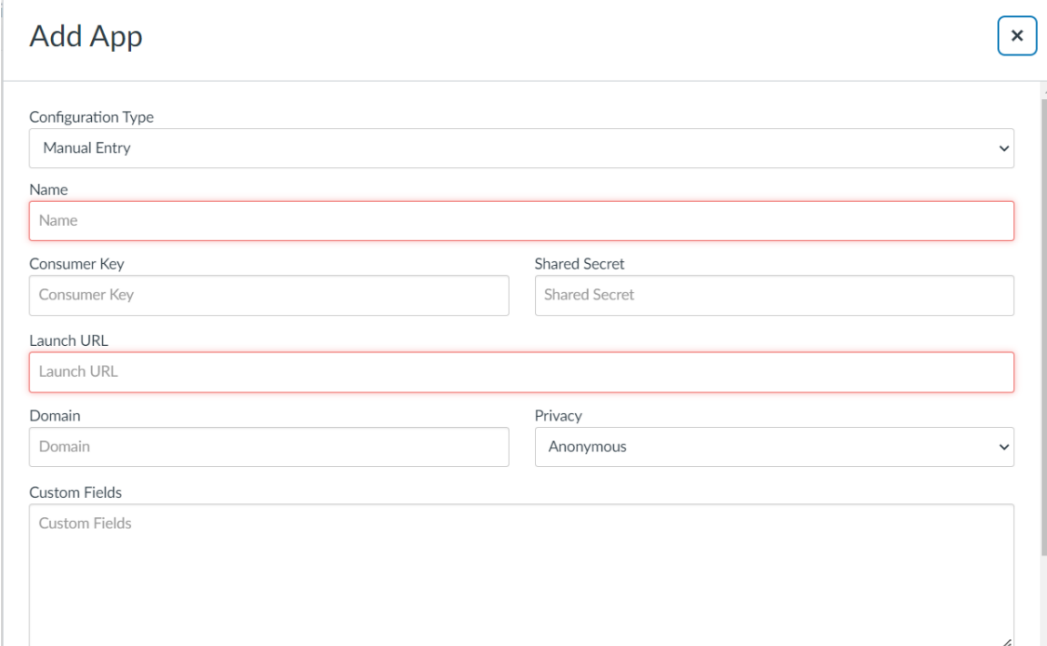
The screenshot shows the 'Digital Learning Suite > Settings' page. On the left is a dark sidebar with navigation icons for Account, Admin, Dashboard, Courses, Calendar, Inbox, History, and Help. The main content area has a top navigation bar with tabs: Home, Course Details, Sections, Navigation, Apps (selected), Feature Options, and Integrations. Below the tabs, the 'External Apps' section is displayed. It includes a 'View App Configurations' button, a description of apps, a link to 'See some LTI tools that work great with Canvas', and a filter bar with 'All', 'Not Installed', and 'Installed' options. A grid of six app tiles is shown: AcadSource, Accepi, ACCESS VIDEO ON DEMAND, acclaim, Accommodate HQ, and Accredible Certificates & Badges.

- 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**.

This screenshot is identical to the one above, showing the 'Digital Learning Suite > Settings' page with the 'Apps' tab selected. It displays the 'External Apps' section with the same navigation elements, description, filter bar, and grid of app tiles (AcadSource, Accepi, ACCESS VIDEO ON DEMAND, acclaim, Accommodate HQ, and Accredible Certificates & Badges).

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



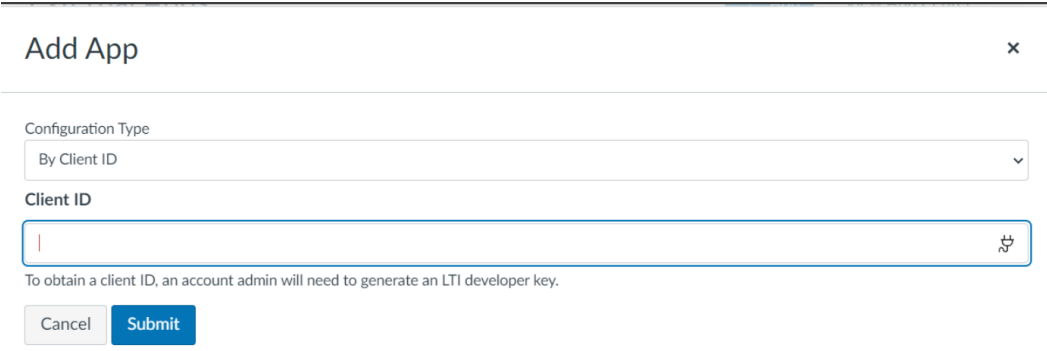
The screenshot shows the 'Add App' window with the following fields highlighted with red borders:

- Name**: A text input field with the placeholder text 'Name'.
- Launch URL**: A text input field with the placeholder text 'Launch URL'.

Other visible fields include:

- Configuration Type**: A dropdown menu currently set to 'Manual Entry'.
- Consumer Key**: A text input field with the placeholder text 'Consumer Key'.
- Shared Secret**: A text input field with the placeholder text 'Shared Secret'.
- Domain**: A text input field with the placeholder text 'Domain'.
- Privacy**: A dropdown menu currently set to 'Anonymous'.
- Custom Fields**: A large text area with the placeholder text 'Custom Fields'.

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

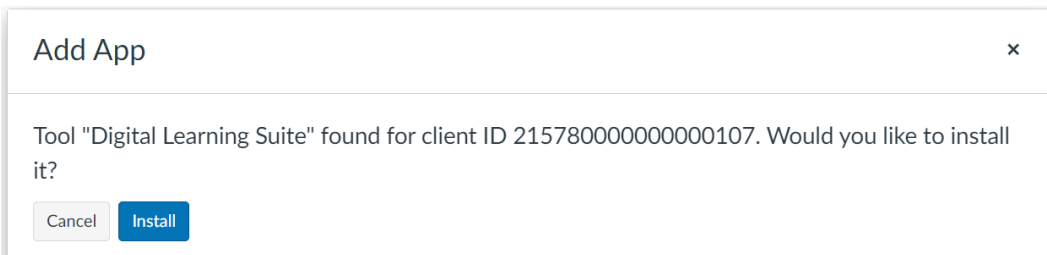


The screenshot shows the 'Add App' window with the following changes:

- Configuration Type**: The dropdown menu is now set to 'By Client ID'.
- Client ID**: A new text input field is present, currently empty.

Below the Client ID field, there is a note: "To obtain a client ID, an account admin will need to generate an LTI developer key." At the bottom, there are 'Cancel' and 'Submit' buttons.

- 6 Click **Install**.



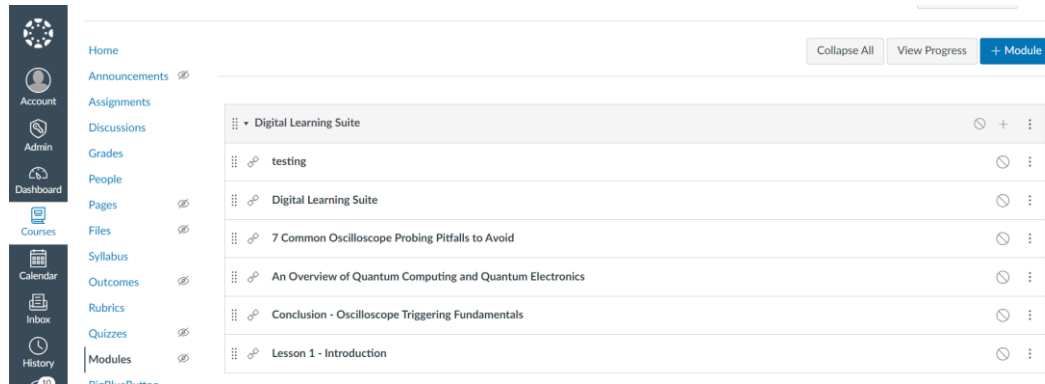
The screenshot shows the 'Add App' window with the following message:

Tool "Digital Learning Suite" found for client ID 215780000000000107. Would you like to install it?

At the bottom, there are 'Cancel' and 'Install' buttons.

Import Your Course Content

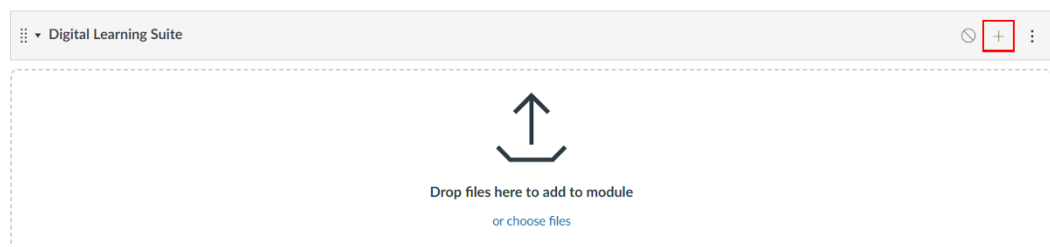
- 1 Click on the **Courses** panel and navigate to **Modules**.
- 2 On the **Modules** page, click **+ Module** to add a new module to the course.



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

A screenshot of a 'Add Module' dialog box. The title bar says 'Add Module' with a close button (X) on the right. Inside the dialog, there is a text input field containing 'Digital Learning Suite'. Below the input field is a checkbox labeled 'Lock until'. Underneath that is a section titled 'Prerequisites' with a blue '+ Add prerequisite' link. At the bottom right of the dialog are two buttons: 'Cancel' and '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.

The screenshot shows a dialog box titled "Add Item to Digital Learning Suite". At the top, it says "Add External Tool to Digital Learning Suite". Below this, there is a link icon and text: "Select a tool from the list below, or enter a URL for an external tool you already know is configured with Basic LTI to add a link to it to this module." A list of tools is displayed, each with a blue hyperlink and a magnifying glass icon to its right. The tools are: AppJoTest, Digital Learning Suite, ExternalToolJo, KeyLab_Testscript, New Analytics, Quizzes 2, and testing. Below the list is a "URL:" label and an empty text input field. At the bottom right, there are "Cancel" and "Add Item" buttons.

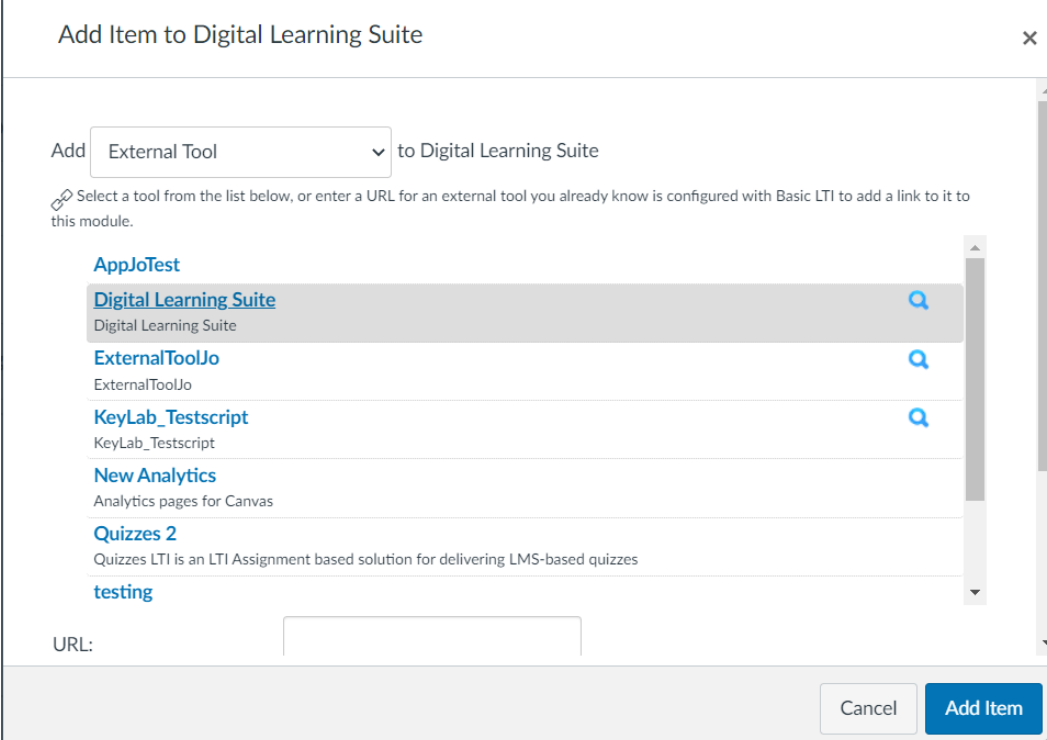
Tool Name	Link
AppJoTest	AppJoTest
Digital Learning Suite	Digital Learning Suite
ExternalToolJo	ExternalToolJo
KeyLab_Testscript	KeyLab_Testscript
New Analytics	New Analytics
Quizzes 2	Quizzes 2
testing	testing

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

The screenshot shows a dialog box titled "Link Resource from External Tool". It contains a "Catalog of Available Contents" section. At the top of this section, there is a "List Type" dropdown menu set to "Lesson", a "All Courses" dropdown menu, a "Filter" button, and an "Add Contents" button. Below this, there is a list of topics, each with a checkbox to its left. The topics are: "7 Common Oscilloscope Probing Pitfalls to Avoid", "An Overview of Quantum Computing and Quantum Electronics", and "Architecting a Real Time Radar Recorder".

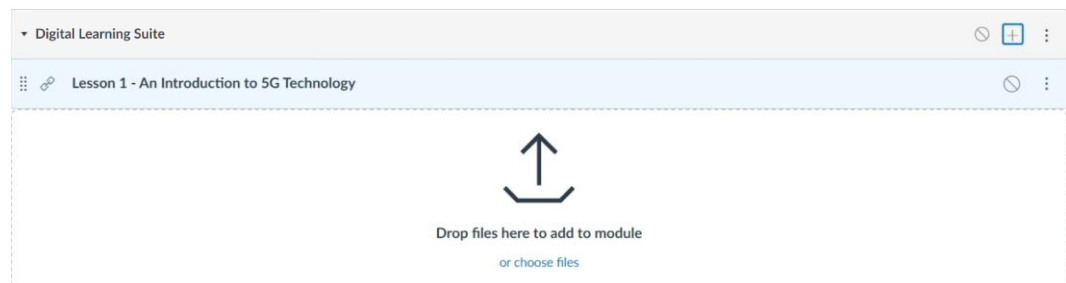
Topic	Selected
7 Common Oscilloscope Probing Pitfalls to Avoid	<input type="checkbox"/>
An Overview of Quantum Computing and Quantum Electronics	<input type="checkbox"/>
Architecting a Real Time Radar Recorder	<input type="checkbox"/>

- 7 Click **Add Item**.



The screenshot shows a dialog box titled "Add Item to Digital Learning Suite" with a close button (X) in the top right corner. Inside the dialog, there is a dropdown menu currently set to "External Tool" with a downward arrow. Below this, a text instruction reads: "Select a tool from the list below, or enter a URL for an external tool you already know is configured with Basic LTI to add a link to it to this module." A list of tools is displayed, each with a magnifying glass icon on the right. The tools are: "AppJoTest", "Digital Learning Suite" (highlighted in grey), "ExternalToolJo", "KeyLab_Testscript", "New Analytics", "Quizzes 2", and "testing". Below the list is a "URL:" label followed by an empty text input field. At the bottom right of the dialog are two buttons: "Cancel" and "Add Item".

- 8 You will see the content added to your module.

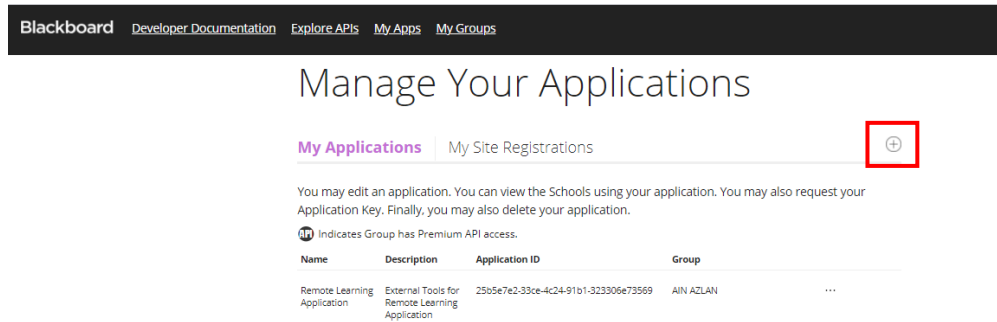


Blackboard

Integrate Digital Learning Suite 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 on +.



- 3 Enter the details below.
 - a Domain: DLS server URL.
 - b Login Initiation URL: <https://<DLS server URL>:30080/lti/launch>
 - c Tool Redirect URI(s): <https://<DLS server URL>:30080/lti/tool>
 - d Tool JWKS URL: <https://<DLS server URL>: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 Digital Learning Suite. This information is auto generated after creating the application.

- 5 Below is an example of a completed form. Click **Update application** when you are done.

Edit application

Enter your applications name and description. Users see this information when adding the application to their environment. Include a version number if there are multiple versions of the application.

* Application Name

Remote Learning Application

* Description

450 character limit

External Tools for Remote Learning Application

* Domain(s)

Separate domains with commas

demo2.realremotelab.keysight.com

Group

AIN AZLAN

My Integration supports LTI 1.3



Login Initiation URL

https://demo2.realremotelab.keysight.com:30080/lti/launch

Tool Redirect URL(s)

Separate URLs with commas

https://demo2.realremotelab.keysight.com:30080/lti/tool

Tool JWKS URL

For a tool's public key access

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

Signing Algorithm

RS256

Custom Parameters

"userName"= "\$User.username"

Issuer

https://blackboard.com

Public keyset URL

https://developer.blackboard.com/api/v1/management/applications/25b5e7e2-33ce-4c24-91b1-323306e73569/jwks.json

Auth token endpoint

https://developer.blackboard.com/api/v1/gateway/oauth2/jwttoken

OIDC auth request endpoint

https://developer.blackboard.com/api/v1/gateway/oidcauth

Cancel


Update application

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

Manage Your Applications

My Applications | My Site Registrations +

You may edit an application. You can view the Schools using your application. You may also request your Application Key. Finally, you may also delete your application.

 Indicates Group has Premium API access.


Name	Description	Application ID	Group
Remote Learning Application	External Tools for Remote Learning Application	25b5e7e2-33ce-4c24-91b1-323306e73569	AIN AZ

[Edit](#)
[Delete](#)
[Manage Keys](#)
[Manage Placements](#)

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

Remote Learning Application Manage Placements

You may edit and delete a placement.

Name	Description	Handle	
Remote Learning Application		a9b795ad-3fab-4fd7-bcfe-6738d21af133	

Done

- 8 Enter the information accordingly.

- a Type: Course Tool
- b Target Link URL: <https://<DLS server URL>:30080/lti/tool>
- c Select the **Launch in new window** check box
- d Click **Register placement**.

* Placement Name

Description Limit placement description to 1000 characters

Type
Course tool

☒ Allow students access

☒ Launch in new window

* Target link URI

Icon URL

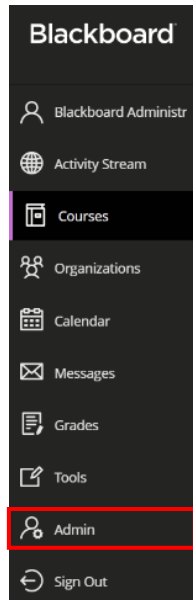
Custom Parameters

Cancel **Update placement**

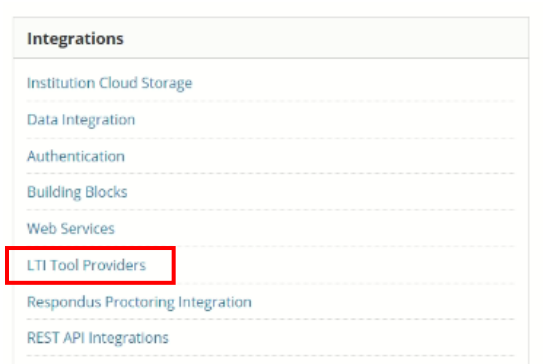
Add External Tools in the Blackboard Platform

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

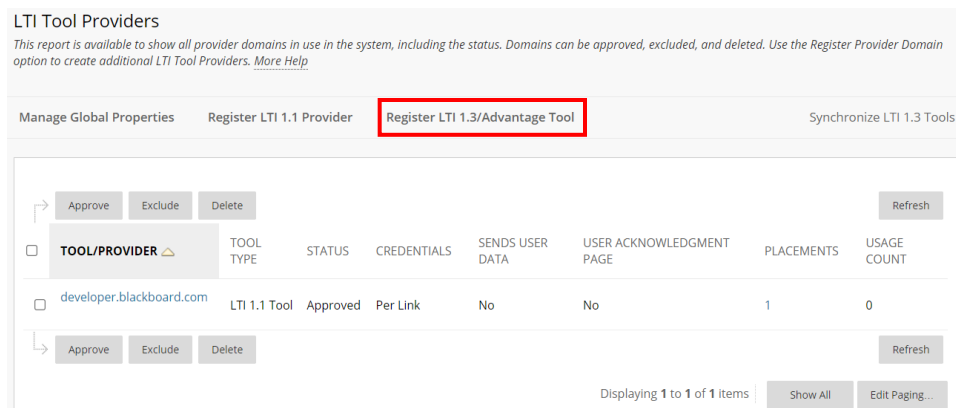
- 1 Go to your Blackboard LMS system and log in with your username and password.
- 2 Click the **Admin** tab.



- 3 Select **LTI Tool Providers**.



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




- [Blackboard](#)
[Developer Documentation](#)
[Explore APIs](#)
[My Apps](#)
[My Groups](#)

Manage Your Applications

[My Applications](#)
[My Site Registrations](#)

You may edit an application. You can view the Schools using your application. You may also request your Application Key. Finally, you may also delete your application.

 Indicates Group has Premium API access.

Name	Description	Application ID	Group
Remote Learning Application	External Tools for Remote Learning Application	25b5e7e2-33ce-4c24-91b1-323306e73569	AIN AZLAN

Should there be 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.

Edit
Manage Placements
Usage Report

Approve
Exclude
Delete

	TOOL TYPE	STATUS	CREDENTIALS	SENDS USER DATA	USER ACKNOWLEDGMENT PAGE	PLACEMENTS	USAGE COUNT
<input type="checkbox"/>	LTI 1.1 Tool	Approved	Per Link	No	No	1	0
<input checked="" type="checkbox"/>	LTI 1.3 Tool	Approved	RS256	Role, Name, Email	No	1	0

Approve Exclude Delete

Displaying 1 to 2 of 2 items | Show All Edit Paging Refresh

6 Review the details and select **Approved** for **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**.

INSTITUTION POLICIES

You can change the following settings for this tool. The fields use global values by default.

User Fields to Send

- ☒ Role in Course
- ☒ Name
- ☒ Email Address

Allow grade service access

- ☒ Yes ☐ No

Allow Membership Service Access

- ☒ Yes ☐ No

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

Manage Global Properties Register LTI 1.1 Provider Register LTI 1.3/Advantage Tool Synchronize LTI 1.3 Tools

<div>→ Approve Exclude Delete</div>									Refresh
<input type="checkbox"/>	TOOL/PROVIDER	TOOL TYPE	STATUS	CREDENTIALS	SENDS USER DATA	USER ACKNOWLEDGMENT PAGE	PLACEMENTS	USAGE COUNT	
<input type="checkbox"/>	developer.blackboard.com	LTI 1.1 Tool	Approved	Per Link	No	No	1	0	
<input checked="" type="checkbox"/>	Remote Learning Application	LTI 1.3 Tool	Approved	RS256	Role, Name, Email	No	1	0	
<div>→ Approve Exclude Delete</div>									Refresh

Displaying 1 to 2 of 2 items Show All Edit Paging...

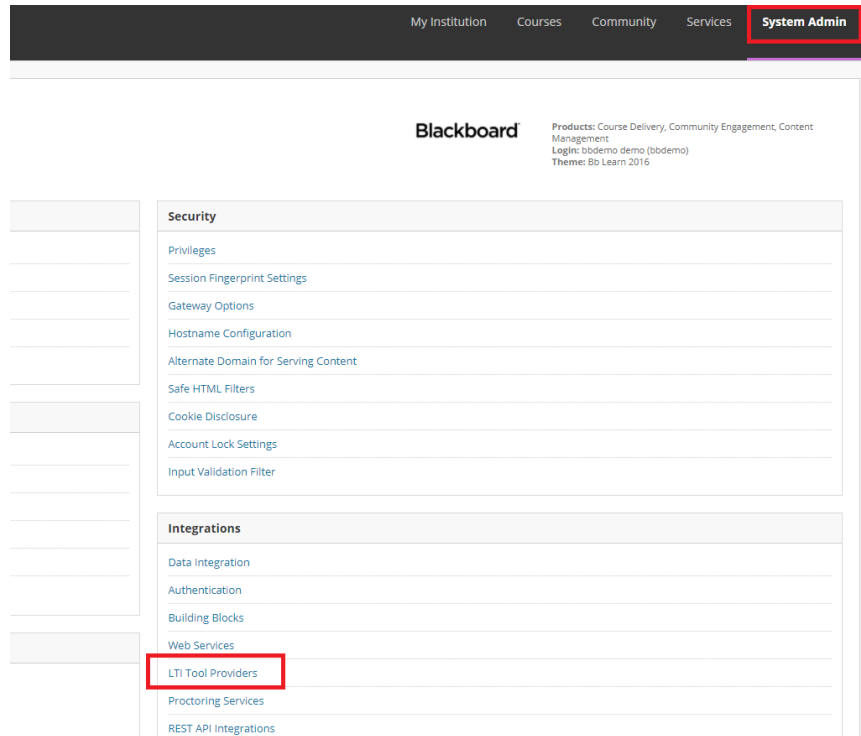
NOTE

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.

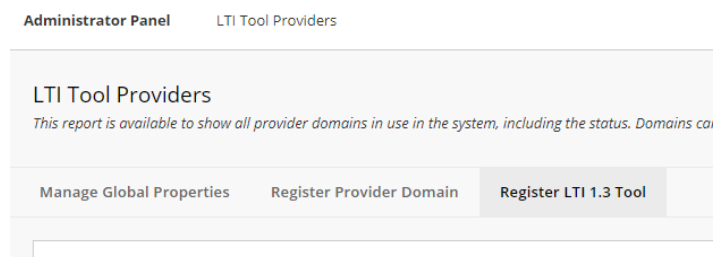
Obtain the Deployment ID

Log in with your account and launch the Digital Learning Suite application.

- 1 Log in to your administrator account on Blackboard.
- 2 Navigate to the **System Admin** tab and click **LTI Tool Providers**.



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



- 4 Enter the Client ID, which is the Application ID created in **Integrate Digital Learning Suite into LTI 1.3 Blackboard**, and 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 Detail to Application

- 1 Go to your Digital Learning Suite 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](#).

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

- 3 The completed form will appear as below.

Issuer

https://blackboard.com

Public keyset URL

https://developer.blackboard.com/api/v1/management/applications/25b5e7e2-33ce-4c24-91b1-323306e73569/jwks.json

Auth token endpoint

https://developer.blackboard.com/api/v1/gateway/oauth2/jwttoken

OIDC auth request endpoint

https://developer.blackboard.com/api/v1/gateway/oidcauth

Launch the Application in Blackboard

Before you launch the Digital Learning Suite 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>).

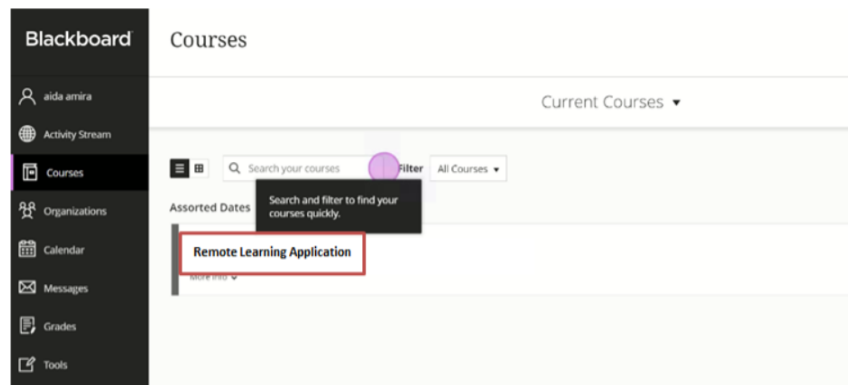
- 1 Log in to launch the course and you should be directed to this page.

Welcome to the new Blackboard!

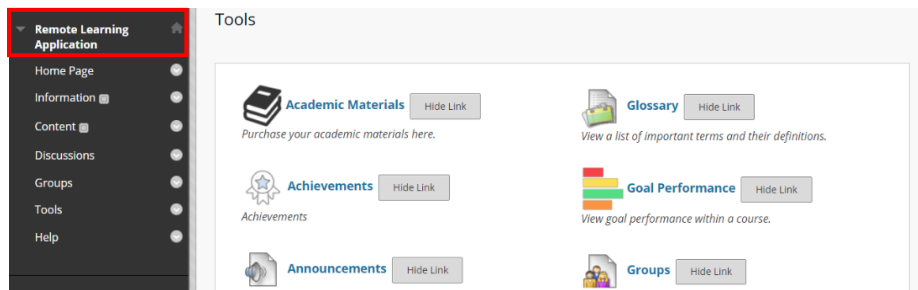


You're going to love the delightful details in our modern design. The intuitive, fluid interactions are simple and fun to use.

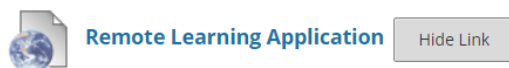
- 2 Select the course.



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



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



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: <http://<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: <http://<DLS server URL>:30080/lti/launch>
 - g Redirection URL(s): <http://<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.

External tool configuration

Expand all

Tool settings

Tool name

Tool URL

Tool description

LTI version

LTI 1.3

Public key type

Keyset URL

Public keyset

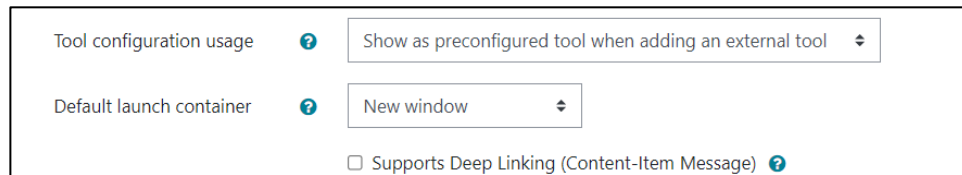
Initiate login URL

Redirection URI(s)

- 4 Set the following:

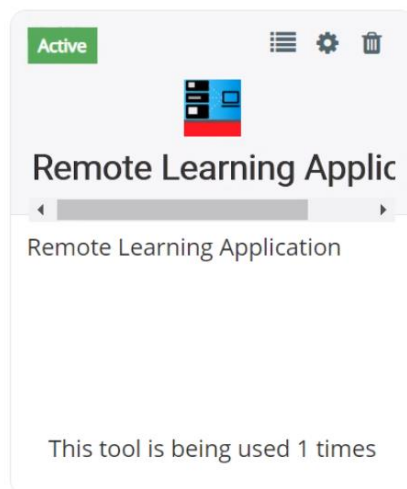
Tool configuration usage: Show as preconfigured tool when adding an external tool

Default launch container: New window



A screenshot of a configuration interface. It contains two rows of settings. The first row is 'Tool configuration usage' with a blue question mark icon and a dropdown menu set to 'Show as preconfigured tool when adding an external tool'. The second row is 'Default launch container' with a blue question mark icon and a dropdown menu set to 'New window'. Below these rows is a checkbox labeled 'Supports Deep Linking (Content-Item Message)' with a blue question mark icon, which is currently unchecked.

- 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.



A screenshot of a 'Tool configuration details' dialog box. It contains a list of configuration details: Platform ID: http://52.74.96.205, Client ID: eNjPvjytlexmft, Deployment ID: 1, Public keyset URL: http://52.74.96.205/mod/lti/certs.php, Access token URL: http://52.74.96.205/mod/lti/token.php, and Authentication request URL: http://52.74.96.205/mod/lti/auth.php. At the bottom right are 'Email' and 'Cancel' buttons.

- 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.

The screenshot shows a 'Settings' dialog box with a dark theme. On the left is a sidebar with four menu items: 'URL Setting', 'External Tool', 'Mail Setting', and 'Client Details'. The 'External Tool' item is selected and highlighted. To the right of the sidebar, under the 'External Tool' section, there is a status indicator 'Configured' with a green checkmark. Below this, several configuration fields are listed with their corresponding values in text boxes:

Setting	Value
Tool name	Remote Learning Application
Issuer	http://52.74.96.205
Client ID	eNjPvjytlexmft
Access Token URL	http://52.74.96.205/mod/lti/token.php
Authorize URL	http://52.74.96.205/mod/lti/auth.php
JWK URL	http://52.74.96.205/mod/lti/certs.php
Deployment ID	1

At the bottom right of the dialog box are two buttons: 'Save' and 'Cancel'.

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](#).

```
GNU nano 4.0 /etc/apt/sources.list
## Major bug fix updates produced after the final release of the
## distribution.
deb https://mirror.kku.ac.th/ubuntu focal-updates main restricted
# deb-src http://my.archive.ubuntu.com/ubuntu focal-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb https://mirror.kku.ac.th/ubuntu focal universe
# deb-src http://my.archive.ubuntu.com/ubuntu focal universe
deb https://mirror.kku.ac.th/ubuntu focal-updates universe
# deb-src http://my.archive.ubuntu.com/ubuntu focal-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
deb https://mirror.kku.ac.th/ubuntu focal multiverse
# deb-src http://my.archive.ubuntu.com/ubuntu focal multiverse
deb https://mirror.kku.ac.th/ubuntu focal-updates multiverse
# deb-src http://my.archive.ubuntu.com/ubuntu focal-updates multiverse

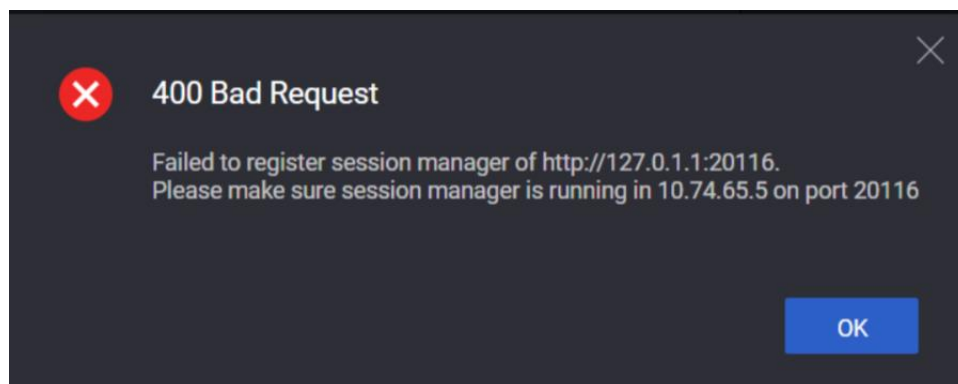
## N.B. software from this repository may not have been tested as
## extensively as that contained in the main release, although it includes
## newer versions of some applications which may provide useful features.
## Also, please note that software in backports WILL NOT receive any review
## or updates from the Ubuntu security team.
deb https://mirror.kku.ac.th/ubuntu focal-backports main restricted universe multiverse
# deb-src http://my.archive.ubuntu.com/ubuntu focal-backports main restricted universe multiverse

## Uncomment the following two lines to add software from Canonical's
## 'partner' repository.
## This software is not part of Ubuntu, but is offered by Canonical and the
## respective vendors as a service to Ubuntu users.
# deb http://archive.canonical.com/ubuntu focal partner
# deb-src http://archive.canonical.com/ubuntu focal partner

deb https://mirror.kku.ac.th/ubuntu focal-security main restricted
# deb-src http://my.archive.ubuntu.com/ubuntu focal-security main restricted
deb https://mirror.kku.ac.th/ubuntu focal-security universe
# deb-src http://my.archive.ubuntu.com/ubuntu focal-security universe
deb https://mirror.kku.ac.th/ubuntu focal-security multiverse
# deb-src http://my.archive.ubuntu.com/ubuntu focal-security multiverse

^G Get Help      ^O Write Out    ^R Where Is     ^R Cut Text     ^J Justify      ^G Cur Pos
^X Exit          ^B Read File    ^_ Replace      ^U Paste Text   ^I To Spell     ^_ Go To L
```

3 Bad Request with two IP addresses at host file



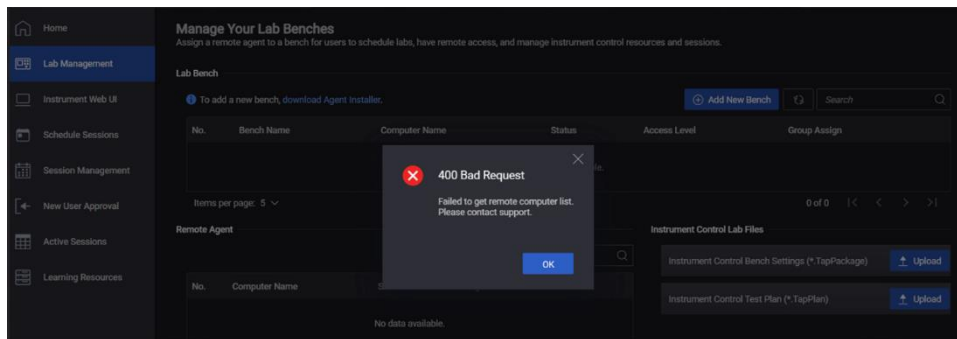
Go to `sudo nano /etc/hosts` and remove the extra IP address 127.0.1.1.

```
GNU nano 4.8
127.0.0.1 localhost
#127.0.1.1 ubuntuuserver

# 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 ubuntuuserver
```

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.

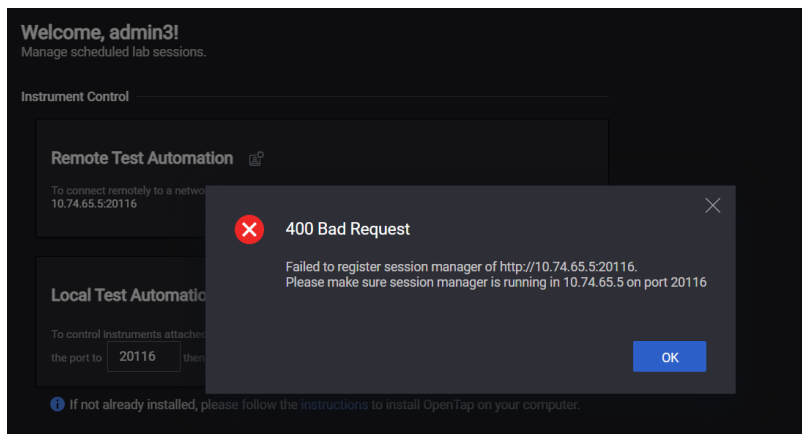


Go to PuTTY and run the following command:

```
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:

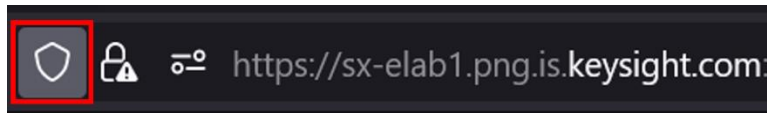
```
sudo -S systemctl enable open-tap
sudo -S systemctl start open-tap
sudo -S systemctl status open-tap
```

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

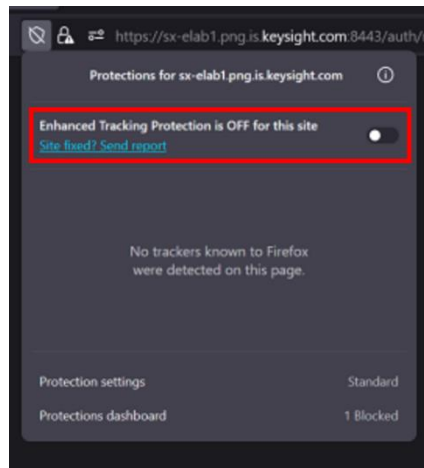
Firefox may block access to a site that uses a self-signed-cert and the user is stopped at the welcome page.

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,.', 'aaaaaabbbbb', 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.



This information is subject to change without notice.

© Keysight Technologies 2023–2024

Printed in Malaysia

Edition 3, March 2024



SR101-90000

www.keysight.com