



# **HPE ProLiant Security Experience**

Hands-On Lab

---

HPE ProLiant Servers differentiated by a security first focus

## Contents

HPE ProLiant Security Experience .....	3
Connecting to the lab environment .....	4
Embedded Server Management with HPE iLO .....	7
Managing Local Users.....	11
Firmware Verification.....	15
Applying Web Proxy configuration.....	18
Connecting to HPE Compute Ops Management .....	20
Return to your HOL Horizon session.....	21
Secure Login Options for Enterprise IT Administrators.....	23
Establishing a connection from HPE iLO to HPE GreenLake .....	26
Creating server groups and associating server settings.....	39
Advanced Security settings for iLO .....	49
iLO SSL Certificate Management.....	61
Deploying the Secure Gateway through VCenter.....	71
Configuring the Secure Gateway and connecting to COM.....	78
Connecting our HPE iLO to COM via the Secure Gateway.....	87

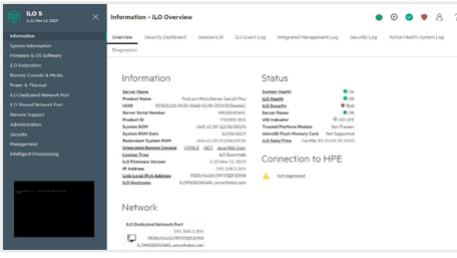
## HPE ProLiant Security Experience

HPE is speeding up time to value with our robust collection of IT Infrastructure management solutions. These tools are certified and optimized for management of HPE hardware and solutions. HPE's ProLiant Gen11 servers are designed from the ground up with security, remote manageability, and life-cycle management in mind.

**HPE iLO**

Embedded

Embedded Server Management that enables you to securely configure, monitor and update your HPE server



**HPE OneView**

On-premises

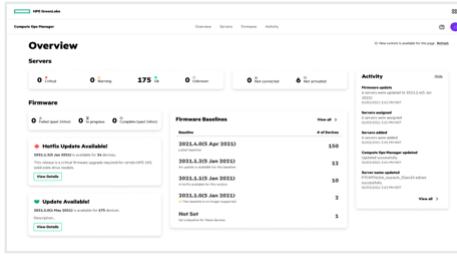
Infrastructure management software that provides composable solutions across compute, storage, and networking.



**HPE Compute Ops Management**

SaaS

Lifecycle management for all of your servers, from edge to cloud, delivered as a secure SaaS application continuously managed and improved by HPE.



Here is a quick overview of our Compute management portfolio.

- Compute Ops Management delivers unified operations as-a-service from edge to cloud. In this HOL you will work with this technology.
- HPE iLO is embedded server management that enables you to securely configure, monitor, and update your HPE servers from anywhere.
- HPE OneView is integrated IT infrastructure management software that automates IT operations and simplifies infrastructure lifecycle management across compute, storage, and networking. It is an onsite management strategy and is not the focus of this workshop.

This HOL aims to take a technical approach to how these tools can be used to manage HPE ProLiant Servers with a strong focus around Security.

## Connecting to the lab environment

Logging into the HPE Compute BU Enablement environment.

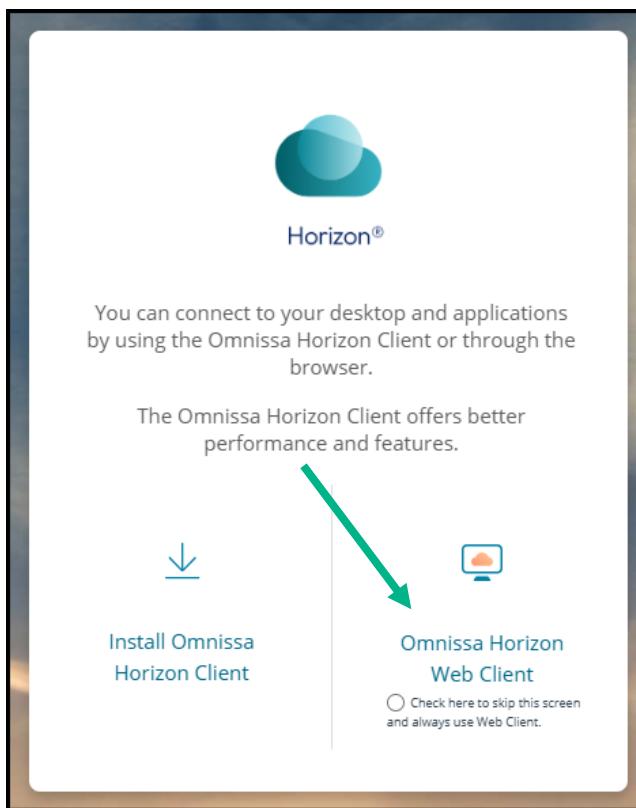
We will be using Horizon to connect to our lab environment. To get to your HPE Compute resources and view the server details page, follow the steps below.

1. Using your Chrome browser, go to our Horizon based HPE Compute BU Enablement access at:

External to HPE and not connected to an HPE VPN – <https://labs.compute.cloud.hpe.com>

Internal to HPE or connected to an HPE VPN - – <https://techenablement.hpecorp.net>

2. On the Horizon login screen, **click the Omnissa Horizon Web Client** button.

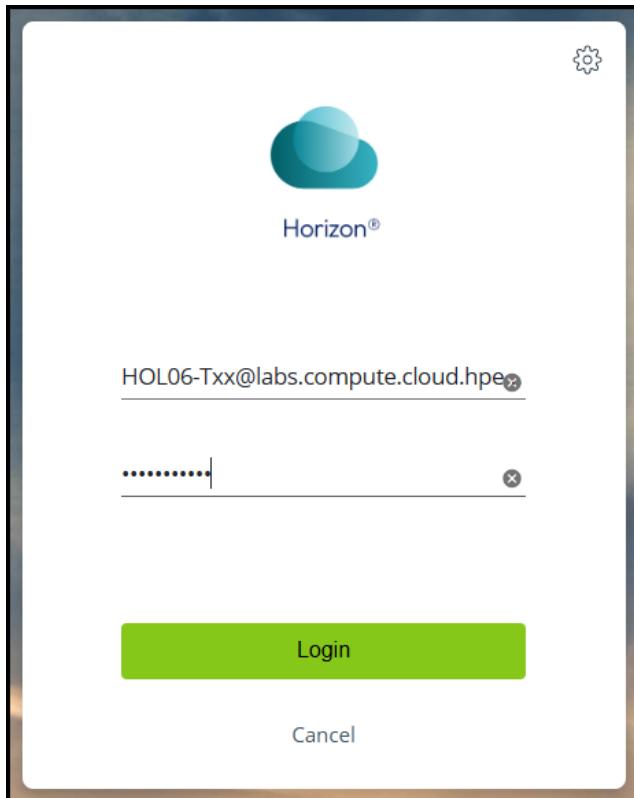


3. Enter the username and password supplied by your instructor and click the Login button.

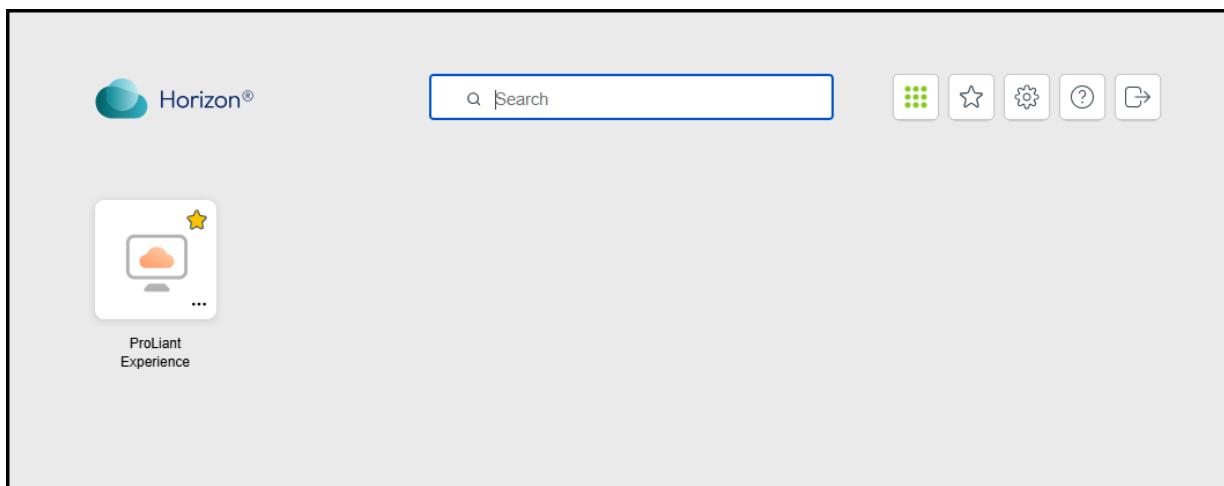
Username: **HOL06-T01@labs.compute.cloud.hpe.com** through **HOL06-**

**T25@labs.compute.cloud.hpe.com**, (depends on your team assignment)

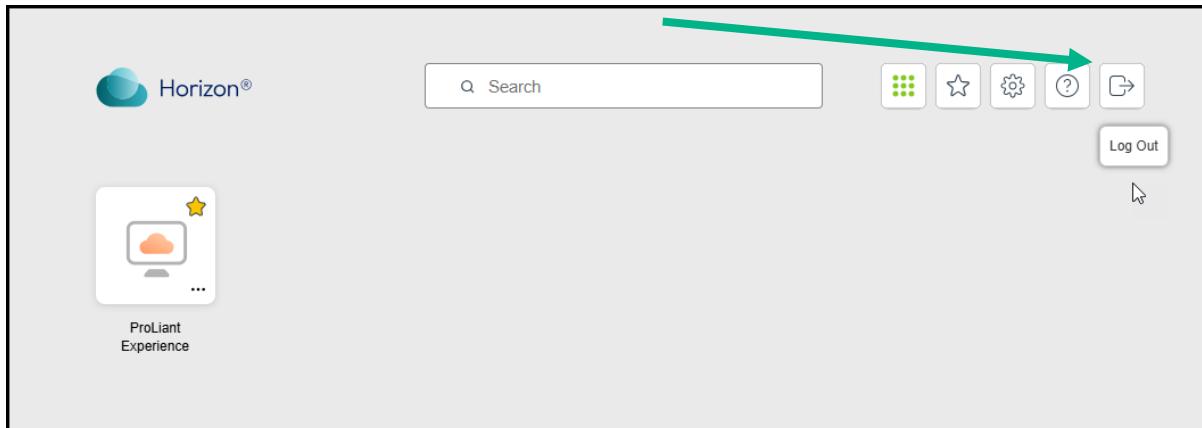
Password: Supplied by instructor



4. **Click on the graphic** that represents your Lab environment.



- When you are finished with the lab, please use the logout button.



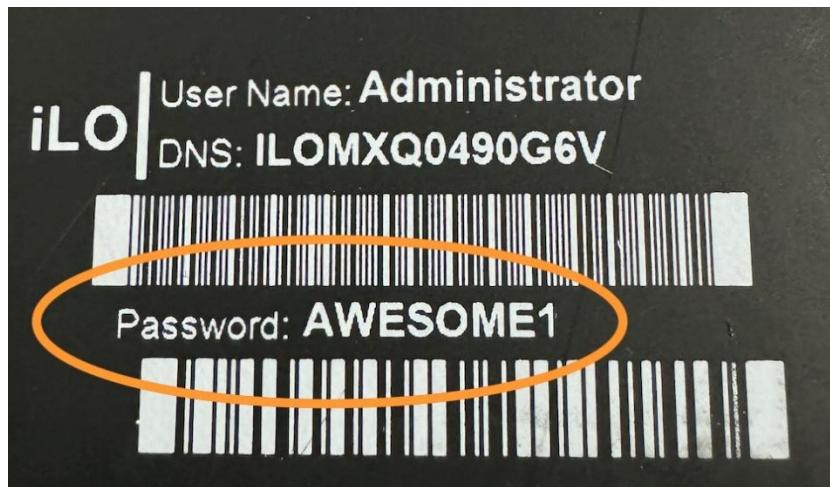
You are now in a VPN-enabled Chrome browser session. For these labs to work, you will need to stay within the context of this browser session. You have a secure connection to our remote lab in Houston, but it doesn't work like a traditional VPN session. Only what you launch from this browser session, is what is connected to the remote environment.

This concludes this portion of the lab.

## Embedded Server Management with HPE iLO

Integrated Lights-Out (iLO) is an embedded server management technology by Hewlett-Packard Enterprise (HPE) which provides out-of-band management facilities. The key features of iLO include virtual KVM console, virtual media, power management, environmental parameters monitoring, text console record and replay, and remote console capabilities. It allows administrators to manage servers remotely, regardless of the state of the operating system or the server itself. This remote management is possible through a dedicated Ethernet port for iLO on the server.

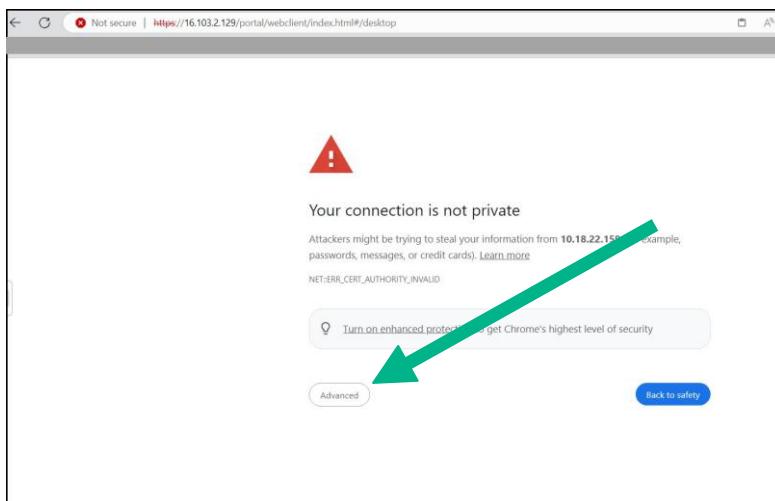
This portion of the lab exercises assumes the server has power, the iLO ethernet port is connected to a management network switch and the default password information has been gathered off the toe-tag on the front of the server.



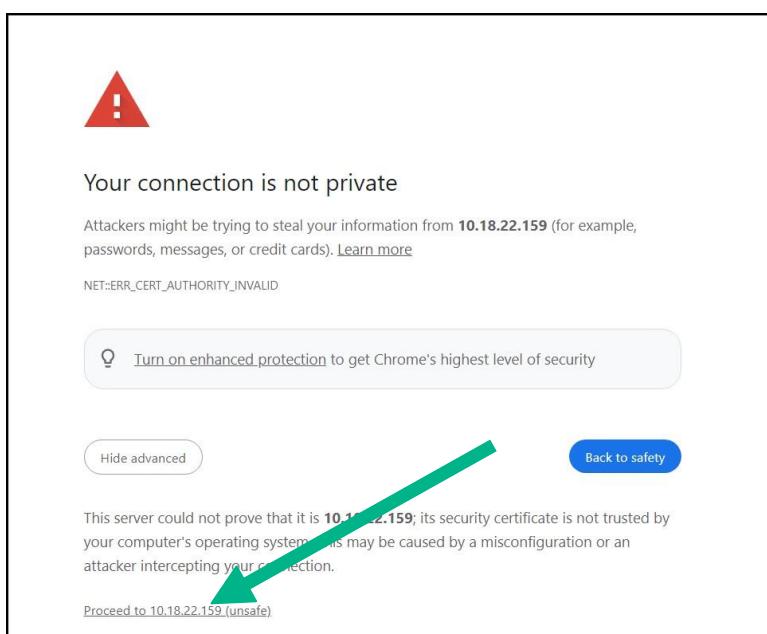
In this lab environment, a DHCP server is issuing IP addresses to known hosts using DHCP reservations. This ensures the lab unit you will access obtains the same IP address each time it boots after the lab is reset. Consult the table below for your team's name and number and default Administrator credentials. Also make notes of your server serial number.

<b>Team Name &amp; Number</b>	<b>iLO IP Address</b>	<b>Username</b>	<b>Default Factory Password</b>
Team-01	10.18.22.151	Administrator	5RMJFSM7
Team-02	10.18.22.152	Administrator	7P7WGPW7
Team-03	10.18.22.153	Administrator	CDPKGFK7
Team-04	10.18.22.154	Administrator	W8DPMPL6
Team-05	10.18.22.155	Administrator	MMJYCRM6
Team-06	10.18.22.156	Administrator	GMJR8CJ7
Team-07	10.18.22.157	Administrator	V57C5CW5
Team-08	10.18.22.158	Administrator	GC2Y6CM2
Team-09	10.18.22.159	Administrator	XLQZKVC5
Team-10	10.18.22.160	Administrator	WBNRMQY6
Team-11	10.18.22.161	Administrator	QTJZ2RN7
Team-12	10.18.22.162	Administrator	JSYDJDC5
Team-13	10.18.22.163	Administrator	VYH2NG72
Team-14	10.18.22.164	Administrator	SP26KQG8
Team-15	10.18.22.165	Administrator	SP26KQG8
Team-16	10.18.22.166	Administrator	JLN7ZJ25
Team-17	10.18.22.167	Administrator	8BVWHRSC
Team-18	10.18.22.168	Administrator	NY8FJ6NH
Team-19	10.18.22.169	Administrator	WLLLXVR8
Team-20	10.18.22.170	Administrator	9RJMJS2F
Team-21	10.18.22.171	Administrator	DZJN9WVT
Team-22	10.18.22.172	Administrator	69GF577X
Team-23	10.18.22.173	Administrator	NSDZVKQ8
Team-24	10.18.22.174	Administrator	LRVWY2C9
Team-25	10.18.22.175	Administrator	L97XNQJM

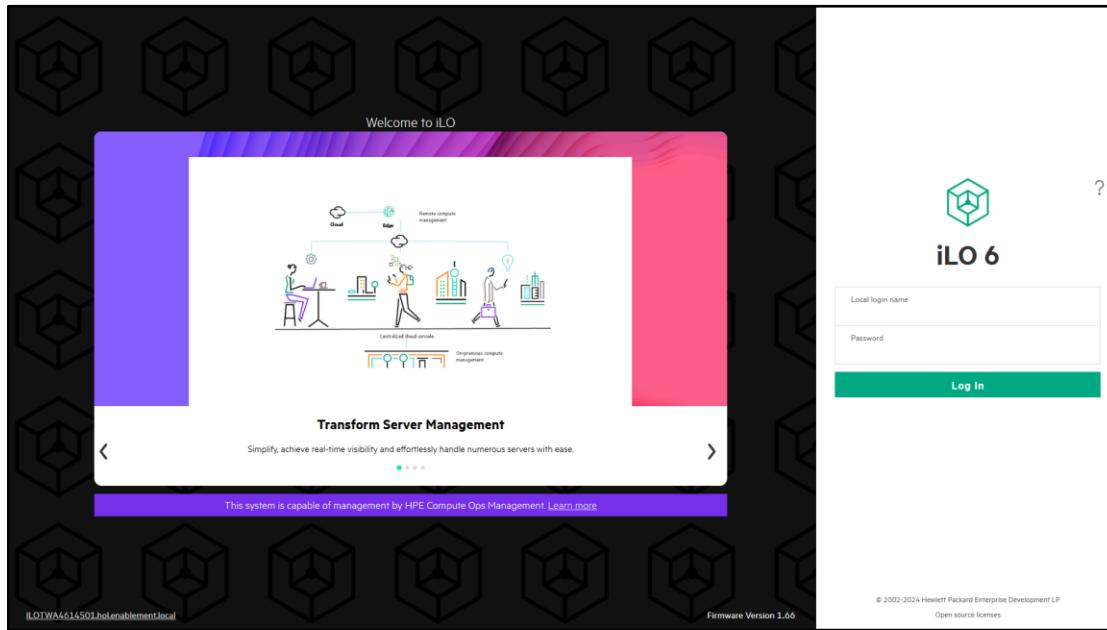
1. Use your Horizon enabled Chrome browser session that you connected with in the previous section.  
Remember that for these labs to work, you will need to stay within the context of this browser session.
2. Using the table above **Open a browser** (i.e. **Chrome** or **Edge**) and **type in the IP address** of your assigned server iLO. **NOTE: DO NOT USE IE**
3. If presented with a message saying “Your connection is not private” this is the self-signed SSL certificate presented to you for the iLO you are about to use. **Click Advanced.**



4. On the newly displayed prompt, **click on the Proceed to 10.18.22.xx** to continue to the iLO login screen.



5. Now enter **Administrator** and the **password from the table above**, into the Local login name and Password fields.
6. Click **Log In**.



7. Administrators are presented with valuable information about their server in the home screen. The Server, Status and iLO dashboards give quick access to information, and the navigation bar across the top displays tabs to drill into Security, Active Sessions, several different logs, and diagnostic information.

This concludes this portion of the lab.

## Managing Local Users

One of the first things administrators typically do is ensure their corporate standards are followed. This includes things like creating Local User access in iLO and setting the iLO IP addresses to a static address. There are other default iLO settings that the administrator might want to change from factory default.

1. In the left-hand navigation pane of your iLO, click **Administration**.

Local Users								
<table border="1"> <thead> <tr> <th>Login Name</th> <th>User Name</th> <th>Status</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>Administrator</td> <td>Administrator</td> <td>Enabled</td> <td><input checked="" type="checkbox"/> <input type="checkbox"/></td> </tr> </tbody> </table>	Login Name	User Name	Status	Actions	Administrator	Administrator	Enabled	<input checked="" type="checkbox"/> <input type="checkbox"/>
Login Name	User Name	Status	Actions					
Administrator	Administrator	Enabled	<input checked="" type="checkbox"/> <input type="checkbox"/>					

Service								
<table border="1"> <thead> <tr> <th>Login Name</th> <th>User Name</th> <th>Status</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>TechEnablement</td> <td>TechEnablement</td> <td>Enabled</td> <td><input checked="" type="checkbox"/> <input type="checkbox"/></td> </tr> </tbody> </table>	Login Name	User Name	Status	Actions	TechEnablement	TechEnablement	Enabled	<input checked="" type="checkbox"/> <input type="checkbox"/>
Login Name	User Name	Status	Actions					
TechEnablement	TechEnablement	Enabled	<input checked="" type="checkbox"/> <input type="checkbox"/>					

2. For the purposes of this lab, we will **leave the Administrator account with the default toe-tag password** and set up another administrative user account to access the iLO.
3. Click **New** in the Local Users frame and enter the following settings to create your new user account.

<b>Login Name</b>	HPE_Admin
<b>User Name</b>	HPE Admin
<b>New Password</b>	hpent123
<b>Confirm Password</b>	hpent123
<b>Role</b>	Administrator

**Add Local User**

**User Information**

Login Name	HPE_Admin
User Name	HPE Admin
New Password	*****
Confirm Password	*****

**User Permissions**

Role	Administrator
Privileges	<input type="checkbox"/> select all <input checked="" type="checkbox"/> Login

Optionally you can select Custom for the Role, which allows this user to be assigned the privilege to create iLO hosted firmware recovery sets. **Do not select** this choice for this lab.

**User Permissions**

Role	Administrator
Privileges	<input type="checkbox"/> select all <input checked="" type="checkbox"/> Login <input checked="" type="checkbox"/> Remote Console <input checked="" type="checkbox"/> Virtual Power and Reset <input checked="" type="checkbox"/> Virtual Media <input checked="" type="checkbox"/> Host BIOS <input checked="" type="checkbox"/> Configure iLO Settings <input checked="" type="checkbox"/> Administer User Accounts <input checked="" type="checkbox"/> Host NIC <input checked="" type="checkbox"/> Host Storage <input type="checkbox"/> Recovery Set
IPMI/DCMI Privilege based on above settings:	
<input type="text" value="administrator"/> <input type="checkbox"/> Service Account	

- Click on **Add User** to save the new account.

5. You should now see that the new user has been added to the User Administration list.

The screenshot shows the User Administration page with the following details:

- Local Users:**

Login Name	User Name	Status	Actions
Administrator	Administrator	Enabled	Checkmark icons across all columns
HPE_Admin	HPE Admin	Enabled	Checkmark icons across most columns, except the last one which has an 'X'
- Service:**

Login Name	User Name	Status	Actions
TechEnablement	TechEnablement	Enabled	Checkmark icons across all columns
- Buttons at the bottom:** New, Edit, Delete, Enable

6. Logout and then log back in with your newly created user.
7. Take Note – You have just created a fully privileged Administrator account with a very simple password. We will circle back on this in a later part of the Lab.
8. Return to the Administration section in iLO and Click on the Directory Groups tab.

The screenshot shows the Administration - Directory Groups page with the following details:

- Directory Groups:**

Group	SID	Actions
Administrators		Checkmark icons across all columns
Authenticated Users	S-1-5-11	Mixed checkmark and 'X' icons across columns
- Buttons at the bottom:** New, Edit, Delete

The Directory Groups tab is where administrators can enter up to six directory groups using Kerberos authentication and schema-free directory integration. More information can be found in the iLO help and the HPE Support Center. [https://support.hpe.com/hpsc/public/docDisplay?docId=sd00002007en\\_us](https://support.hpe.com/hpsc/public/docDisplay?docId=sd00002007en_us)

This concludes this portion of the lab.

## Firmware Verification

The Firmware Verification feature allows you to run an on-demand scan or implement scheduled scans.

To respond to detected issues, you can configure iLO to:

- Log the results.
- Log the results and initiate a repair action that uses a recovery install set.

Depending on the scan results, information is logged in the Active Health System Log and the Integrated Management Log. The following firmware types are supported:

- iLO Firmware
- System ROM (BIOS)
- System Programmable Logic Device (CPLD)
- Server Platform Services (SPS) Firmware (supported servers only)
- Innovation Engine (IE) Firmware
- Server Platform Services-IE Full Recovery Image (supported servers only)

When a firmware verification scan is in progress, you cannot install firmware updates or upload firmware to the iLO Repository. If an invalid iLO or System ROM (BIOS) firmware file is detected, the invalid file is saved to a quarantine area in the iLO Repository. You can download the invalid file to investigate its type and origin.

Quarantined images are not displayed on the iLO Repository page, and you cannot select them when you use the Flash Firmware feature.

- Click on the **Firmware Verification** tab to explore the iLO capability to manually scan the system firmware to check the validity and health of the firmware components.

Firmware Name	Firmware Version	Health	State	Recovery Set Version
iLO 6	1.66 Dec 13 2024	<span>OK</span>	<span>Enabled</span>	Not present
System ROM	A58 v1.30 (10/04/2024)	<span>OK</span>	<span>Enabled</span>	Not present
System Programmable Logic Device	0x03	<span>OK</span>	<span>Enabled</span>	Not present

- Click **Scan Settings** and **Enable Background Scan** with an Integrity Failure Action of **Log Only**. The default setting is 7 days, but for this lab, change the **Scan Interval** to 1.

- Click **Submit** to save the scan settings. You should see that the scan settings have been saved successfully.

The screenshot shows the 'Firmware Verification' tab selected in the navigation bar. A success message 'Scan settings saved successfully' is displayed. The 'Firmware Status' table lists three components: iLO 6, System ROM, and System Programmable Logic Device, all in 'OK' health status and 'Enabled' state. A 'Scan Settings' button is visible in the top right corner.

Firmware Name	Firmware Version	Health	State	Recovery Set Version
iLO 6	1.66 Dec 13 2024	<span>OK</span>	<span>Enabled</span>	Not present
System ROM	A58 v1.30 (10/04/2024)	<span>OK</span>	<span>Enabled</span>	Not present
System Programmable Logic Device	0x03	<span>OK</span>	<span>Enabled</span>	Not present

- Click **Run Scan** to trigger a runtime firmware verification of the component firmware to ensure validity. This scan is performed by the iLO processor and does not consume clock cycles from the server's CPUs. This action can be called from the API or a language binding like HPE iLO REST Utility or PowerShell.

The screenshot shows the 'Firmware Verification' tab selected. A message indicates a 'New scan in progress, please wait ...'. The 'Firmware Status' table shows the same three components as before, but their 'State' column now includes a small circular progress icon. At the bottom, there are two buttons: 'Run Scan' and 'Send Recovery Event'.

Firmware Name	Firmware Version	Health	State	Recovery Set Version
iLO 6	1.66 Dec 13 2024	<span>OK</span>	<span>Scanning</span>	Not present
System ROM	A58 v1.30 (10/04/2024)	<span>OK</span>	<span>Scanning</span>	Not present
System Programmable Logic Device	0x03	<span>OK</span>	<span>Enabled</span>	Not present

- Return to the iLO Information screen.

This concludes this portion of the lab.

## Applying Web Proxy configuration

HPE iLO enables organizations to customize the security settings within the iLO controller to comply with their security requirements. This may include uploading a trusted SSL Security Certificate, integration into Directory Services, turning on a Login Security Banner and many others. For this exercise, we will be enabling a proxy server for the iLO to be used in the environment.

1. Login to your team assigned iLO with the **HPE\_Admin** account you created earlier.
2. In the left-hand navigation pane click **Security**.
3. Make sure you have focused on the **Security / Access Settings** tab.

Server		Network		iLO	
Server Name	localhost:mgmt.hpe.local	Anonymous Data	Enabled	Global Component Integrity	Disabled
Server FQDN / IP Address	[Not set]	Enhanced Download Performance	Enabled	Component Integrity Policy	No Policy
		IPMI/DCMI over LAN	Disabled	Downloadable Virtual Serial Port Log	Disabled
		IPMI/DCMI over LAN Port	623	Idle Connection Timeout (minutes)	30
		IPMI over KCS	Enabled	ILO Functionality	Enabled
		Remote Console	Enabled	ILO RIBCL Interface	Enabled
		Remote Console Port	17990	ILO ROM-Based Setup Utility	Enabled
		Secure Shell (SSH)	Enabled	ILO Web Interface	Enabled
		Secure Shell (SSH) Port	22	Remote Console Thumbnail	Enabled
		SNMP	Enabled	Require Host Authentication	Disabled
		SNMP Port	161	Require Login for iLO RBSU	Disabled
		SNMP Trap Port	162	Serial Command Line Interface Speed	9600
		Virtual Media	Enabled	Serial Command Line Interface Status	Enabled - Authentication Required
		Virtual Media Port	17998	Show ILO IP during POST	Enabled
		Virtual Serial Port Log Over CLI	Disabled	Show Server Health on External Monitor	Enabled
		Web Server	Enabled	VGA Port Detect Override	Enabled
		Web Server Non-SSL Port Enabled	Enabled	Virtual NIC	Disabled
		Web Server Non-SSL Port	80		
		Web Server SSL Port	443		
		Web Proxy	Disabled		
		Web Proxy Server	[Not set]		
		Web Proxy Port	1		
		Web Proxy Username	[Not set]		

Account Service		Update Service	
Authentication Failures Before Delay	1 failure causes no delay	Downgrade Policy	
Authentication Failure Delay Time	10 seconds	Accept 3rd Party Firmware Update Packages	Disabled
Authentication Failure Logging	Enabled - Every 3rd Failure		
Minimum Password Length	8		
Password Complexity	Disabled		

4. In the middle column, in the **Network** section, click the **edit** (pencil) icon.
5. Now scroll down to the **Web Proxy** section.
6. Click the checkbox for **Web Proxy**
7. Now enter **hpeproxy.its.hpecorp.net** in the **Web Proxy Server** field
8. Enter **443** in the **Web Proxy Port** fields.

9. Leave the other settings blank.

Web Server SSL Port	
443	
<input checked="" type="checkbox"/> Web Proxy	
Web Proxy Server	
hpeproxy.its.hpecorp.net	
Web Proxy Port	
443	
Web Proxy Username	
Web Proxy Password	

10. Click **OK** to save the changes you entered.

This concludes this portion of the lab.

## Connecting to HPE Compute Ops Management

The HPE GreenLake Cloud Platform enables IT administrators to connect and manage devices and cloud services under a unified service presented by HPE. HPE compute, storage, and networking devices may be centrally managed whether on-premises, at the edge, co-located, or on the other side of the world.

This single HPE GreenLake dashboard allows administrators to launch domain specific applications like Compute Ops Management, Aruba Central, Data Services, along with tools to manage governance like OpsRamp and gain insights in the HPE Sustainability Insight Center.

The screenshot shows the HPE GreenLake Cloud Platform dashboard. At the top, there is a header with the HPE GreenLake logo, the workspace name "COM Security Lab 01", and navigation links for "Home", "Services", and "Devices". On the right side of the header are icons for notifications, user profile, and other settings. Below the header, there are three main sections: "Getting Started", "Recent Services", and "Featured Services". The "Getting Started" section contains two cards: "Find Services" (Discover and launch services from our catalog) and "Manage Workspace" (Set up this workspace, users, access and more). A "Dismiss" button is located above the Manage Workspace card. The "Recent Services" section shows a card for "Compute Ops Management" with a "Launch" button. To the right of these sections is a "Quick Links" sidebar with links to "Manage Workspace", "Device Inventory", "Service Subscriptions", "User Management", "Locations", "Switch Workspace", "Reporting", "Feedback", and "Support Hub". At the bottom of the dashboard, there are "Learn" and "View Catalog" buttons.

For this exercise, we are going to focus on the onboarding of our devices into the GreenLake platform so that they may be managed by HPE Compute Ops Management.

You will need to login to the GreenLake environment. For this portion of the lab, you will use a different username and password from what you used to start the labs. Your assignment is based on your team number and is in the table below.

Once you have located your username and password, proceed to Step 1 of this lab.

Return to your HOL Horizon session.

1. Open a new tab and connect to HPE GreenLake at <https://common.cloud.hpe.com> and then enter your assigned user information from the following table as the Username. Your instructor will provide a password if it is different from the table below.

<b>Team Number</b>	<b>GreenLake Username</b>	<b>Userpassword</b>
Team-001	comholuser+1@gmail.com	2025!Summ3r
Team-002	comholuser+2@gmail.com	2025!Summ3r
Team-003	comholuser+3@gmail.com	2025!Summ3r
Team-004	comholuser+4@gmail.com	2025!Summ3r
Team-005	comholuser+5@gmail.com	2025!Summ3r
Team-006	comholuser+6@gmail.com	2025!Summ3r
Team-007	comholuser+7@gmail.com	2025!Summ3r
Team-008	comholuser+8@gmail.com	2025!Summ3r
Team-009	comholuser+9@gmail.com	2025!Summ3r
Team-010	comholuser+10@gmail.com	2025!Summ3r
Team-011	comholuser+11@gmail.com	2025!Summ3r
Team-012	comholuser+12@gmail.com	2025!Summ3r
Team-013	comholuser+13@gmail.com	2025!Summ3r
Team-014	comholuser+14@gmail.com	2025!Summ3r
Team-015	comholuser+15@gmail.com	2025!Summ3r
Team-016	comholuser+16@gmail.com	2025!Summ3r
Team-017	comholuser+17@gmail.com	2025!Summ3r
Team-018	comholuser+18@gmail.com	2025!Summ3r
Team-019	comholuser+19@gmail.com	2025!Summ3r
Team-020	comholuser+20@gmail.com	2025!Summ3r
Team-021	comholuser+21@gmail.com	2025!Summ3r
Team-022	comholuser+22@gmail.com	2025!Summ3r
Team-023	comholuser+23@gmail.com	2025!Summ3r
Team-024	comholuser+24@gmail.com	2025!Summ3r
Team-025	comholuser+25@gmail.com	2025!Summ3r

Connecting to Sign-in with your HPE account to access HPE GreenLake edge-to-cloud Platform

### Sign In

Username

Remember me

**Next**

OR

**Sign in with SSO**

Need help signing in?

Don't have an account? [Sign up](#)

Connecting to Sign-in with your HPE account to access HPE GreenLake edge-to-cloud Platform

### Sign In

Username

Password

Remember me

**Sign In**

OR

**Sign in with SSO**

Need help signing in?

2. Click **Next** to be prompted for a password.

3. Type in the password of **2025!Summ3r** (or the password supplied by your instructor) and press the **Enter** key or click **Sign In**.
4. If there a short advertising message, enjoy it and then close the pop-up window.
5. When presented with a choice of workspaces, choose **COM Security Lab XX** (where **XX** is your Team Number) and **Go to Workspace**.

Welcome to HPE GreenLake

Here's a list of workspaces we found associated with [comholuser+1@gmail.com](mailto:comholuser+1@gmail.com):

**Workspaces**

	HPE Tech Enablement HOLs	<a href="#">Go to Workspace</a>
	COM Security Lab 01	<a href="#">Go to Workspace</a>

[Don't see your workspace?](#) [Back to Sign In](#)

[Create a new workspace](#) [Create Workspace](#)

6. You are now on the HPE GreenLake Cloud Platform homepage. You can see your workspace choice, to the right of the HPE GreenLake logo.

**Getting Started**

- Find Services** Discover and launch services from our catalog.
- Manage Workspace** Set up this workspace, users, access and more.

**Recent Services**

- Compute Ops Management** Compute [Launch](#)

**Featured Services**

[View Catalog](#)

**My Services**

**Quick Links**

- [Manage Workspace](#)
- [Device Inventory](#)
- [Service Subscriptions](#)
- [User Management](#)
- [Locations](#)
- [Switch Workspace](#)
- [Reporting](#)
- [Feedback](#)
- [Support Hub](#)

**Learn**

This concludes this section of the lab.

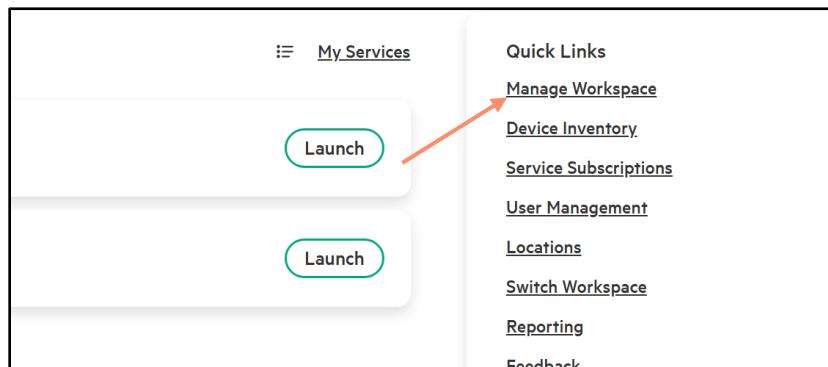
## Secure Login Options for Enterprise IT Administrators

In the previous section of this lab, we were able to login to our HPE Compute Ops Management Workspace with an email address and somewhat complex password. In today's world, this is no longer secure enough to meet Industry Security Standards and additional safeguards should be configured.

Our HPE GreenLake Cloud Platform supports Multi-Factor Authentication as well as SAML SSO which combining both together, can go a long way to ensuring any bad actors do not access your IT Estate, especially through Compute Ops Management.

For this Lab, we will just walk you through the various locations in HPE GreenLake Cloud Platform where this can be configured, but we will not actually set it up at this time.

1. From the **Quick Links** on the right-hand side of the Home Page, click **Manage Workspace**.



2. Select the **Workspace Details** tile.

**Manage Workspace**  
Manage your HPE GreenLake workspace.

**COM Security Lab 23**

Workspace ID  
870c840ad75b11ef9a1e823dadb361ea

Workspace Status  
Registered

Workspace Type  
Standard Enterprise Workspace

Organization  
HPE Tech Enablement

**Workspace Details**  
Manage your workspace's details including name, phone number, email, and MFA configuration.

**Workspace identity & access**  
Manage users and their access to this workspace's services and resources.

**Audit Log**  
View changes and processes within all your applications.

**Personal API clients**  
Access application data programmatically through an API.

**IP Access Rules**  
Set up and manage IP access.

**Locations**  
Manage device addresses to automate supporting services.

**Usage Monitoring**  
Track subscription and system resource usage.

**Automations**  
Automate workflows for efficiency and productivity.

**Reporting**  
Manage and create reports on the platform from different data sources.

3. In the Actions pull down, navigate to the **Manage MFA** list.

**Manage Workspace**  
**COM Security Lab 23**

Name	COM Security Lab 23
Description	--
Type	Standard Enterprise Workspace
Workspace ID	870c840ad75b11ef9a1e823dadb361ea
Organization	HPE Tech Enablement
Country	United States
Address	1701 E Mossy Oaks Rd Spring, Texas 77389
Workspace contact phone number	--
Workspace contact email	com.demoad@gmail.com
Multi-factor authentication (MFA)	Not required

**Activate Windows**  
Go to Settings to activate Windows

Actions ▾  
[Edit](#)  
**Manage MFA**  
[Delete workspace](#)

4. This is where Multifactor Authentication can be configured for all Users within the Workspace. Currently supported methods are Okta Verify, Security Key or Biometric Authenticator and Google Authenticator.

The screenshot shows the HPE GreenLake workspace management interface. On the left, there's a list of workspaces, with 'COM Security Lab 23' selected. On the right, a modal window titled 'Manage multi-factor authentication' is open. It contains a note about requiring MFA for all users and a checkbox labeled 'Require MFA' which is checked.

Name	Value
Description	--
Type	Standard Enterprise Workspace
Workspace ID	870c840ad75b11ef91e823dacb361ea
Organization	HPE Tech Enablement
Country	United States
Address	1701 E Mossy Oaks Rd Spring, Texas 77389
Workspace contact phone	--

## Note: For the purpose of this lab, we will NOT be configuring MFA on these Workspaces.

When enabling Multifactor Authentication (MFA), you significantly enhance the security of your account when signing in to HPE GreenLake. By requiring multiple forms of verification, such as a password and a one-time code sent to your mobile device, MFA adds an extra layer of protection against unauthorized access. This reduces the risk of account compromise, even if your password is stolen or guessed. Implementing MFA is a crucial step in safeguarding your sensitive data and ensuring secure access to HPE GreenLake services.

Note: MFA can also be configured at the user level from the **HPE user account details**. However, please do **NOT** enable it for this lab.

The screenshot shows the 'My HPE Account' page. At the top, there are navigation links for Home, Services, Devices, and a user icon. Below that is a section for 'Com Holuser' with the email 'comhol...+25@gmail.com'. A red arrow points to the link 'HPE User Account Details'. Further down are links for 'HPE GreenLake Preferences', 'Visit hpe.com', and 'Sign out of HPE'. At the bottom is a large green button labeled 'My HPE Account'.

This concludes this section of the lab.

## Establishing a connection from HPE iLO to HPE GreenLake

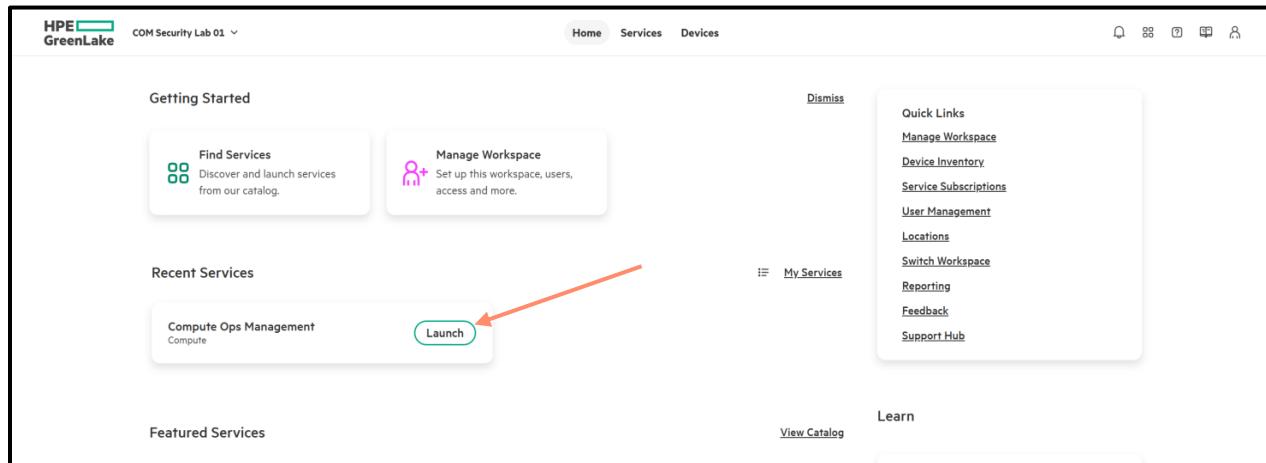
For our lab purposes, the HPE GreenLake Workspace company in this environment is called **COM Security Lab XX**.

The connection between iLO and HPE GreenLake is initiated by the iLO for security purposes. During the onboarding process, an HPE-issued client certificate is used by the iLO to connect to HPE Compute Ops Management. The HPE CA Certificate uses SHA256 with a key size of EC 384 bits and is transmitted over a Mutual Transport Layer Security (mTLS) connection from the iLO to HPE GreenLake and Compute Ops Management over HTTPS (port 443). In a typical TLS setup, only the server is authenticated by the client. In mTLS, both the client and the server authenticate each other, providing enhanced security by ensuring that both parties are authenticated before establishing a secure communication channel.

For more information regarding the security protocols and firewall requirements, consult the [HPE Compute Ops Management security guide](#).

To initiate the connection from HPE iLO to the HPE Compute Ops Management, we first need to obtain an Activation Key.

1. From the HPE GreenLake Recent Services section, choose the **Compute Ops Management Launch** button to connect to HPE Compute Ops Management main menu.



2. Navigate to the **Servers** tab across the top of the page.

Compute Ops Management

Overview Servers Inventory Manage Firmware Reports Activity

Overview

Servers health status iLO security status Groups compliance

3. Click the **Add server** button.

Compute Ops Management

Overview Servers Inventory Manage Firmware Reports Activity

Servers

Add server

4. At this time, we will select **Direct connect** as our Server Connection type. Click **Next**.

Add server

Step 1 of 3

**Connection type**

[Learn more about adding a server](#)

Get an activation key and use it in iLO to onboard server(s) to Compute Ops Management. The server will be added to HPE GreenLake device inventory if not previously added.

⚠ Ensure that your HPE GreenLake Platform application role includes **edit** permissions for **Devices and Subscription Service**.

Server connection type

Direct connect

Secure gateway

Next

5. Here we can select how long our Activation Key will be valid for and which Subscription Key we will apply. For this lab, let's choose **30 minutes** and **any available subscription key** and click **Next**.

Step 2 of 3

## Activation key options

**Expiration**  
Choose how long the activation key will be valid

30 minutes ▾

**Subscription key (optional)**  
Select an existing subscription key or enter a new subscription key to be assigned to the server, as part of server onboarding to Compute Ops Management.

K7YYUYTUE2977 ▾

**Next**

6. Once you have reviewed the details, click **Finish and generate activation key**.

Step 3 of 3

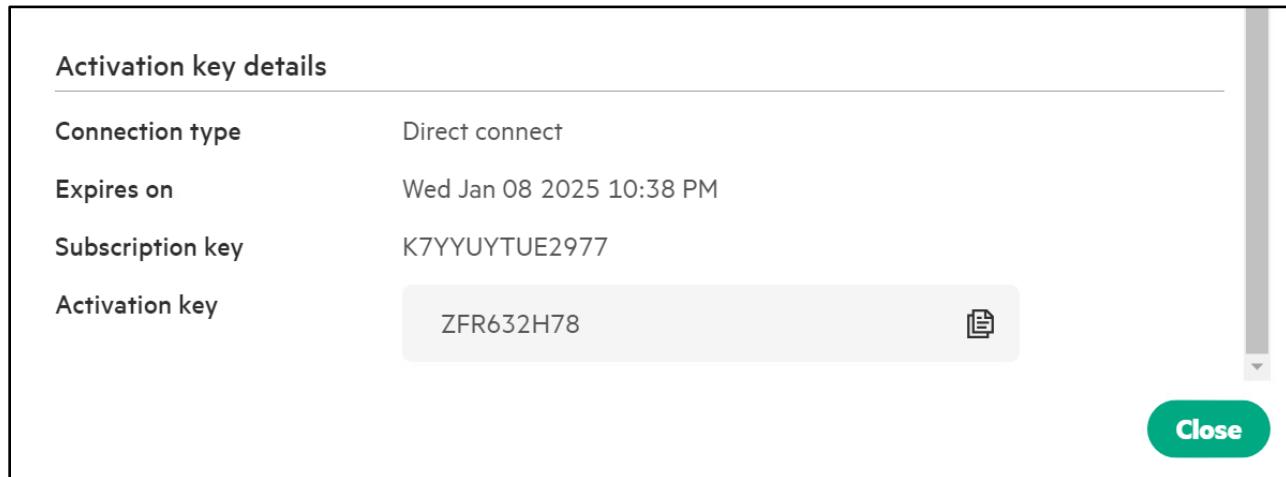
## Review

**Activation key details**

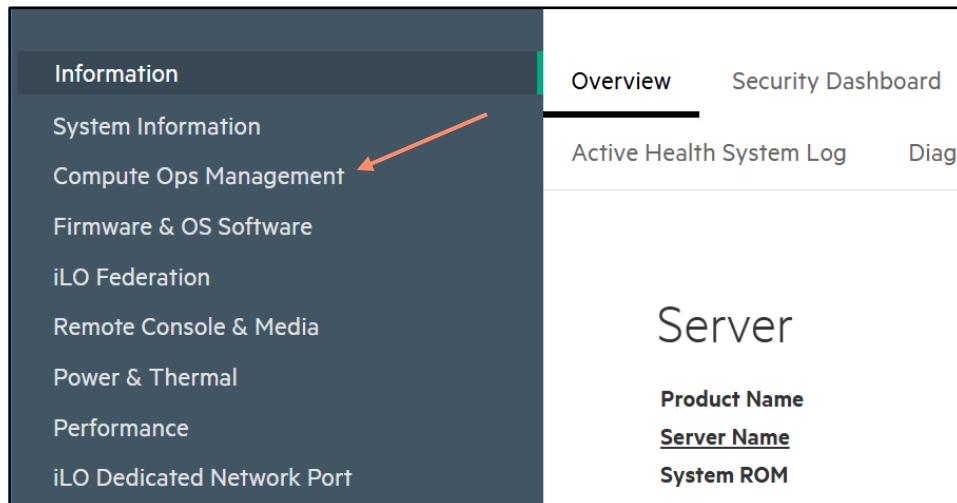
Connection type	Direct connect
Expiration	Wed Jan 08 2025 10:36 PM
Subscription key	K7YYUYTUE2977

**Finish and generate activation key**

- We will now take note of our Activation Key, so we can use it in our HPE iLO to connect to Compute Ops Management. Click the **copy icon** and then close this pop up.



- Return to the Web Browser Tab, which is connected to your assigned Server's iLO, then navigate to **Compute Ops Management** on the left-hand side of your screen.



9. Click **Enable** to enable the Compute Ops Management connection.

## Compute Ops Management

**Connection Status**  Not Enabled

**Introducing HPE Compute Ops Management**  
Configure iLO to seamlessly monitor, manage, and gain real-time visibility of your distributed compute environment.

The screenshot shows the 'Compute Ops Management' page. At the top right, there's a 'Connection Status' section with a checkbox labeled 'Not Enabled'. Below it is a brief introduction to Compute Ops Management. The main area features two columns: 'Secure' (purple background) and 'Automate' (blue background). The 'Secure' column contains text about server access, monitoring, and management. The 'Automate' column contains text about tasks for efficiency, deployment, and management. At the bottom right is a green 'Enable' button. A red arrow points from the text above the 'Enable' button towards it, indicating where to click.

**Cloud-based compute management for the distributed enterprise**

**Secure**  
server access, monitoring and management reduces exposure to security risks and compliance issues

**Automate**  
tasks for efficiency, reduce manual effort in deployment, and achieve seamless, simplified management

**Enable**

10. Then click on **Enter Activation Key**.

## Compute Ops Management

### Connection Status

⚠ Activation Key Required

Recommendations([View a video tutorial](#)):

An activation key is required for iLO to connect to HPE Compute Ops Management. To obtain an activation key

1. Log in to an HPE GreenLake workspace <https://common.cloud.hpe.com/>, and then start a HPE Compute Ops Management service instance.
2. Click **Servers**, and then click **Add server**.
3. Enter the required details, and then click **Get activation key**.
4. Click the copy icon to copy the generated key, and then click **Close**.  
Save the activation key in a secure location. You can use it to activate multiple servers in the service instance you used to generate the key, until the key expires.
5. Return to this page, enter the activation key, and then click **Save** to initiate a connection to HPE Compute Ops Management.

For more information, see the [HPE Compute Ops Management Getting Started Guide](#).

[Disable](#)

**Enter Activation Key**

11. Then paste the **Activation Key** you copied previously and hit **Save**.

### Enter Activation Key

X

To obtain an activation key

1. Log in to an HPE GreenLake workspace <https://common.cloud.hpe.com/>, and then start a Compute Ops Management service instance.
2. Click **Servers**, and then click **Add server**.
3. Enter the required details, and then click **Get activation key**.
4. Click the copy icon to copy the generated key, and then click **Close**.  
Save the activation key in a secure location. You can use it to activate multiple servers in the service instance you used to generate the key, until the key expires.
5. Return to this page, enter the activation key, and then click **Save** to initiate a connection to Compute Ops Management.

For more information, see the [HPE GreenLake for Compute Ops Management Getting Started Guide](#).

Activation key

ZFR632H78

**Save**

12. After a few seconds, it should now show you as **Connected** with your **Workspace ID** and **Connection Type**.

## Compute Ops Management

Connection Status	Connected
HPE GreenLake Workspace ID	04ac5888d75a11ef908216479ea8874e
Connection Type	Direct

Use HPE Compute Ops Management to perform some next actions:

- Subscribe to email notification for real time health issues
- Assign location to automatically create a support case when hardware fails

[Edit Settings](#) [Launch HPE GreenLake](#)

Whilst we have **demonstrated** the **manual way of onboarding a Server** to HPE Compute Ops Management, we are cognizant that you may need to do this for **10's to 100's** of Servers for your Customer's environment. To **streamline** this process, these steps can be **automated using different methods and scripting languages**, one **example** being [Prepare-and-Connect-iLOs-to-COM.ps1](#). To see the script in action and understand how it works, you can watch a [demonstration video](#)

This concludes this section of the lab.

## Securing your Server Fleet with HPE Compute Ops Management

HPE Compute Ops Management provides the foundation for cloud compute services that enable a simple, self-service, and real-time experience for IT professionals to access compute services from anywhere across their edge- to-cloud environment.

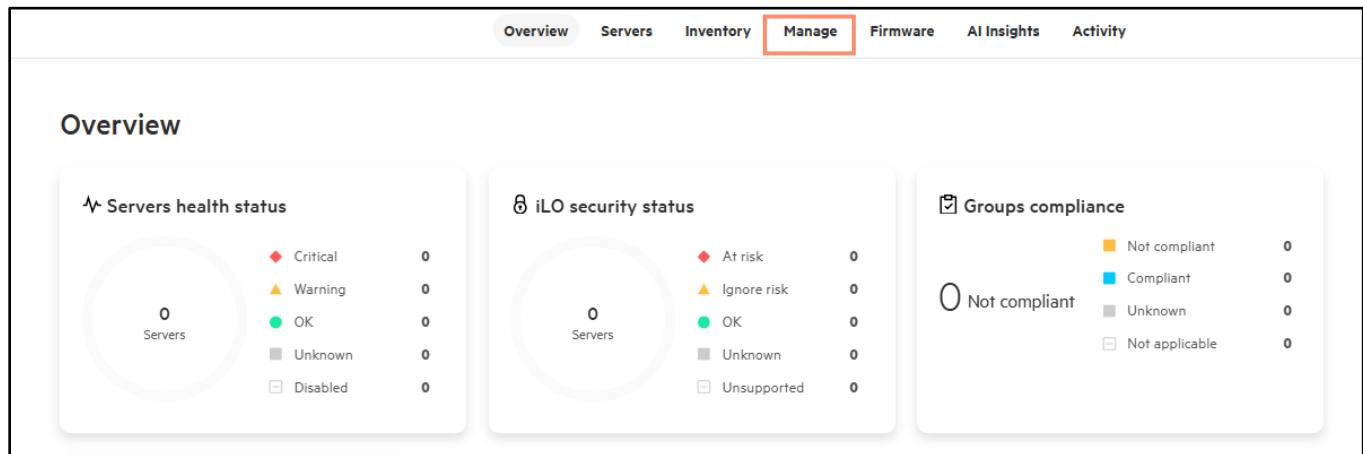
This equips organizations with a unified compute management experience that streamlines compute operations through one cloud-based console providing instant availability to new services and features as they become available.

### Configuring Server Groups and Applying Server Settings

In this portion of the lab, we will focus on the security configuration and lifecycle management aspect of your assigned server. We will create settings for the systems and place those settings into Groups. This ensures consistency across all servers assigned to those groups.

Return to your HOL Horizon Browser session.

1. From the HPE Compute Ops Management main menu. Select the **Manage** option.



2. Now pick the tile for **Settings**.

**Manage**

- Groups**  
Groups allow easier device management of server and OneView appliances.
- Settings**  
Settings allow consistent configuration management across devices in a group.
- Email notification policy preference**  
Configure an email notification policy preference to apply when servers are activated for management.
- Metrics data collection and utilization alerts**  
Opt-in to allow Compute Ops Management to collect usage metrics for sustainability AI insights, utilization reporting and alerting.
- Data Services Cloud Console integration**  
Set up integration with Data Services Cloud Console allowing configuration of external storage.
- ServiceNow integration**  
Set up automatic incident creation
- Aruba Central integration**  
Set up integration with Aruba Central to view server network adapter to switch connectivity.
- Active health system log analyzer**  
Upload and analyze AHS logs for a server not connected to Compute Ops Management.
- Approval policies**  
Specify actions that will require an approval to execute on specified groups.

3. Take notice of some of the settings in the Name column and also the Type column associated with each setting. HPE provides some pre-defined settings based on HPE ProLiant UEFI Workload Profiles. These settings are popular with administrators using HPE best practices for workloads like virtualization.

**Manage**

## Settings

Name	Category	Type	Groups
Decision Support	BIOS/Workload profile	HPE pre-defined	0 ...
General Peak Frequency Compute	BIOS/Workload profile	HPE pre-defined	0 ...
General Power Efficient Compute	BIOS/Workload profile	HPE pre-defined	0 ...
General Throughput Compute	BIOS/Workload profile	HPE pre-defined	0 ...
Graphic Processing	BIOS/Workload profile	HPE pre-defined	0 ...
High Performance Compute (HPC)	BIOS/Workload profile	HPE pre-defined	0 ...
I/O Throughput	BIOS/Workload profile	HPE pre-defined	0 ...
ILO settings enabled for security	ILO	HPE pre-defined	0 ...
Low Latency	BIOS/Workload profile	HPE pre-defined	0 ...
Mission Critical	BIOS/Workload profile	HPE pre-defined	0 ...
Transactional Application Processi...	BIOS/Workload profile	HPE pre-defined	0 ...
Virtual Radio Access Network (vRA...	BIOS/Workload profile	HPE pre-defined	0 ...
Virtualization - Max Performance	BIOS/Workload profile	HPE pre-defined	0 ...
Virtualization - Power Efficient	BIOS/Workload profile	HPE pre-defined	0 ...

4. Now click on **Create setting**.

The screenshot shows the 'Settings' page under the 'Manage' section. A red arrow points to the 'Create setting' button at the top right of the table header. To the right of the table, there is a sidebar titled 'Activity' listing various server events.

Name	Category	Type	Groups
Decision Support	BIOS/Workload profile	HPE pre-defined	0
General Peak Frequency Compute	BIOS/Workload profile	HPE pre-defined	0
General Power Efficient Compute	BIOS/Workload profile	HPE pre-defined	0
General Throughput Compute	BIOS/Workload profile	HPE pre-defined	0
Graphic Processing	BIOS/Workload profile	HPE pre-defined	0
High Performance Compute (HPC)	BIOS/Workload profile	HPE pre-defined	0
I/O Throughput	BIOS/Workload profile	HPE pre-defined	0
iLO settings enabled for security	iLO	HPE pre-defined	0
Low Latency	BIOS/Workload profile	HPE pre-defined	0
Mission Critical	BIOS/Workload profile	HPE pre-defined	0
Team06-Firmware	Server firmware	User defined	1
Team06-OS Image	Server operating system image	User defined	1
Team06-Storage	Server internal storage	User defined	0
Transactional Application Processi...	BIOS/Workload profile	HPE pre-defined	0
Virtual Radio Access Network (vRA...	BIOS/Workload profile	HPE pre-defined	0
Virtualization - Max Performance	BIOS/Workload profile	HPE pre-defined	1
Virtualization - Power Efficient	BIOS/Workload profile	HPE pre-defined	0

5. On the Server setting details page, **enter your Team name with -Firmware** appended to it. Also **enter your team's name in as a Description**. Finally pick the **Category of Firmware** from the pull-down box.

Step 1

## Setting details

Name\*

Description

Category\*

Select a category for this setting

Select

- Server firmware
- Server internal storage
- Server operating system image
- Server external storage
- OneView appliance settings
- OneView Synergy appliance settings
- OneView VM server templates

Next →

6. Click **Next** to continue.
7. Now in step two of the process, **use the pull-down menu in the Gen10/+ and Gen11 section** to select the latest versions of SPP and the latest patch bundles if available.

Step 2 of 2

### Firmware baseline setting

[Learn about firmware baselines](#)

**Gen10/+ baseline**

Choose a base SPP bundle

2024.04.00.00 \*latest base SPP available ▾

Patch bundle associated with SPP 2024.04.00.00

2024.04.00.01 \*latest patch available ▾

Baseline Patch 2024.04.00.01 + SPP  
reference 2024.04.00.00 (27 May 2024)

**Gen11 baseline**

Choose a base SPP bundle

2024.04.00.00 \*latest base SPP available ▾

Patch bundle associated with SPP 2024.04.00.00

2024.04.00.01 \*latest patch available ▾

Baseline Patch 2024.04.00.01 + SPP  
reference 2024.04.00.00 (27 May 2024)

**2024.04.00.01 patch bundle**

Released: 27 May 2024  
Base SPP of patch: 2024.04.00.00

Description

Patch bundle version 2024.04.00.01 is an update over Gen10/Gen10 Plus SPP version 2024.04.00.00 release including iLOS 3.04 along with support for RHEL 9.4.

[Learn more](#)

**2024.04.00.01 patch bundle**

Released: 27 May 2024  
Base SPP of patch: 2024.04.00.00

8. Now select **Finish and create server setting**.

Step 2 of 2

### Firmware baseline setting

[Learn about firmware baselines](#)

**Gen10/+ baseline**

Choose a base SPP bundle

2024.04.00.00 \*latest base SPP available ▾

Patch bundle associated with SPP 2024.04.00.00

2024.04.00.01 \*latest patch available ▾

Baseline Patch 2024.04.00.01 + SPP  
reference 2024.04.00.00 (27 May 2024)

**Gen11 baseline**

Choose a base SPP bundle

2024.04.00.00 \*latest base SPP available ▾

Patch bundle associated with SPP 2024.04.00.00

2024.04.00.01 \*latest patch available ▾

Baseline Patch 2024.04.00.01 + SPP  
reference 2024.04.00.00 (27 May 2024)

**2024.04.00.01 patch bundle**

Released: 27 May 2024  
Base SPP of patch: 2024.04.00.00

Description

Patch bundle version 2024.04.00.01 is an update over Gen10/Gen10 Plus SPP version 2024.04.00.00 release including iLOS 3.04 along with support for RHEL 9.4.

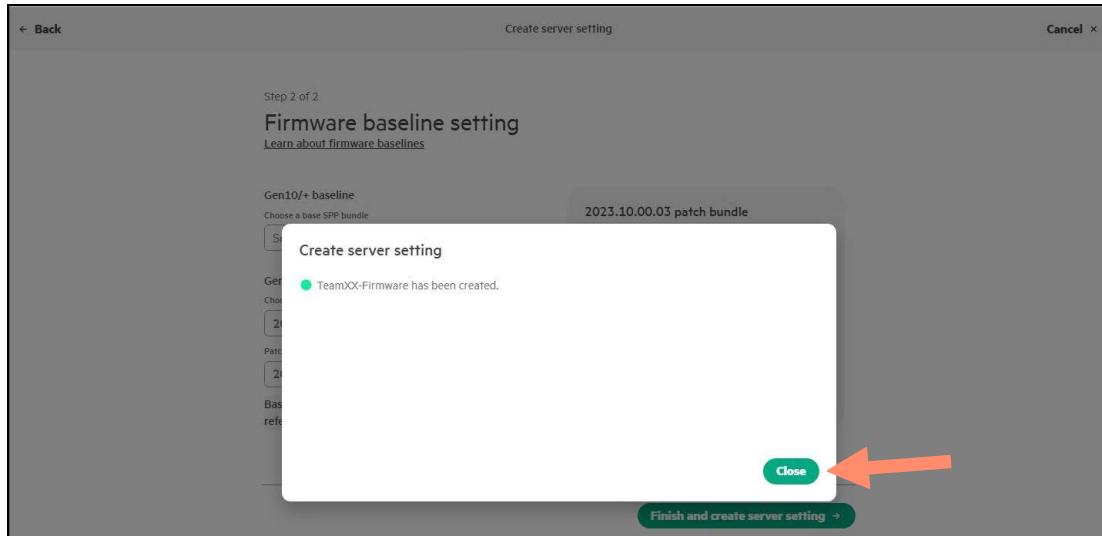
[Learn more](#)

**2024.04.00.01 patch bundle**

Released: 27 May 2024  
Base SPP of patch: 2024.04.00.00

**Finish and create server setting →**

9. You should see the setting for firmware successfully created. Click on **Close** to finish the process.



10. The next two settings we will look to add to our Server Group in the next section of the Lab is a **HPE Pre-Defined BIOS/Workload profile** and the most important setting **iLO settings enabled for security**. Click on these to find out more.

The screenshot shows a 'Settings' page with a list of server profiles. The columns are: Name, Category, Type, and Groups. The 'Name' column is sorted by name. The 'iLO settings enabled for security' row is highlighted with a red box. The 'Create setting' button is located at the top right of the table area.

Name	Category	Type	Groups
25-Firmware	Server firmware	User defined	0 ...
Decision Support	BIOS/Workload profile	HPE pre-defined	0 ...
General Peak Frequency Compute	BIOS/Workload profile	HPE pre-defined	0 ...
General Power Efficient Compute	BIOS/Workload profile	HPE pre-defined	0 ...
General Throughput Compute	BIOS/Workload profile	HPE pre-defined	0 ...
Graphic Processing	BIOS/Workload profile	HPE pre-defined	0 ...
High Performance Compute (HPC)	BIOS/Workload profile	HPE pre-defined	0 ...
I/O Throughput	BIOS/Workload profile	HPE pre-defined	0 ...
iLO settings enabled for security	iLO	HPE pre-defined	0 ...
Low Latency	BIOS/Workload profile	HPE pre-defined	0 ...
Mission Critical	BIOS/Workload profile	HPE pre-defined	0 ...
Transactional Application Processi...	BIOS/Workload profile	HPE pre-defined	0 ...
Virtual Radio Access Network (vRA...	BIOS/Workload profile	HPE pre-defined	0 ...
Virtualization - Max Performance	BIOS/Workload profile	HPE pre-defined	0 ...
Virtualization - Power Efficient	BIOS/Workload profile	HPE pre-defined	0 ...

The **iLO settings enabled for Security** setting can be used to apply HPE recommended iLO security settings to reduce the overall security risk of a server:

The screenshot shows a configuration interface for an 'iLO settings enabled for security' profile. At the top left is a back arrow labeled 'Settings'. The title 'iLO settings enabled for security' is centered above a 'Details' section. Below 'Details' are four entries: 'Description' (This profile applies the HPE recommended security settings. When applied, this policy reduces the overall security risk of a server.), 'Used by' (--), 'Category' (iLO), and 'Type' (HPE pre-defined). A horizontal line separates this from the 'iLO settings' section. The 'iLO settings' section contains a table with seven rows, each showing a setting name, its category, and its value. The table has three columns: 'Setting', 'Category', and 'Value'.

Setting	Category	Value
Require login for iLO RBSU	Security access - iLO	Enabled
SNMPv1 request	SNMP - SNMP alert	Disabled
IPMI/DCMI over LAN	Security access - Network	Disabled
Authentication failure logging	Security access - Account service	Enabled - Every 3rd Failure
Password complexity	Security access - Account service	Enabled
Minimum password length	Security access - Account service	8
Global component integrity	Security access - iLO	Enabled

This concludes this section of the lab.

## Creating server groups and associating server settings

Server groups allow you to organize servers based on specific criteria (e.g., location, function, or role). When you create or edit a server group, you can apply server settings and server group policies. Servers directly managed by HPE Compute Ops Management can be added to server groups where these settings will be applied to all the systems in the group.

- Now return to the **Manage** tab in HPE Compute Ops Management and this time select **Groups**.

The screenshot shows the 'Manage' tab in the HPE Compute Ops Management interface. The 'Groups' section is highlighted with an orange arrow. Other sections visible include 'Metrics data collection', 'Data Services Cloud Console integration', 'ServiceNow integration', and 'Aruba Central integration'.

- At the **Groups** page, click on **Create a group**.

The screenshot shows the 'Groups' page in the HPE Compute Ops Management interface. A callout bubble points to the 'Create a group' button, which is highlighted with an orange arrow. The page also includes a message: 'Let's get started by creating a group.'

3. In the Group details section, **enter your Team name** in the Name field and **then again for the Description field**. Select **Server** as the type, then click on **Next** to continue in the wizard.

Step 1 of 4

## Group details

Name\*

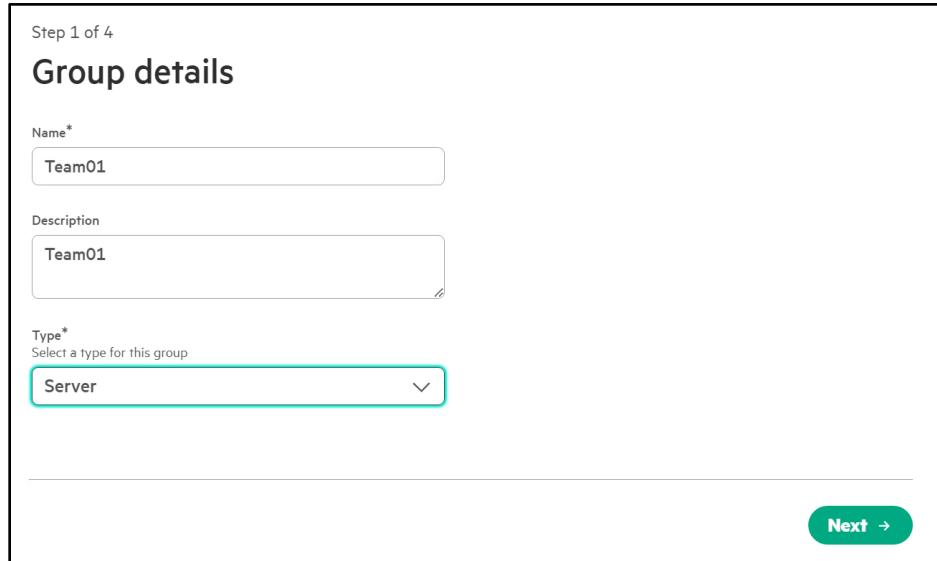
Description

Type\*

Select a type for this group

Server

**Next →**



4. In the next screen of the wizard, **use the pulldown menu** to **choose** your previously created **Firmware setting**.

Step 2 of 4

## Server settings (optional)

[Learn about settings for a group](#)

Choose a firmware server setting

Select

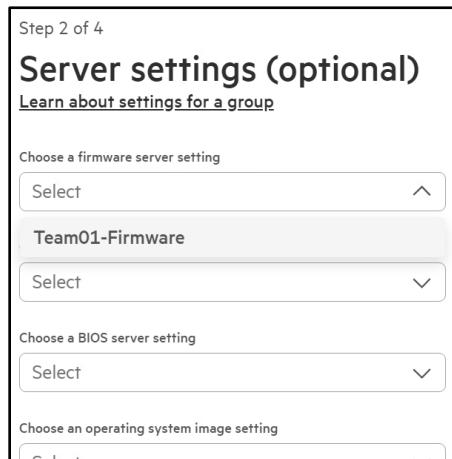
Team01-Firmware

Select

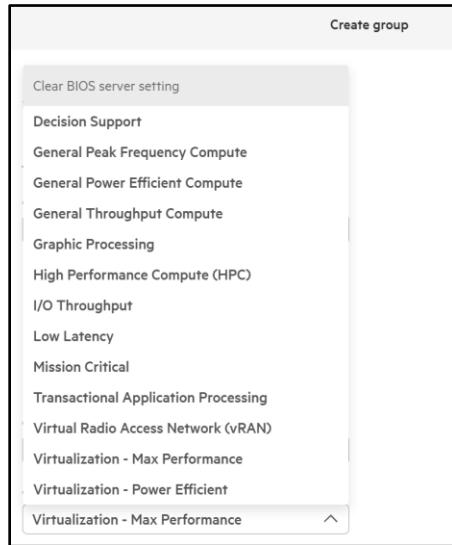
Choose a BIOS server setting

Select

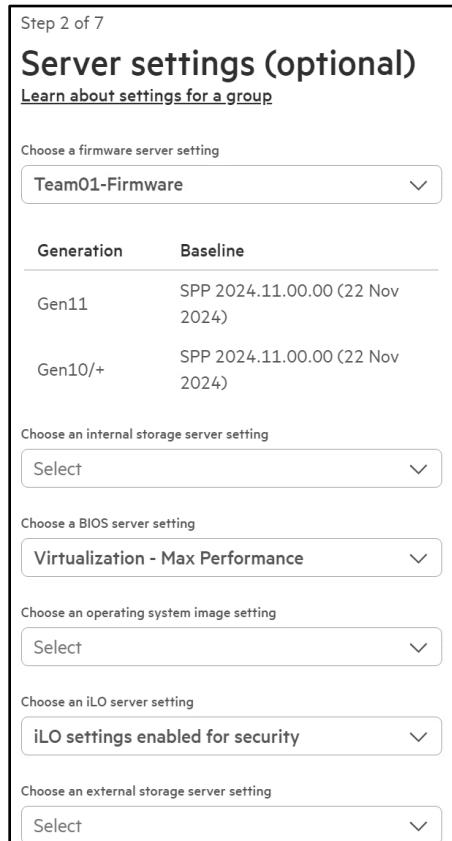
Choose an operating system image setting



5. In the section, to **choose a BIOS server setting**, choose a setting that meets the needs of the customer.



6. In the section **Choose an iLO server setting** box select **iLO settings enabled for security**.



7. Leave the rest of the options in this initial section at their default values, and then select **Next** to advance in the wizard.
  
8. Normally we would enable the Auto apply, but for the purpose of this Lab we will leave it **disabled**.

Step 3 of 7

## Firmware server setting policies (optional)

[Learn about group policies](#)

**Firmware baseline setting**

**Team1-Firmware**

Generation	Baseline
Gen11	SPP 2024.11.00.00 (22 Nov 2024)
Gen10+/-	SPP 2024.11.00.00 (22 Nov 2024)

**Policies**

**Downgrade components to match baseline**  
 If this policy is enabled, any component version higher than the baseline will be downgraded to match the baseline. This affects how compliance is calculated. [Learn more](#)

**Downgrade components to match baseline**

**Auto apply firmware baseline when server is added to the group**  
 When a server is added to the group, the specified baseline is applied immediately if the server is activated or when the server is activated at a later time.

**Auto apply firmware baseline**

**2024.11.00.00 base SPP bundle**

**Released:** 22 Nov 2024

**Description**

Gen11 SPP 2024.11.00.00 SPP supports Gen11 Intel and AMD based Server Platforms and Options. This release supports newer Gen11 servers based on 5th generation AMD EPYC Processors.

[Learn more](#)

**2024.11.00.00 base SPP bundle**

**Released:** 22 Nov 2024

**Description**

Gen10/Gen10 Plus SPP 2024.11.00.00 release supersedes Gen10/Gen10 Plus SPP 2024.09.00.00 and includes support for Red Hat Enterprise Linux 9.5.

[Learn more](#)

**Next →**

9. Click **Next** to continue.

10. **Enable** the Auto apply BIOS settings policy and then select **Next**.

Step 4 of 7

## BIOS server setting policies (optional)

[Learn about group policies](#)

**BIOS setting**

[Virtualization - Max Performance](#)

**Policies**

Auto apply BIOS setting when server is added to the group  
When a server is added to the group, the specified BIOS setting is applied immediately if the server is activated or when the server is activated at a later time.

Auto apply BIOS setting

Reset BIOS configuration settings to defaults when server is added to the group  
Reset server's BIOS settings to default values before applying the BIOS setting.

Reset BIOS configuration settings to defaults

**Next →**

11. For **auto applying the iLO Setting**, leave this **disabled** for now so we can **manually apply this later** in the Lab, click **Next** to continue.

Step 5 of 7

## iLO settings policy (optional)

[Learn about group policies](#)

**iLO setting**

[iLO settings enabled for security](#)

**Policy**

Auto apply iLO setting when server is added to the group

Auto apply iLO setting

**iLO settings enabled for security**

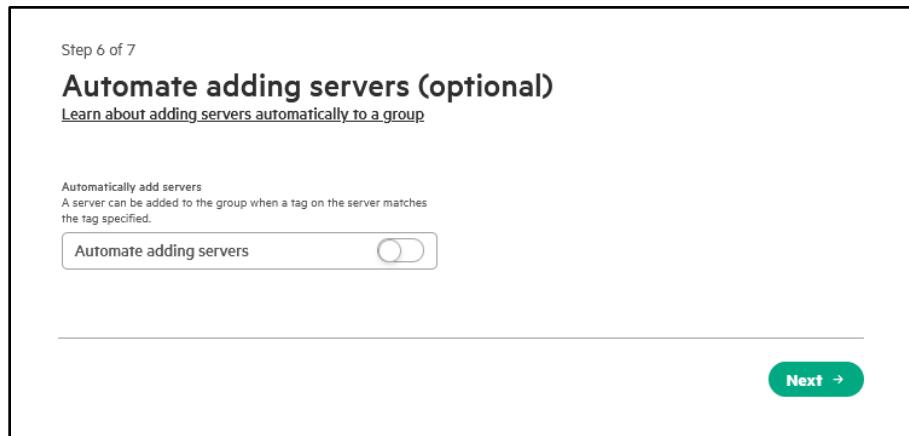
**Description**

This profile applies the HPE recommended security settings. When applied, this policy reduces the overall security risk of a server.

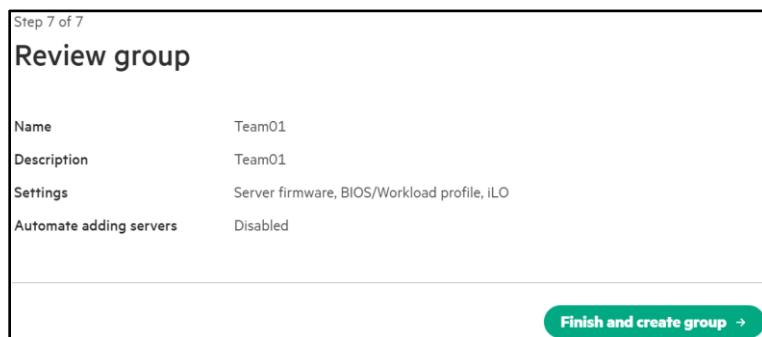
[Learn more](#)

**Next →**

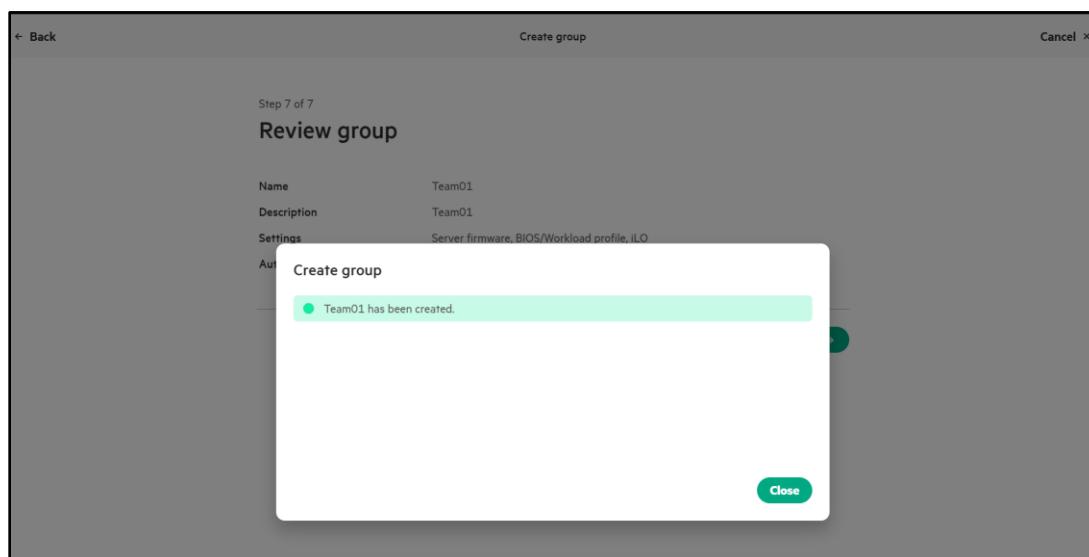
12. For the question of how we are adding our servers to the group, we are going to setup the group for manual addition of servers to the group. Select **Next** to move to the finish.



13. At the last step, review the areas you have settings defined and then select **Finish and create group**.



14. The group should be created, and you can click on **Close** to finish the process.



15. Now within the Groups section, you can select your Server group. Click the **Hyperlink** for your **Team Name**.

Health	Name	Type	Security	Devices	Settings	Compliance	Job state	
●	Team01	Server	Unknown	0	3	Not applicable	No active job in progress	...

16. Scroll through the details of your server group and take note of the Compliance section. This will help administrators understand if any configuration drift occurs in the future.

### Team01

0 servers

#### Details

Group health	● OK
Type	Server
Description	Team01
Job state	No active job in progress

#### Health

Critical	◆ 0 servers
Warning	▲ 0 servers
Normal	● 0 servers
Unknown	■ 0 servers
Disabled	□ 0 servers

#### Scheduled actions

No actions have been scheduled

#### iLO security

At risk	◆ 0 servers
Ignore risk	▲ 0 servers
OK	● 0 servers
Unknown	■ 0 servers
Unsupported	□ 0 servers

17. Scroll down to **Settings and compliance**. These are the details of what you just defined at the group level.

### Settings and compliance

ⓘ This group's compliance is 'Not applicable.' [View details](#)

Server firmware	<a href="#">Team01-Firmware</a>
BIOS/Workload profile	<a href="#">Virtualization - Max Performance</a>
iLO	<a href="#">iLO settings enabled for security</a>

### External storage server settings

External storage setting not set

### Group policies

Server firmware

Policy	Setting
Downgrade components to match baseline	Disabled
Auto apply firmware baseline when server is added to the group	Enabled
Power off server after firmware update	Disabled

BIOS/Workload profile

Policy	Setting
Auto apply BIOS setting when server is added to the group	Enabled

iLO

Policy	Setting
Auto apply iLO settings when server is added to the group	Disabled

18. Scroll back up to the top of the page and click on the **Actions** button (to the right of the frame) to reveal how functions are performed on the entire group.

19. Click **Add servers**.

< Groups

### Team01

0 servers

Details

Group health	<span style="color: green;">● OK</span>
Type	Server
Description	Team01
Job state	No active job in progress

Health

Critical	<span style="color: red;">◆</span> 0 servers
Warning	<span style="color: orange;">▲</span> 0 servers
Normal	<span style="color: green;">●</span> 0 servers
Unknown	<span style="color: grey;">■</span> 0 servers
Disabled	<span style="color: grey;">□</span> 0 servers

Actions ▾
 

- Edit
- Delete
- Recover
- View servers
- Add servers
- Remove servers
- Update firmware
- Check firmware compliance
- Check external storage compliance
- Check iLO settings compliance
- Apply BIOS settings
- Apply internal storage configuration
- Install operating system image
- Apply ILO settings
- Apply external storage configuration

20. **Select your server** by clicking the **checkbox** next to its name then click **Continue** to proceed to the summary.

**Add servers**  
[Learn more about group actions](#)

Select the servers to be added to Team01. The list includes servers not yet assigned to a group. The list does not include OneView servers, which cannot be added to a group.

	Name	Model
<input checked="" type="checkbox"/>	2M2946009Z	ProLiant DL160 Gen10

**Cancel**  **Continue**

21. Review the actions that will take place on your server before clicking **Add 1 server**.

**Add servers**  
[Learn more about group actions](#)

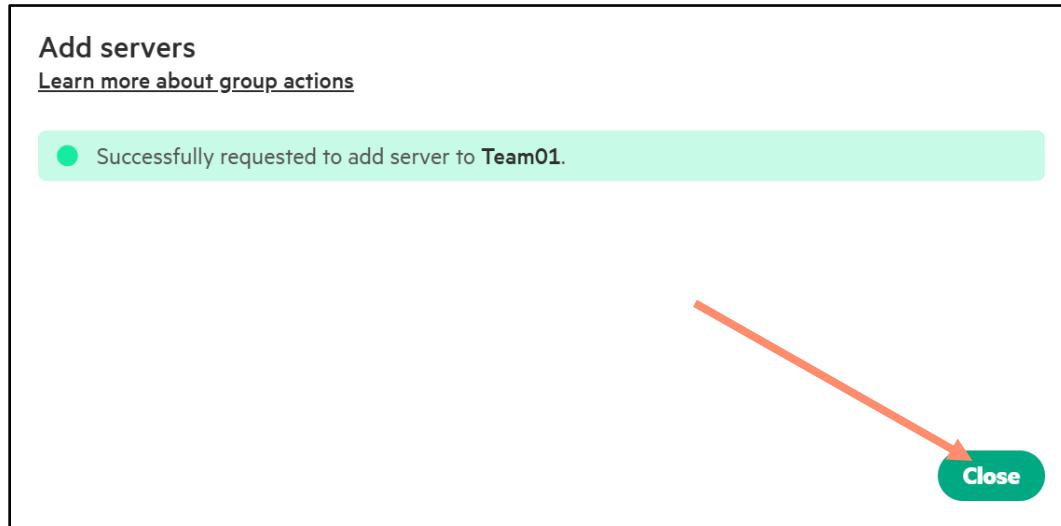
You are adding **1** server:

2M2946009Z

**▲** Team01 has a(n) **BIOS** automatic configuration policy enabled. The automatic configuration will begin soon after this add operation if the server is activated or when the server is activated at a later time.

**Cancel**  **Add 1 server**

22. Click **Close** to return to your team's server group.



23. The settings designated to automatically apply to servers as they are added to the group will be applied.

**Note the Recent group activity** pane and observe the actions as the settings are applied to your server.

Details	
Group health	● OK
Type	Server
Description	Team01
Job state	Group iLO Settings compliance in progress

Health	
Critical	0 servers
Warning	0 servers
Normal	1 server
Unknown	0 servers
Disabled	0 servers

Scheduled actions	
No actions have been scheduled	

**Recent group activity**

- Group iLO settings compliance  
Team01 iLO settings compliance state changed to Compliant  
1/28/2025 12:43:07 PM
- Group iLO settings compliance  
Team01 iLO settings compliance check in progress  
1/28/2025 12:43:04 PM
- Group firmware compliance  
Team01 firmware compliance state changed to Compliant  
1/28/2025 12:43:04 PM
- Server automatic configuration  
2M2946009Z automatic configuration is complete  
1/28/2025 12:42:33 PM

BIOS settings

This concludes this section of the lab.

## Advanced Security settings for iLO

HPE iLO6 (Integrated Lights-Out) provides robust security features to mitigate risks in networked environments. Feature like Trusted Platform Module (TPM) or TM Status, Local User Account Controls and Directory Group Account Controls that support Kerberos authentication or schema-free directory integration. You can set server name and FQDN/IP addresses yourself but consider leaving those values blank to let the host OS assign them. There are Secure Shell (SSH) Key Settings that can be managed for secure communication to the iLO6 management processor itself.

In this lab we will look at security parameters like in Network Settings where we can enable/disable various services (e.g., SSH, SNMP, Virtual Media.) We will configure anonymous data and IPMI/DCMI over LAN. Idle Connection Timeout values can be set.

While security is crucial, striking a balance between protection and usability is essential. Implement settings based on your organization's needs.

Finally, the iLO Security Dashboard provides real-time insights to monitor and manage security settings proactively.

1. Navigate back to your **assigned Servers iLO**.
2. From the iLO Information page, click on the **Security Dashboard** tab across the top of the page.

The screenshot shows the 'Information - Security Dashboard' for an iLO 6 system. The top navigation bar includes tabs for Overview, Security Dashboard (which is selected), Session List, iLO Event Log, Integrated Management Log, Security Log, Active Health System Log, and Diagnostics. The top right corner features several icons for power, network, and system status, along with a help icon.

The main content area displays the 'Overall Security Status : Risk' in a red header bar. Below it, the 'Security State' is listed as 'Production' and 'Server Configuration Lock' is shown as 'Disabled'. A table lists various security parameters with their current status (Risk or OK), state (Enabled, Disabled, or True), and an 'Ignore' button.

Security Parameter	Status	State	Ignore
Require Login for iLO RBSU	Risk	Disabled	<input type="button" value="Ignore"/>
Secure Boot	Risk	Disabled	<input type="button" value="Ignore"/>
Password Complexity	Risk	Disabled	<input type="button" value="Ignore"/>
SNMPv1	Risk	Enabled	<input type="button" value="Ignore"/>
Global Component Integrity	Risk	Disabled	<input type="button" value="Ignore"/>
Default SSL Certificate In Use	Risk	True	<input type="button" value="Ignore"/>
Security Override Switch	OK	OFF	<input type="button" value="Ignore"/>
IPMI/DCMI Over LAN	OK	Disabled	<input type="button" value="Ignore"/>
Minimum Password Length	OK	OK	<input type="button" value="Ignore"/>

3. Switch between browser tabs to return to Compute Ops Management. From your Server page in Compute Ops Management, the iLO Security Status shows at risk. Click on the **Details** link. Note that there is no yellow caution triangles currently ignored.

**iLO security status**

**>Password Complexity**  
The Password Complexity setting is disabled. This configuration increases system vulnerability to attack.  
**Recommendation:** Enable the "Password Complexity" setting.

**Require Login for ILO RBSU**  
Require Login for ILO RBSU setting is disabled. This configuration allows unauthenticated ILO access through the UEFI System Utilities.  
**Recommendation:** Enable the Require Login for ILO RBSU setting.

**SNMPv1**  
SNMPv1 is enabled. This configuration increases system vulnerability to attack.  
**Recommendation:** Disable SNMPv1 setting.

**Secure Boot**  
The UEFI Secure Boot setting is disabled. In this configuration, the UEFI system firmware does not validate the boot loader, Option ROM firmware, and other system software executing on the trusted signatures. This configuration breaks the chain of trust established by ILO base power-on.  
**Recommendation:** Enable the Secure Boot setting in the UEFI System Utilities.

**Ignore - 0**

**Configure iLO ignore risk setting**      Cancel

- 4.
5. Return to the iLO6 **Security dashboard** screen. Select the option for **SNMPv1** and toggle on the ability to **ignore the error**. This is not a best practice for the “real world”, but we are demonstrating the connection between your iLO6 and COM.

Security Parameter	Status	State	Ignore
Require Login for ILO RBSU	⚠️ Risk	Disabled	<input type="checkbox"/>
Secure Boot	⚠️ Risk	Disabled	<input type="checkbox"/>
Password Complexity	⚠️ Risk	Disabled	<input type="checkbox"/>
<b>SNMPv1</b>	⚠️ Risk	Enabled	<input checked="" type="checkbox"/>
Global Component Integrity	⚠️ Risk	Disabled	<input type="checkbox"/>
Default SSL Certificate In Use	⚠️ Risk	True	<input type="checkbox"/>

Note: This task can be easily automated using the **Enable-HPECOMIloIgnoreRiskSetting** cmdlet from the **HPECOMCmdlets** PowerShell module.

6. Back at the COM screens, you see that now we do have an error that is ignored.

**iLO security status**

Recommendation: Create the "iLO component integrity" setting.

**Password Complexity:**  
The Password Complexity setting is disabled. This configuration increases system vulnerability to attack.  
Recommendation: Enable the "Password Complexity" setting.

**Require Login for iLO RBSU:**  
The Require Login for iLO RBSU setting is disabled. This configuration allows unauthenticated iLO access through the UEFI Systems Utilities.  
Recommendation: Enable the Require Login for iLO RBSU setting.

**Secure Boot:**  
The UEFI Secure Boot setting is disabled; in this configuration, the UEFI system firmware does not validate the boot loader, Option ROM firmwares, and other system software executables for trusted signatures. This configuration breaks the chain of trust established by iLO after power-on.  
Recommendation: Enable the Secure Boot setting in the UEFI Systems Utilities.

**Ignore - 1**  
**SNMPv1:**  
SNMPv1 is enabled. This configuration increases system vulnerability to attack. The parameter risk is ignored.  
Recommendation: Disable SNMPv1 setting in iLO.  
Note: This risk was configured to be ignored on 06/11/2024, 2:31 PM CDT

**Configure iLO ignores risk setting**   **Cancel**

7. Return the environment to where it was when you started. We will now permanently fix the SNMPv1 error. Click on the browser tab that returns you to your iLO6 instance and **Management – SNMP Settings**.

**Management - SNMP Settings**

**SNMP Settings**

**SNMP Alerts**

Trap Source Identifier

iLO Hostname  
 OS Hostname

SNMPv1 Request  
 SNMPv1 Trap  
 SNMPv3 Request  
 SNMPv3 Trap  
 Cold Start Trap Broadcast

Periodic HSA Trap Configuration  
Disabled

**SNMP Settings**

System Location  
System Contact  
System Role  
System Role Detail  
Read Community 1  
Read Community 2  
Read Community 3  
Status  
Enabled  
SNMP Port  
161

**SNMPv3 Settings**

**Send Test Alert**   **Apply**

**Apply**

8. In the SNMP Alerts section, uncheck **SNMPv1 Request** and **SNMPv1 Trap**.

**SNMP Alerts**

Trap-Source Identifier  
 iLO Hostname  
 OS Hostname

SNMPv1 Request  
 **SNMPv1 Trap**

SNMPv3 Request

SNMPv5 Trap

Cold Start Trap Broadcast

Periodic HSA Trap Configuration  
 Disabled

**Send Test Alert** **Apply**

9. Click the **Apply** button.

10. Return to the **Security Dashboard** and validate that **SNMPv1** has been disabled.

Parameter	Status	State	Action
Require Login for iLO RBSU	Risk	Disabled	<input type="radio"/>
Secure Boot	Risk	Disabled	<input type="radio"/>
Password Complexity	Risk	Disabled	<input type="radio"/>
Global Component Integrity	Risk	Disabled	<input type="radio"/>
Default SSL Certificate In Use	Risk	True	<input type="radio"/>
Security Override Switch	OK	OFF	<input type="radio"/>
IPMI/DCMI Over LAN	OK	Disabled	<input type="radio"/>
Minimum Password Length	OK	OK	<input type="radio"/>
Authentication Failure Logging	OK	Enabled	<input type="radio"/>
Require Host Authentication	OK	Disabled	<input type="radio"/>
<b>SNMPv1</b>	OK	Disabled	<input type="radio"/>
Last Firmware Scan Result	OK	OK	<input type="radio"/>

11. Return to the Details page that you have loaded in Compute Ops Management. Note that SNMPv1 is no longer a risk.

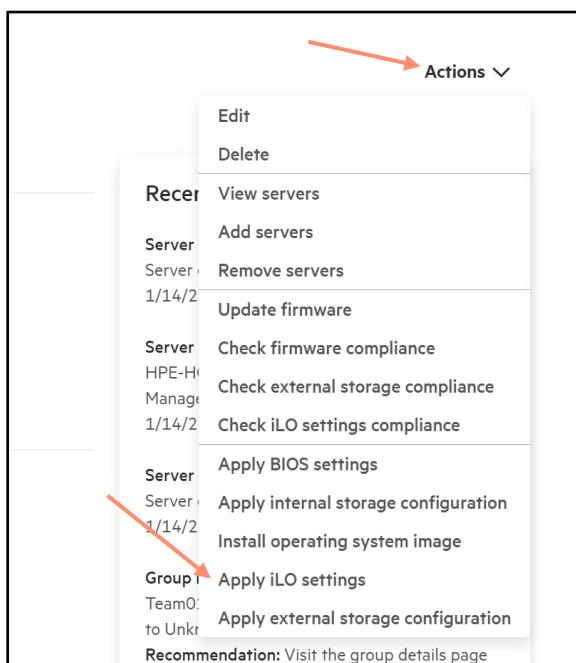
There are other items that need particular attention, such as Secure Boot and the use of self-signed certificates. These two are essential for iLO security. We will later cover how to generate a CA-signed certificate. For information on Secure Boot, you can refer to the [UEFI System Utilities User Guide for HPE Compute Gen10, Gen10 Plus Servers](#).

12. We will now utilize Compute Ops Management to push out all the recommended iLO Security Settings to our assigned Server. Let's click on **Manage** and then **Groups**.

13. Click on the **hyperlinked Name** of your **Group/Team**.

1 item						
Health	Name	Type	Security	Devices	Settings	Comp
●	<a href="#">Team01</a>	Server	At risk	1	3	Unknown

14. From the **Actions** drop down menu, select **Apply iLO Settings**.



15. To view the list of iLO settings that will be configured, click the **iLO settings enabled for security** link.

Step 1 of 2

### Select servers

Team01

[Learn more about applying iLO settings](#)

**iLO settings** [iLO settings enabled for security](#) (highlighted with a red box)

⚠ Global Component Integrity cannot be enabled on 1 of 1 servers as its only applicable on Gen11 servers.

Servers to apply settings on

1 items	
<input type="checkbox"/>	Name
<input type="checkbox"/>	HPE-HOL52

16. This list shows the **HPE recommended iLO settings** that will be pushed to our server to reduce the overall security risk:

Setting	Category	Value
Require login for iLO RBSU	Security access - iLO	Enabled
	SNMP - SNMP alert	Disabled
IPMI/DCMI over LAN	Security access - Network	Disabled
Authentication failure logging	Security access - Account service	Enabled - Every 3rd Failure
Password complexity	Security access - Account service	Enabled
Minimum password length	Security access - Account service	8
Global component integrity	Security access - iLO	Enabled

Note: Some iLO security settings might require a server reboot to take effect.

17. Click the **X** to close this popup.
18. Select your **assigned Server** from the list and hit **Next**.

Step 1 of 2

### Select servers

Team01

[Learn more about applying iLO settings](#)

iLO settings    [iLO settings enabled for security](#)

⚠ Global Component Integrity cannot be enabled on **1 of 1** servers as its only applicable on Gen11 servers.

Servers to apply settings on

1 items

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	HPE-HOL52

**Next →**

19. Review your changes, then hit **Apply iLO Settings**.

20. Hit **Close** on the pop up, to return to your Group details.

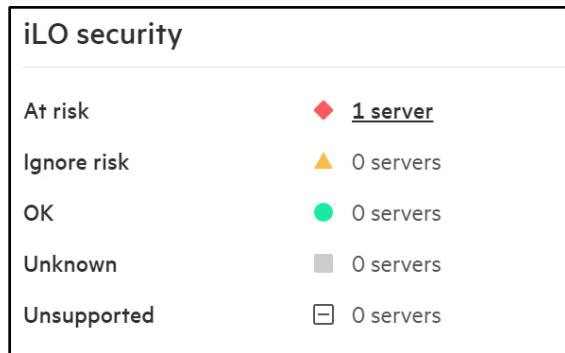


21. In the **Recent group Activity**, you should now see the **iLO settings being successfully applied** and the **settings compliance** changed to **Compliant**.

A screenshot of the "Recent group activity" section. It displays four log entries:

- Group iLO settings compliance**  
Team01 iLO settings compliance check successful  
1/15/2025 12:33:09 AM
- Group iLO settings compliance**  
Team01 iLO settings compliance state changed to Compliant  
1/15/2025 12:33:09 AM
- Group iLO settings**  
Team01 Apply iLO settings successful  
1/15/2025 12:32:08 AM
- Group iLO settings compliance**  
Team01 iLO settings compliance check in progress  
1/15/2025 12:32:08 AM

22. If we look to the **left of the screen**, we can see our **iLO Security** section still showing **At risk**. Let's click on the **hyperlink**.



23. On the right, click again to select the **Server at Risk**.



24. We will then be directed to the Details page for our assigned Server. Where **iLO security status** is seen, Click on **Details**.

Summary	Health	Firmware	Hardware	Storage
<b>Details</b>				
<b>State</b>	Connected			
<b>Group</b>	<u>Team01</u>			
<b>Connection type</b>	Direct			
<b>Model</b>	ProLiant DL325 Gen10 Plus			
<b>Serial number</b>	CN70461J1W			
<b>iLO security status</b>	◆ At risk		<a href="#">Details</a>	
<b>UUID</b>	34383350-3737-4E43-3730-3436314A3157			
<b>iLO IP address</b>	<u>172.30.231.109</u>			<a href="#">Remote console</a>

25. You should see **two items still at Risk**, both of these have **dependencies** outside of the COM deployed iLO settings which may require manual intervention to resolve.

◆ At risk - 2
◆ Needs attention - 2
<b>Default SSL Certificate In Use</b>
Management processor's default self-signed certificate is in use.
<b>Recommendation:</b> Import a certificate signed by a trusted certificate authority.
<b>Secure Boot</b>
The UEFI Secure Boot setting is disabled. In this configuration, the UEFI system firmware does not validate the boot loader, Option ROM firmware, and other system software executables for trusted signatures. This configuration breaks the chain of trust established by iLO from power-on
<b>Recommendation:</b> Enable the Secure Boot setting in the UEFI System Utilities.

26. In the next section of this Hands On Lab, we will be following steps to **Request and Apply a Signed Certificate** from a **trusted Certificate Authority**.

27. Return to the **iLO web browser** of your assigned Server.

28. Earlier in the lab, we created a new Administrator privileged User with a simple password. Let's go back to **Administration** and look at creating another new user.

	Login Name	User Name	Status	Actions
<input type="checkbox"/>	Administrator	Administrator	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>
<input type="checkbox"/>	TechEnablement	TechEnablement	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>
<input type="checkbox"/>	ReadOnly	ReadOnly	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>

29. Click **New** in the Local Users frame and enter the following settings to create your new user account.

<b>Login Name</b>	HPE_Admin1
<b>User Name</b>	HPE Admin1
<b>New Password</b>	hpent123
<b>Confirm Password</b>	hpent123
<b>Role</b>	Administrator

### Add Local User

User Information

Login Name	HPE_Admin1
User Name	HPE_Admin1
New Password	*****
Confirm Password	*****

User Permissions

Role	Administrator
Privileges	<input type="checkbox"/> select all <input checked="" type="checkbox"/> Login <input checked="" type="checkbox"/> Remote Console <input checked="" type="checkbox"/> Virtual Power and Reset <input checked="" type="checkbox"/> Virtual Media <input checked="" type="checkbox"/> Host BIOS <input checked="" type="checkbox"/> Configure iLO Settings <input checked="" type="checkbox"/> Administer User Accounts <input checked="" type="checkbox"/> Host NIC <input checked="" type="checkbox"/> Host Storage <input type="checkbox"/> Recovery Set
IPMI/DCMI Privilege based on above settings:	administrator
<input type="checkbox"/> Service Account	

**Add User**

30. When we implemented our **iLO Security Settings**, it forces any **new iLO Accounts** to meet **Password complexity requirements**. Your current user login is affected by the change.

The password you entered does not satisfy the password complexity requirements. Enter a password that includes three of the four password complexity requirements. For more information, see the online help.

**Add User**

31. Set the password as **HPESecurePasswOrd!** and then click **Add User**.

HPE provides the Security Dashboard for every iLO5 and iLO6 enabled platform and aggregates multiple platform's security status in HPE Compute Ops Management. For more information on HPE ProLiant Security visit [www.hpe.com/info/ilo](http://www.hpe.com/info/ilo) and view the HPE iLO 6 Security Technology Brief.

This concludes this section of the lab.

## iLO SSL Certificate Management

By default, iLO uses a self-signed certificate in SSL connections. While this allows for encrypted communication, it lacks the trust and verification provided by a Certificate Authority (CA). A CA-signed certificate is issued by a trusted third-party CA, which verifies the identity of the server (i.e. the iLO). This ensures that the communication is with a legitimate iLO device, significantly reducing the risk of man-in-the-middle (MITM) attacks where an attacker could intercept and alter the communication.

Using a CA-signed certificate on iLO provides several benefits:

- **Trust and Verification:** Ensures that both the client and server can verify each other's identity through a trusted CA.
- **Enhanced Security:** Prevents unauthorized entities from intercepting and misusing sensitive credentials.
- **Avoiding Security Warnings:** Browsers and other clients trust CA-signed certificates, avoiding confusing security warnings.

To enhance overall security and trust, it is recommended to configure iLO with a CA-signed certificate. An easy way to achieve this is by using iLO's support for obtaining and renewing SSL certificates automatically via the Simple Certificate Enrollment Protocol (SCEP) with the Microsoft Network Device Enrollment Service (NDES). To learn more, see [iLO Automatic certificate enrollment](#).

This method offers several key benefits over the manual method of using a Certificate Signing Request (CSR) and requesting a certificate from a Certificate Authority (CA). It significantly reduces administrative overhead by automating the process of certificate issuance and renewal, ensuring that certificates are always up-to-date without manual intervention. This automation minimizes the risk of service disruptions due to expired certificates and enhances security by regularly refreshing cryptographic keys. Additionally, it provides a scalable solution for managing certificates across a large number of devices, ensuring consistent and compliant security practices throughout the organization.

To learn more about NDES, see [Active Directory Certificate Services \(AD CS\): Network Device Enrollment Service \(NDES\)](#)

By default, this feature is disabled in iLO. In this section, we are going to enable it and configure automatic certificate enrollment in iLO to obtain a trusted SSL certificate signed by a CA.

If you are looking for information about how to do it manually, see [Generate CSR and Import an SSL Certificate](#).

1. The first step is to download the root CA certificate of the certificate enrollment server to secure the connection between the iLO and the SCEP server. Open a new **Web Browser Tab** and **navigate** to <https://holca01.hol.enablement.local/certsrv/>

This server is our internal lab Certificate Authority (CA) server, provided by Microsoft Active Directory Certificate Services.

2. Login with Username - **ENABLEMENT\ndes\_svc** and Password **Get-My-Cert!**

3. Click **Download a CA certificate.**

**Microsoft Active Directory Certificate Services – HOLCA01-CA** [Home](#)

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

4. Ensure **Base 64** is selected as the Encoding method and then click **Download CA certificate**.

**Microsoft Active Directory Certificate Services – HOLCA01-CA** [Home](#)

**Download a CA Certificate, Certificate Chain, or CRL**

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

**CA certificate:**

Current [HOLCA01-CA]

**Encoding method:**

DER  
 Base 64

[Install CA certificate](#)

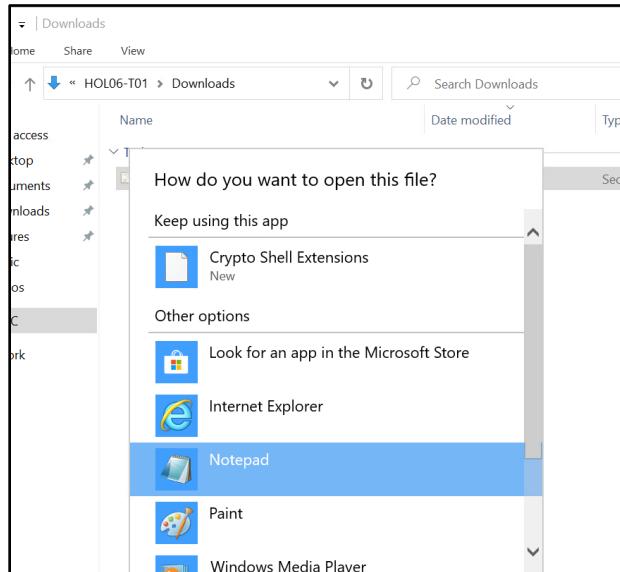
[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

5. **Open the Folder** where it was just saved to and then **open the file in Notepad**.



6. **Confirm any security warnings** and copy the entire content of the certificate. You can use **CTRL+A** to select all, then **CTRL+C** to copy. This will be used **later** in the process.

```

certnew - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIID1TCACan2gAwIBAgIQeqRM0+4TcbtB3bQaaLZOC DANBgkqhkiG9w0BAQsFADbd
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGjAYBgoJkiaJk/IzZAEZFgpIbmFibGVt
ZW50MRMwEQYKCZImiZPyLGQBGRYDaG9sMRMwEQYDVQQDEwpIT0xDQTAXLUNBMB4X
DT1MDiYODE1NDU0M1oXDTMwMDiYODE1NTU0M1owXTEVMBMGcgmSJomT8ixkARKw
BWxvY2FsMRowGAYKCZImiZPyLGQBGRYKZW5hYmx1bwVudDETMBEGCgmSJomT8ixk
ARKWA2hbDETMBEGA1UEAxMKSE9MQ0EwMS1DQTCASiwdQYJKoZIhvcNAQEBBQAD
ggEPADCCAQggEBAMT+oGS6ySKJZLoF9diGkjyDtwdWjv7g1KA4wsPTKDrHq4jz
91/86InTxulwtFSpoQ1cnT93BUBFVqHwb7dg4kR+ikuerhs4dUN2YegCh+uDmh
414hIwlauHjCejbzjZ12566AF08zh1TKRvNpok4P/0ZKtcnMTsrgYFkZyg@T6E5
YVR1RQ/uPsBzC1DXjwQSaZQr3hfOxzWj1R1DPm6dOsZC13F3ICBiZB4JzmxIwmY
ZHysffZmujnbnDh1fNymJNB5ZXJFvnZ8UmF+mW/1T4ctitOhLBZ45DfaJccD1zsUZ
mLGza1z9pexx5A2o/5XUawQz5CZJRKvP6oalpUCAwEAaNRME8wCwVDVR0PBAQD
AgGGMA8GA1udEwEB/wQFMAMBAf8wHQYDVR00BYEFIpNatd9MFbTy2ErXAB4sAf
DrDuMBAGC5sGAQQBgjcVAQDAGEMA0GCSqGSIb3DQEBCwUA41BAQAP5SPNsy8P
MWZ3ETgofkSwC8BoKrsbfgsaS7tC6psvQXUgWV33725WEthUSiXjom1tk2YEvlba
0JOXbJxF9Vt2ldBnRTi6XYwHxFLG2YS2bdCqtFeBe2F1LVKQv9zoCgE31qxBne
wjKFaa1p57EwCE9EkotfEibWvmb2Tcb77DQ9weGxmXnpts0QWssqdZlbiXSeg
11/8mx93SV9iFMdexvgyH2ZhTGz3UOPRwNgXXO3R0NTztCB/4KY1Tx+eZKLVUS1
cfdyAOjywPjIJQlvymae12kiy6mYMTam2e2jY7xZ5ZjP8TjOpTeOkuuZmAANDNG9
ZePebeHdi2Ne
-----END CERTIFICATE-----

```

Ln 1, Col 1

7. Next, you need to **retrieve** the **challenge password** from the certificate enrollment server – In a new tab navigate to [https://holca01.hol.enablement.local/certsrv/mscep\\_admin/](https://holca01.hol.enablement.local/certsrv/mscep_admin/)

**Network Device Enrollment Service**

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).

To complete certificate enrollment for your network device you will need the following information:

The thumbprint (hash value) for the CA certificate is: **C11BF096 51F4F0CE F65D752A 504D9636**

The enrollment challenge password is: **EBD8142CEBEB9D28**

This password can be used only once and will expire within 60 minutes.

Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password.

For more information see [Using Network Device Enrollment Service](#).

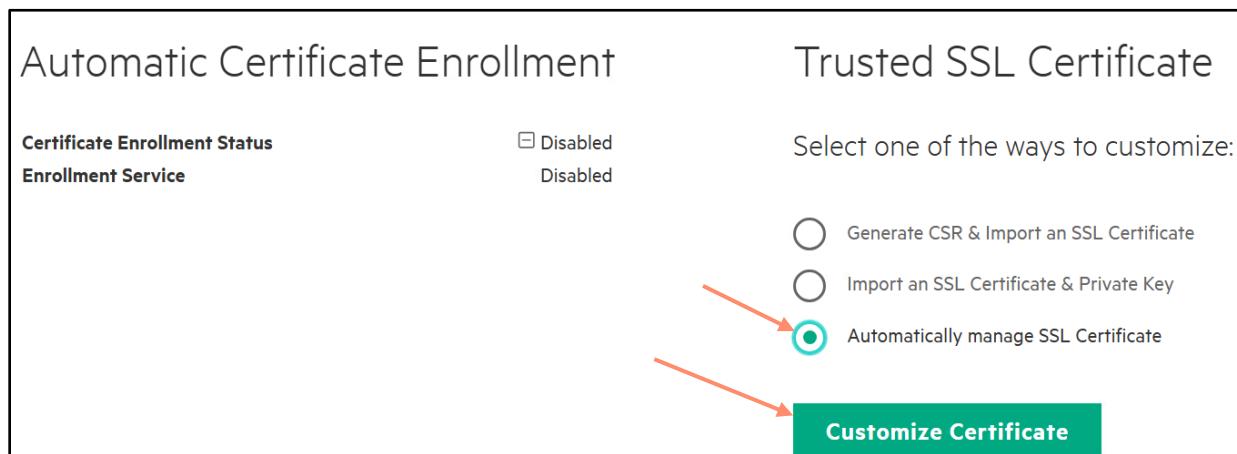
This URL is where you can obtain the challenge password that will be used later by the iLO to secure the connection with the NDES server during the certificate enrollment process. Note that the NDES server is the same as our internal lab CA server. Although this server plays both roles in our configuration, it is not mandatory to combine them, as it is possible to separate these two roles onto two different servers. The server must have the NDES role installed and be configured with a default certificate template that supports server authentication, compatible with iLO.

8. **Record** the **enrollment challenge password**, it will also be **required later** during the **setup** of the **iLO**.
9. We will now navigate back to our **iLO Web UI**, click on the **Security** menu on the left, then **SSL Certificate**.

The screenshot shows the iLO 5 interface with the following details:

- Left Sidebar:** Shows various system management options like Information, System Information, Compute Ops Management, Firmware & OS Software, ILO Federation, Remote Console & Media, Power & Thermal, Performance, ILO Dedicated Network Port, ILO Shared Network Port, Remote Support, Administration, Security (highlighted), Management, and Lifecycle Management.
- Top Bar:** Shows the date (5 Dec 21 2024) and navigation links for Access Settings, ILO Service Port, Secure Shell Key, Certificate Mapping, CAC/Smartcard, **SSL Certificate** (selected), Directory, and Encryption.
- SSL Certificate Information:**
  - Issued To:** CN = ILOM19460001.hol.enablement.local, O = Hewlett Packard Enterprise, OU = ILO, L = Americas, ST = Houston, C = US
  - Issued By:** CN = Default issuer (Do-not Trust), O = Hewlett Packard Enterprise, OU = ILO, L = Americas, ST = Houston, C = US
  - Valid From:** Jan 29 17:21:54 2023 GMT
  - Valid Until:** Jan 29 17:21:54 2040 GMT
  - Serial Number:** 0c8350Ac002e4x0b
- Automatic Certificate Enrollment:** Status: Enabled, Enrollment Service: Enabled.
- Trusted SSL Certificate:** Options: Generate CSR & Import an SSL Certificate, Import an SSL Certificate & Private Key, and **Automatically manage SSL Certificate** (selected).
- Customize Certificate:** A green button at the bottom right.

10. Note that the iLO currently uses a self-signed certificate, which is considered insecure. To correct this issue, we will enable Automatic Certificate Enrollment in iLO. Select **Automatically manage SSL Certificate** then click on **Customize Certificate**



11. Then enter:

1. Server URL: <https://holca01.hol.enablement.local/certsrv/mscep/mscep.dll>
2. Challenge password: type the enrollment challenge password recorded earlier
3. In the CA Certificate section, paste the content of the certificate you copied earlier from **Notepad**.
4. On the right side, leave the defaults CSR information and check the box for Include iLO IP Address(es)

**Certificate Enrollment Settings**

1	Server URL https://holca01.hol.enablement.local/certsrv/mscep/mscep.dll
2	Challenge Password .....
3	CA Certificate Name Not Loaded
CA Certificate SB3DQEBCwUA4IB AQCjyx3c80YK1RufPuKVMWYQUDthlEcdpBuefyLrJhSlmUnmayf BGC717REW8 09Hxm7wUIDb+qT9NECDDU93yGhXsnBS+s2yTLUFqW5SYQuKu OQiJfcXX0dfFHH3 N3V/YjeoFimib00QQ3Ohila8eABu0brwzb+kSiKU72jUEjwp9buo LGs4YKppkw VAQ5npkDQ78N3oWr2lf6hCOSHux4yNJ9HAL3lxnvb4n3eA8RraQ jexvoohX45ymR Y865rLINzupemytP2BfpUppoH+na4wXqtby1vBq9GfBdSc7KyvVt HaefLi97Rqq5 SQB8Jpaqtqw+TgHu0LeDwpmW -----END CERTIFICATE-----	
<input checked="" type="checkbox"/> Include iLO IP Address(es) <span style="float: right;">CA's will reject this field</span>	

**Enable**

12. Then click **Enable**.

13. To see the progress of the certificate enrollment status, refresh the page by clicking on the **SSL Certificate** tab.

**Automatic Certificate Enrollment**

Certificate enrollment service is enabled successfully. Refer to the Security logs page for more information.

<b>Certificate Enrollment Status</b>	<b>In Progress</b>
<b>Enrollment Service</b>	<b>Enabled</b>

Generation and renewal of SSL certificate will be managed automatically by the SCEP server. iLO will initiate the enrollment request to SCEP server by enabling the enrollment service and will obtain the trusted SSL certificate signed by the CA.

There are five steps to configure automatic certificate enrollment:

- Obtain the challenge password from the SCEP server
- Configure iLO with SCEP server and challenge password. Customize CSR subject fields
- Import the CA certificate of the SCEP server.
- Click on Enable to initiate Certificate Enrollment process
- Check Certificate Enrollment status and reset iLO

**Certificate Enrollment Settings**

Server URL: https://holca01.hol.enablement.local/certsrv/mscep/mscep.dll	Country (C) US
Challenge Password	State (ST) Texas
CA Certificate Name Not Loaded	City or Locality (L) Spring

14. If you get a **Failed** status, you can check the iLO Security logs in **Information / Security Log**. This is where SCEP activity is generated.

**Information - Security Log**

ID	Severity	Class	Description	Last Update	Count	Category
99	⚠️	Security Configuration	Unable to complete SSL certificate enrollment. Reason: Connectivity issues with SCEP server.	06/18/2025 16:58:09	1	Security, Administration, Configuration
98	ⓘ	Security Configuration	Certificate enrollment service is enabled.	06/18/2025 16:58:09	1	Security, Administration, Configuration
97	ⓘ	Security Configuration	Certificate enrollment configuration setting is changed.	06/18/2025 16:58:09	1	Security, Administration, Configuration
96	⚠️	Security Configuration	PCR Measurements Changed, Component Type BIOS PCR Index PCR14	06/18/2025 13:47:41	1	Security, Firmware, Maintenance
95	⚠️	Security Configuration	PCR Measurements Changed, Component Type BIOS PCR Index PCR13	06/18/2025 13:47:41	1	Security, Firmware, Maintenance
94	⚠️	Security Configuration	PCR Measurements Changed, Component Type BIOS PCR Index PCR12	06/18/2025 13:47:41	1	Security, Firmware, Maintenance
93	⚠️	Security Configuration	PCR Measurements Changed, Component Type BIOS PCR Index PCR11	06/18/2025 13:47:41	1	Security, Firmware, Maintenance

Note: If you face an enrollment failure, it is necessary to disable the certificate enrollment process by clicking on **Disable** before attempting a new enrollment.

## Automatic Certificate Enrollment

**Certificate Enrollment Status**

<span style="color: red;">*</span> Failed
Enabled

Generation and renewal of SSL certificate will be managed automatically by the SCEP server. iLO will initiate the enrollment request to SCEP server by enabling the enrollment service and will obtain the trusted SSL certificate signed by the CA.

There are five steps to configure automatic certificate enrollment:

- Obtain the challenge password from the SCEP server
- Configure iLO with SCEP server and challenge password. Customize CSR subject fields
- Import the CA certificate of the SCEP server.
- Click on Enable to initiate Certificate Enrollment process
- Check Certificate Enrollment status and reset iLO

### Certificate Enrollment Settings

Server URL <code>https://holca01.holenablement.local/certsrv/mscep/mscep.dll</code>	Country (C) US
Challenge Password	State (ST) Texas
CA Certificate Name <code>/C=US/ST=Texas/L=Spring/O=Hewlett Packard Enterprise/OU=HPE C</code>	City or Locality (L) Spring
CA Certificate	Organization Name (O) Hewlett Packard Enterprise
	Organizational Unit (OU) <small>optional</small> HPE Compute
	Common Name (CN) <code>ILOMXQ30809YN.holenablement.local</code>
	<input checked="" type="checkbox"/> <b>Include iLO IP Address(es)</b> <small>some CA's will reject this field</small>

**Update** **Disable**

15. A successful Certificate Enrollment will show as:

### SSL Certificate Information

<b>Issued To</b>	C = US, ST = Houston, L = Americas, O = Hewlett Packard Enterprise, OU = ISS, CN = ILO2M294600DF.hol.enablement.local
<b>Issued By</b>	DC = local, DC = enablement, DC = hol, CN = HOLCA01-CA
<b>Valid From</b>	Mar 4 05:31:41 2025 GMT
<b>Valid Until</b>	Mar 4 05:31:41 2026 GMT
<b>Serial Number</b>	7e:00:00:00:0c:ca:13:cd:0a:aa:8d:53:2e:00:00:00:00:0c

Remove

#### Automatic Certificate Enrollment

**Certificate Enrollment Status**

**Enrollment Service**

✓ Success  
Enabled

**Trusted SSL Certificate**

Select one of the ways to customize:

- Generate CSR & Import an SSL Certificate
- Import an SSL Certificate & Private Key
- Automatically manage SSL Certificate

Customize Certificate

16. Note that now the **iLO** uses a **trusted SSL certificate signed by our certificate authority server**:

### SSL Certificate Information

<b>Issued To</b>	C = US, ST = Houston, L = Americas, O = Hewlett Packard Enterprise, OU = ISS, CN = ILO2M294600DF.hol.enablement.local
<b>Issued By</b>	DC = local, DC = enablement, DC = hol, CN = <b>HOLCA01-CA</b>
<b>Valid From</b>	Mar 4 05:31:41 2025 GMT
<b>Valid Until</b>	Mar 4 05:31:41 2026 GMT
<b>Serial Number</b>	7e:00:00:00:0c:ca:13:cd:0a:aa:8d:53:2e:00:00:00:00:0c

17. But as indicated in the **security logs**, the iLO must be **reset** in order to **activate the new certificate**.

iLO 5
3.10 Dec 12 2024

X

#### Information - Security Log

Overview Security Dashboard Session List ILO Event Log Integrated Management Log **Security Log** Active Health System Log Diagnostics

ID	Severity	Class	Description	Last Update	Count	Category
181	<span style="color: green;">○</span>	Security Configuration	The security state of "ILO Default SSL Certificate In Use" parameter on security dashboard is "OK". State is "False" and ignore option is "False".	02/25/2025 14:51:35	1	Security, Administration, Configuration
180	<span style="color: green;">○</span>	Security Configuration	<b>SSL certificate enrollment is successful. Reset iLO to use the new certificate.</b>	02/25/2025 14:51:19	1	Security, Administration, Configuration
179	<span style="color: green;">○</span>	Security Configuration	Certificate enrollment service is enabled.	02/25/2025 14:51:16	1	Security, Administration, Configuration

18. From the **Information** screen, click on **Diagnostics** and then on **Reset**.

**iLO 5** 3.10 Dec 12 2024

**Information**

- System Information
- Compute Ops Management
- Firmware & OS Software
- iLO Federation
- Remote Console & Media
- Power & Thermal
- Performance
- iLO Dedicated Network Port
- iLO Shared Network Port
- Remote Support
- Administration
- Security
- Management
- Lifecycle Management

**Information - Diagnostics**

**iLO Self-Test Results**

**iLO Health:** ●

	↑ Status	Notes
Power Management Controller	○	Version 1.1.4
CPLD - PALO	○	ProLiant DL160 Gen10 System Programmable Log
NVRAM data	●	
Embedded Flash	●	
EEPROM	●	
Host ROM	●	
Supported host	●	
ASIC Fuses	●	Controller firmware revision 2.11.00

**Reset iLO**

All active connections to iLO are lost when you reset iLO. No configuration changes are made.

**Reset**

19. Give the iLO a **few minutes to reset**, then **open a new tab or browser** to login and confirm that the **connection** is now recognized as **secure** by the browser.

iLO: com-team01.hol.enableme... 10.18.22.151

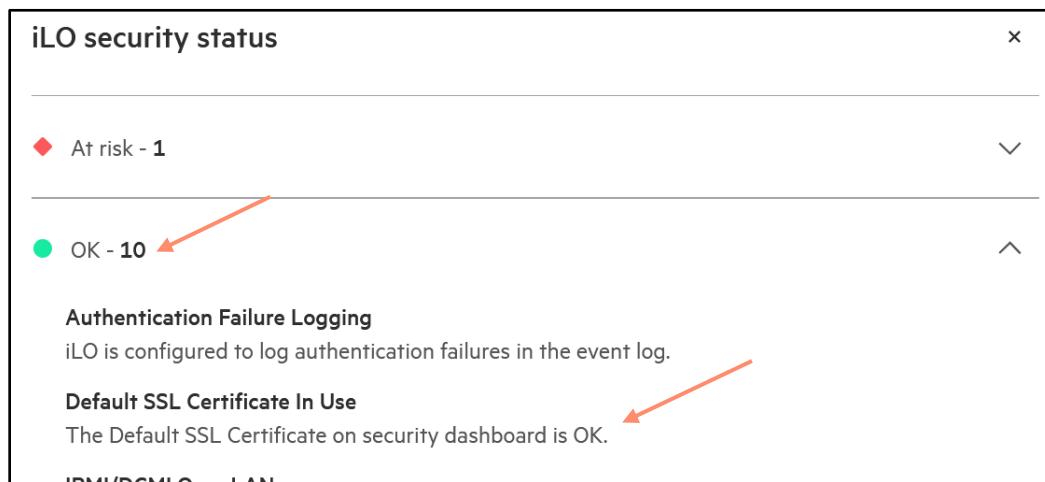
**Security** 10.18.22.151

**Connection is secure**  
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. [Learn more](#)

**Certificate is valid**

Note: For the setup to work end-to-end, the CA certificate must be added to the trusted root certificates of all client machines that connect to the iLO. In our lab environment, this process is automatically handled by our lab domain policy.

20. You can now circle back to **HPE Compute Ops Management** and check the **iLO Security Status**. The **Default SSL Certificate in Use** is now showing **Green**.



Note: This process can also be automated using PowerShell with this [script](#).

## HPE Compute Ops Management Secure Gateway

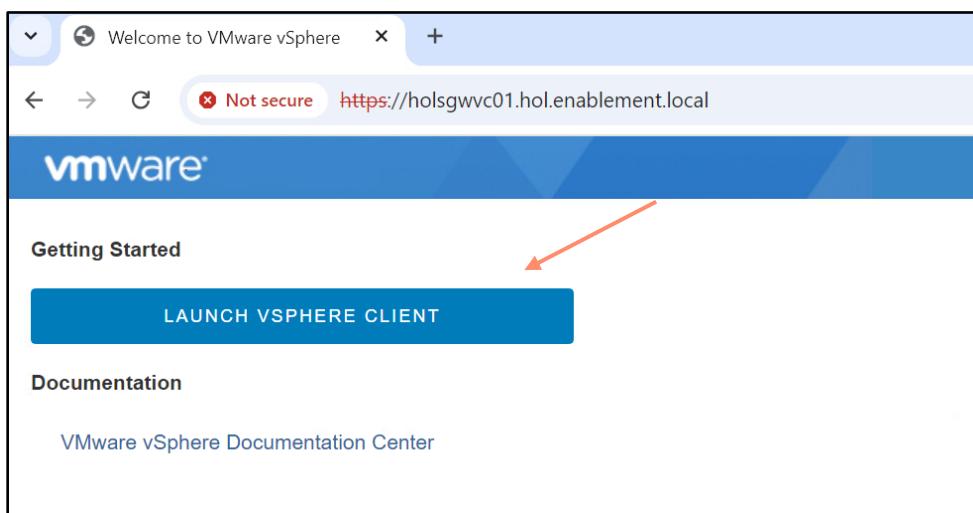
HPE Compute Ops Management customers can aggregate their on-premises HPE iLO connections over a single outbound connection to the management solution. Compute Ops Management secure gateway is an on-premises appliance deployed as a virtual machine.

It can aggregate HPE iLO connections from the customer data center over an outbound connection to Compute Ops Management. The feature helps eliminate the need to have each HPE iLO individually connected over the internet to Compute Ops Management.

### Deploying the Secure Gateway through VCenter

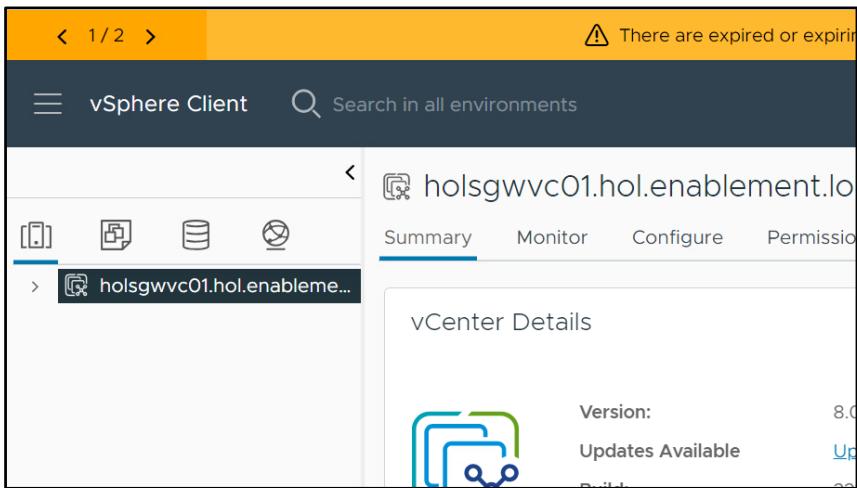
In this portion of the lab, we will focus on deploying an OVF Template supplied by HPE to provision the Virtual Machine Appliance which will function as the Secure Gateway for Compute Ops Management.

1. Open a fresh **Web Browser** or **Tab** and navigate to your VCenter Server at **holsgwvc01.hol.enablement.local**
2. **Confirm any Certificate Issues** to Proceed and then click **Launch vSphere Client**.

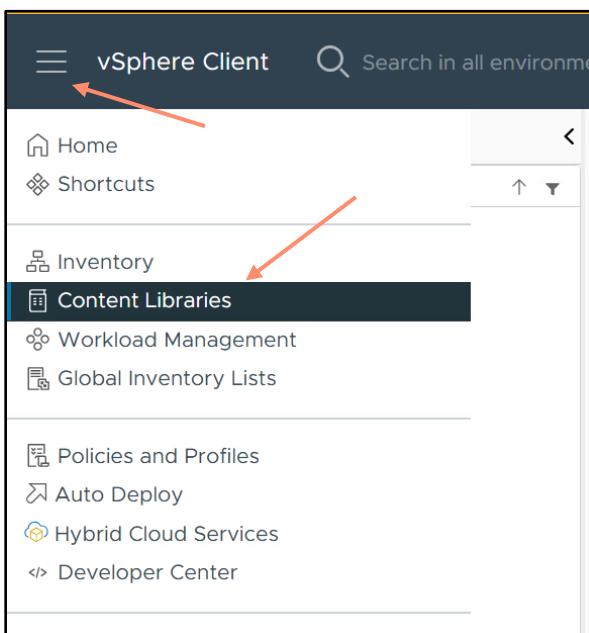


3. Use credentials **Administrator@vsphere.local** and **DiscOver2025!** as the password.

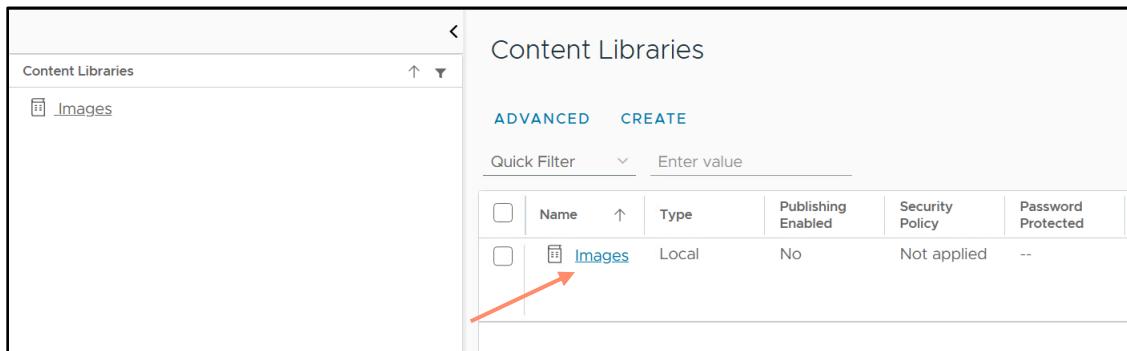
4. You should be now logged in to the vSphere Client



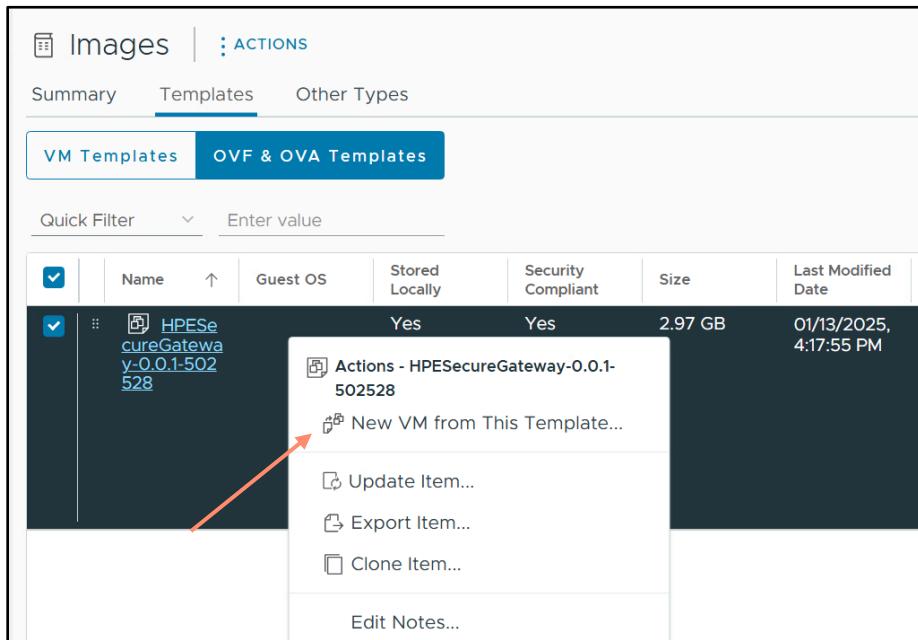
5. On the **left-hand side** of the screen, expand out the **vSphere Client menu**, and click on **Content Libraries**.



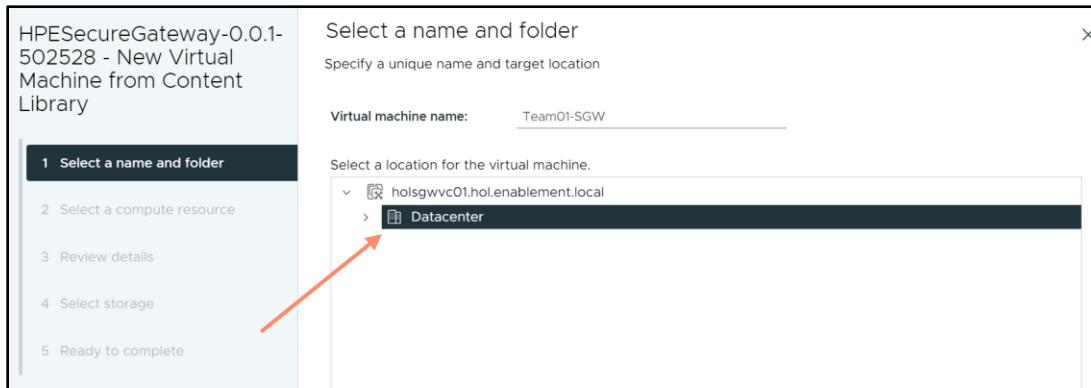
6. Click on **Images**.



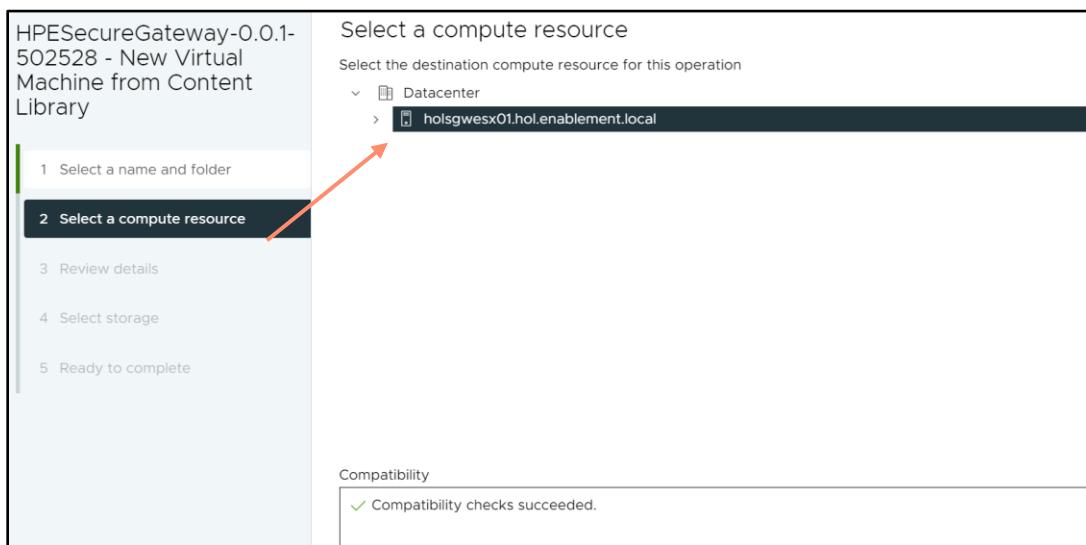
7. Right click on the **HPESecureGateway-X.X.X file** and select **New VM from This Template...**



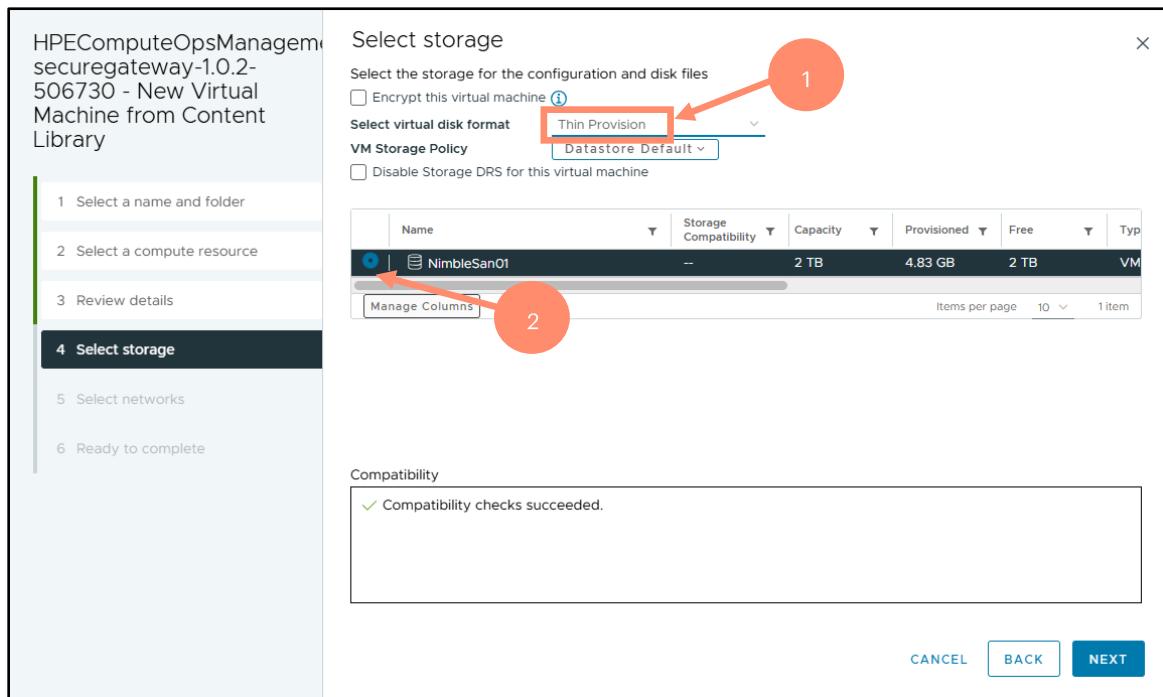
8. Set the Virtual Machine name as **TeamXX-SGW** where **XX** is your team number and select **Datacenter** as the location for the VM.



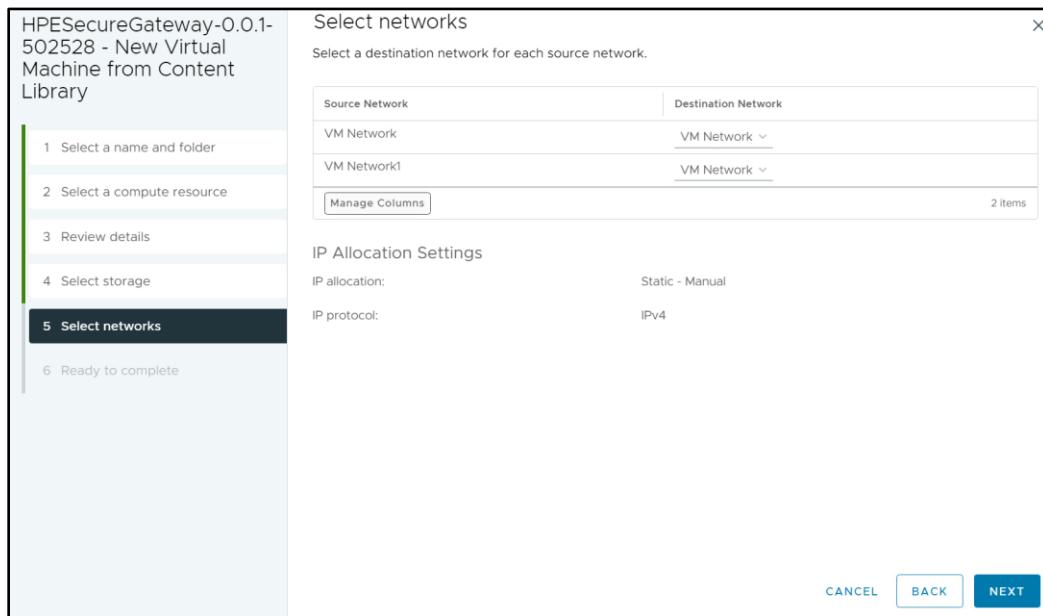
9. Click **holsgwesx01.hol.enablement.local** as the compute resource, then **Next** to proceed.



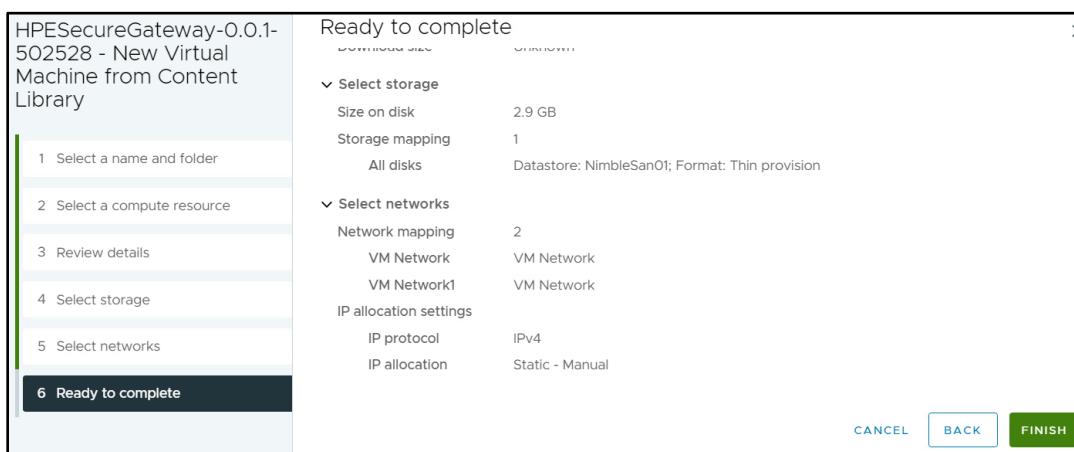
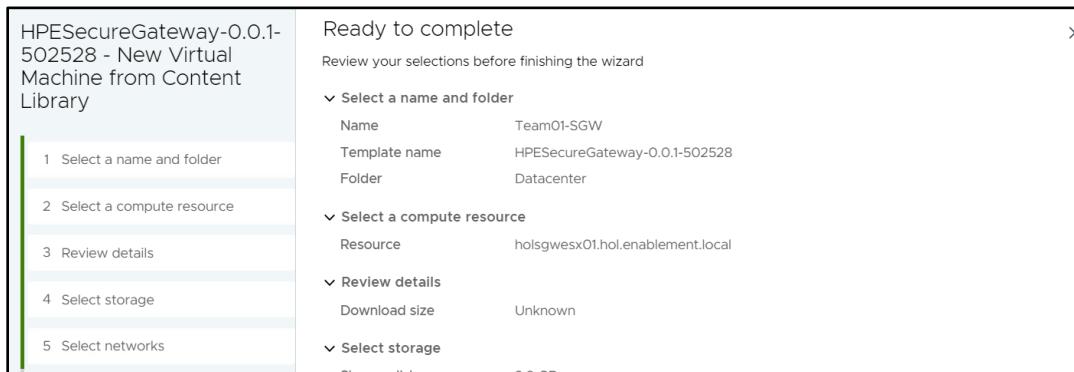
10. Click **Next** on **Review Details** and then for **Select Storage**, click **NimbleSan01**, change **Select virtual disk format** to **Thin Provision** and hit **Next**.



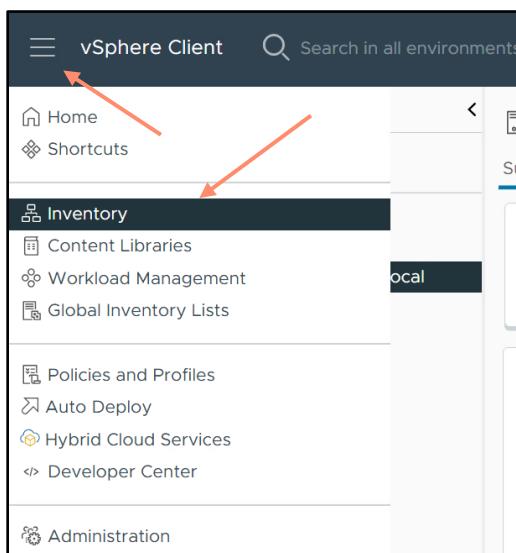
11. Leave the **defaults selected** for **Select Networks** and then **hit Next**.



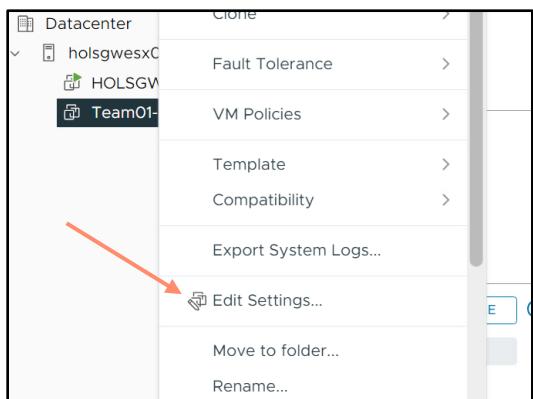
12. One last check and then hit **Finish** to complete the deployment.



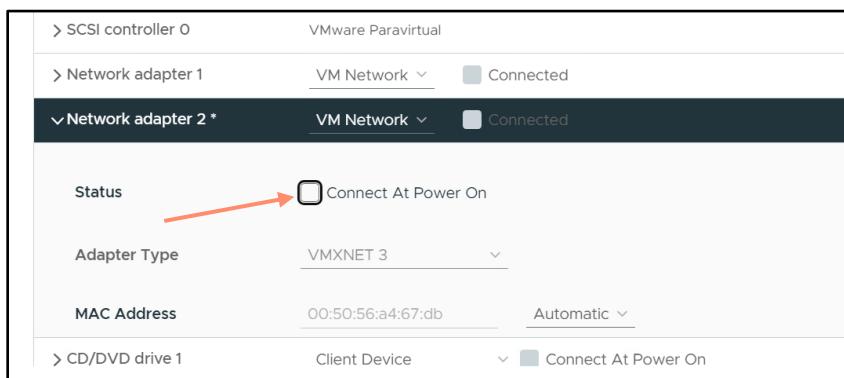
13. You can now navigate back to **Inventory Page** where you will see your **VM has been provisioned**.



14. Modify the network settings of the VM to use only one network interface. Right-click on your VM and select **Edit Settings**.



15. Expand **Network Adapter 2** and deselect **Connect At Power On** and then **OK** to confirm the change.

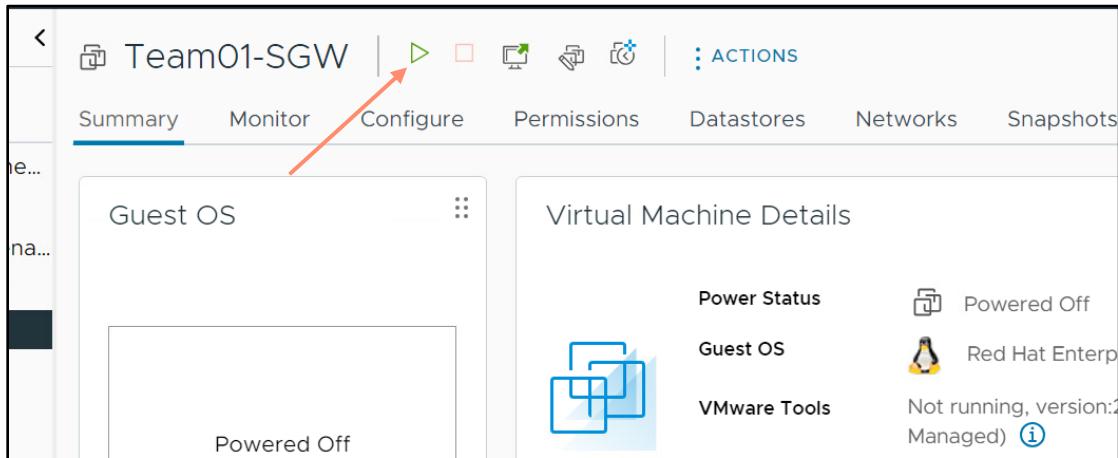


This concludes this section of the lab.

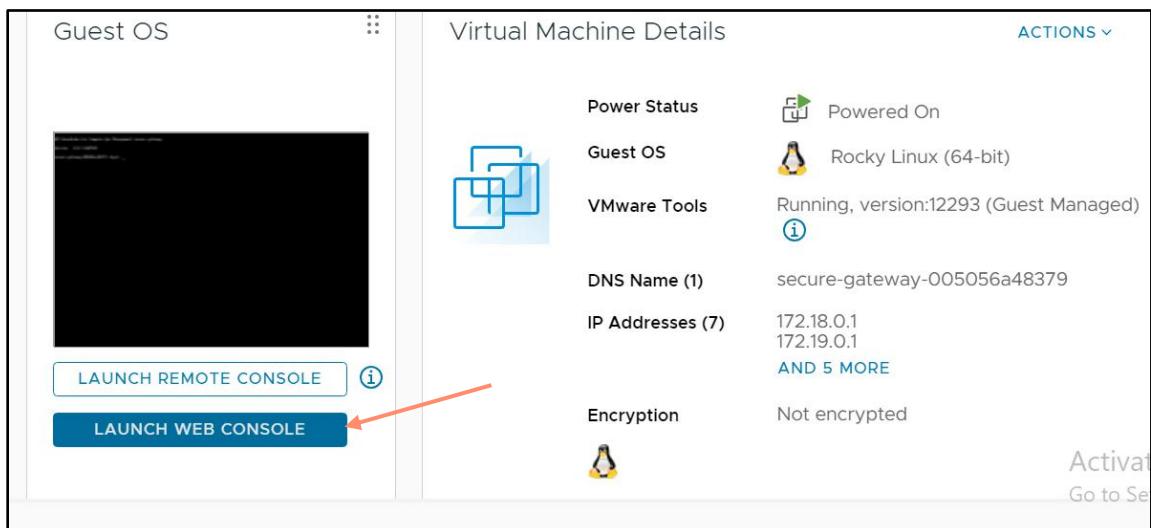
## Configuring the Secure Gateway and connecting to COM

In this portion of the lab, we will power on the VM, configure the Secure Gateway through its Terminal User Interface (TUI) and then connect it to HPE Compute Ops Management.

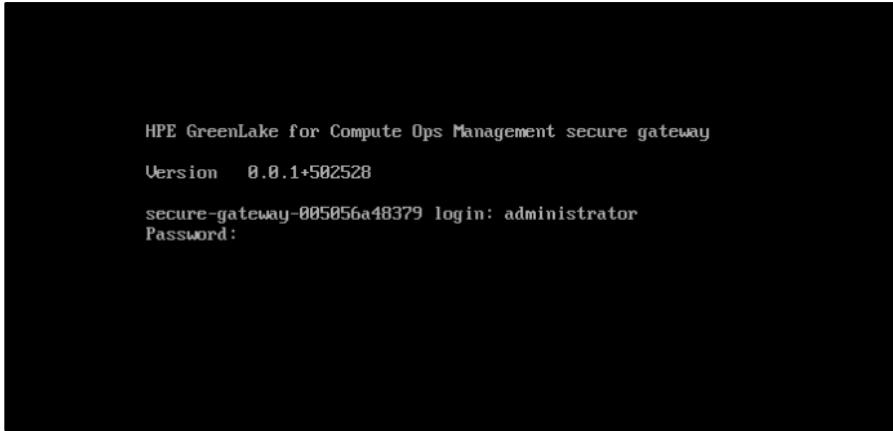
1. There are multiple ways to power on a VM, **click the Green Play button** or any alternative you prefer.



2. Click **Launch Web Console** so you can access the Appliance TUI and continue the configuration.



3. Enter the **default Username and Password** to login which is **administrator / admin**.



Note: For navigating through the TUI, you will need to use the **TAB** and **Enter** keys.

4. For the next two screens we will need to **Accept the T&C's**.
5. We will then update the password to **HPESecurePasswOrd!** and hit **Save**.
6. Hit **Next** on **Step 1 of 5**, as this is just **informational** regarding our **NIC MAC Address**.

7. Enter the fully qualified domain name of your Secure Gateway using the table below.

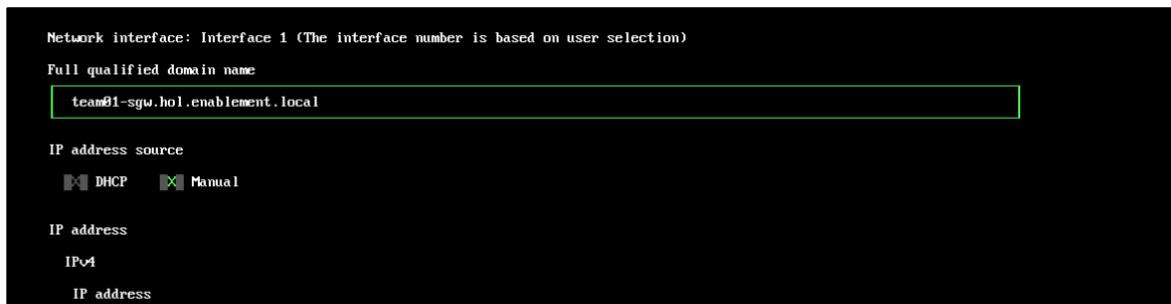
Network interface: Interface 1 (The interface number is based on user selection)

Full qualified domain name

IP address source

<b>Team Number</b>	<b>Full qualified domain name</b>	<b>IP address</b>
Team-01	team01-sgw.hol.enablement.local	10.18.20.51
Team-02	team02-sgw.hol.enablement.local	10.18.20.52
Team-03	team03-sgw.hol.enablement.local	10.18.20.53
Team-04	team04-sgw.hol.enablement.local	10.18.20.54
Team-05	team05-sgw.hol.enablement.local	10.18.20.55
Team-06	team06-sgw.hol.enablement.local	10.18.20.56
Team-07	team07-sgw.hol.enablement.local	10.18.20.57
Team-08	team08-sgw.hol.enablement.local	10.18.20.58
Team-09	team09-sgw.hol.enablement.local	10.18.20.59
Team-10	team10-sgw.hol.enablement.local	10.18.20.60
Team-11	team11-sgw.hol.enablement.local	10.18.20.61
Team-12	team12-sgw.hol.enablement.local	10.18.20.62
Team-13	team13-sgw.hol.enablement.local	10.18.20.63
Team-14	team14-sgw.hol.enablement.local	10.18.20.64
Team-15	team15-sgw.hol.enablement.local	10.18.20.65
Team-16	team16-sgw.hol.enablement.local	10.18.20.66
Team-17	team17-sgw.hol.enablement.local	10.18.20.67
Team-18	team18-sgw.hol.enablement.local	10.18.20.68
Team-19	team19-sgw.hol.enablement.local	10.18.20.69
Team-20	team20-sgw.hol.enablement.local	10.18.20.70
Team-21	team21-sgw.hol.enablement.local	10.18.20.71
Team-22	team22-sgw.hol.enablement.local	10.18.20.72
Team-23	team23-sgw.hol.enablement.local	10.18.20.73
Team-24	team24-sgw.hol.enablement.local	10.18.20.74
Team-25	team25-sgw.hol.enablement.local	10.18.20.75

8. Select the check box for **Manual** IP Address Source



9. For the IP address, use the table above to select your corresponding IP Address

10. For the prefix length, it is **22**.

11. For the **Gateway** value enter **10.18.20.1**.

12. In the **DNS** Configuration area, enter **10.18.20.111** for the **Primary** DNS Server.

13. For the **Secondary** DNS Server enter **10.18.20.112**.

14. Once all entered correctly, select **Next** to proceed.

Network interface: Interface 1 (The interface number is based on user selection)

Full qualified domain name  
team01-sgw.hol.enablement.local

IP address source  
DHCP Manual

IP address  
IPv4  
IP address  
10.10.20.51

Prefix length  
22

Gateway  
10.10.20.1

Domain name server

Preferred DNS server (required)  
10.10.28.111

Alternate DNS server (optional)  
10.10.20.112

<- Back View log Next ->

15. Leave the default options for **Time and Web Proxy** configuration.

16. Now return to your **Web Browser** that's connected to **HPE Compute Ops Management**.

17. From the COM homepage, navigate to **Inventory**, then select **Appliances**.

HPE GreenLake

Compute Ops Management Overview Servers **Inventory** Manage Firmware Reports Activity

Inventory

Servers Monitor and manage servers

Appliances Monitor and manage OneView and secure gateway appliances

18. Click **Add Appliance**, ensure **Secure gateway** is selected.

## Appliance type

[Learn more about adding an appliance](#)

Get an activation key and use it to activate an appliance to Compute Ops Management.

Appliance type

OneView

Secure gateway

Get an activation key and use it in the secure gateway console to onboard appliance(s) to Compute Ops Management. The secure gateway appliance will be added to the Compute Ops Management appliance inventory if not previously added.

19. Set **30 minutes** for how long the activation key will be valid.

Step 2 of 3

## Add appliance options

[Learn more about adding an appliance](#)

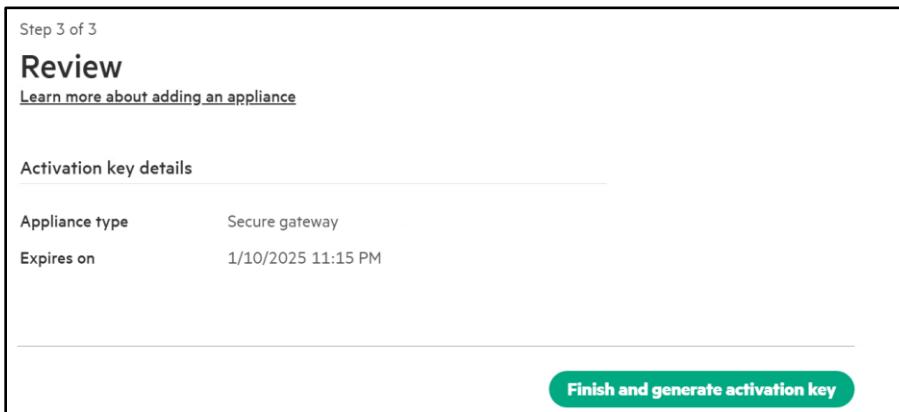
Select how long the activation key for secure gateway will be valid.

Expiration

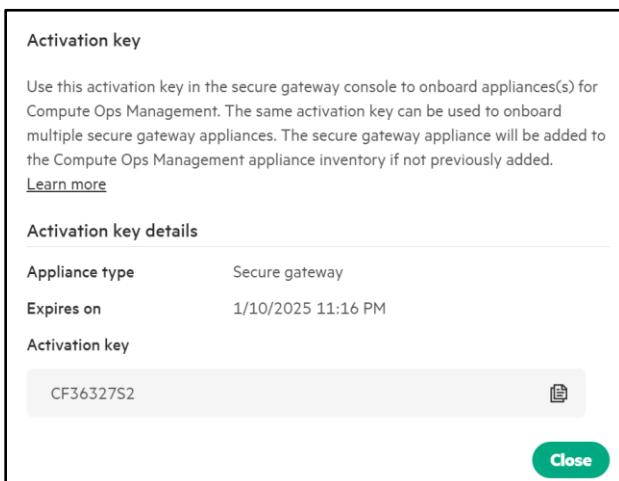
30 minutes ▾

**Next**

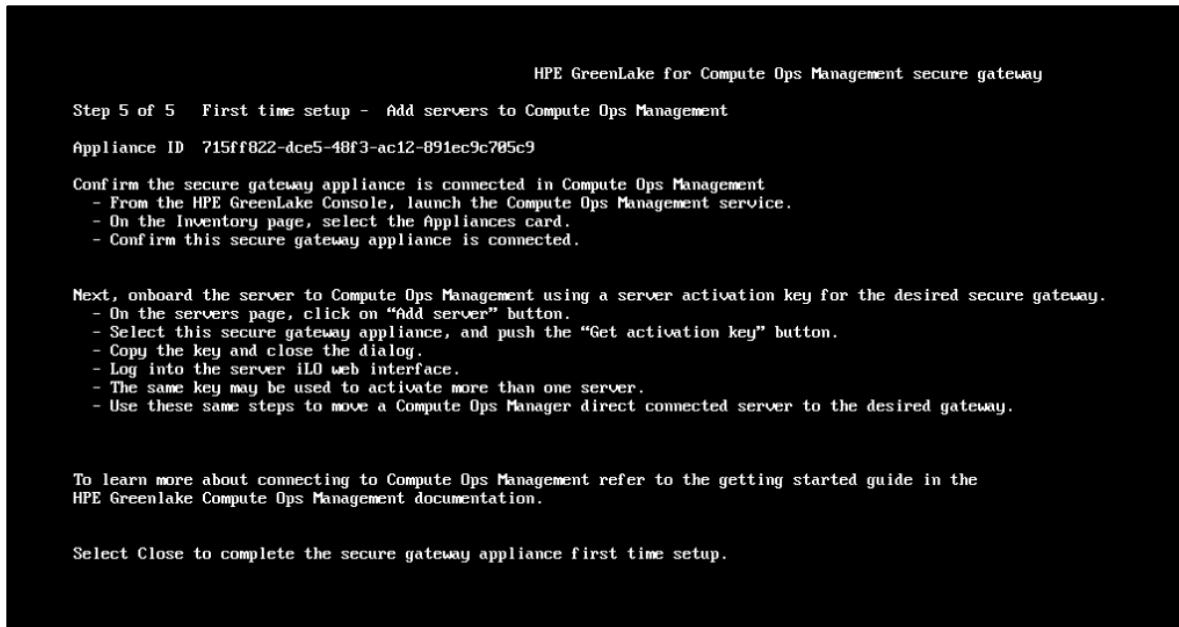
20. Then click **Finish and generate activation key**.



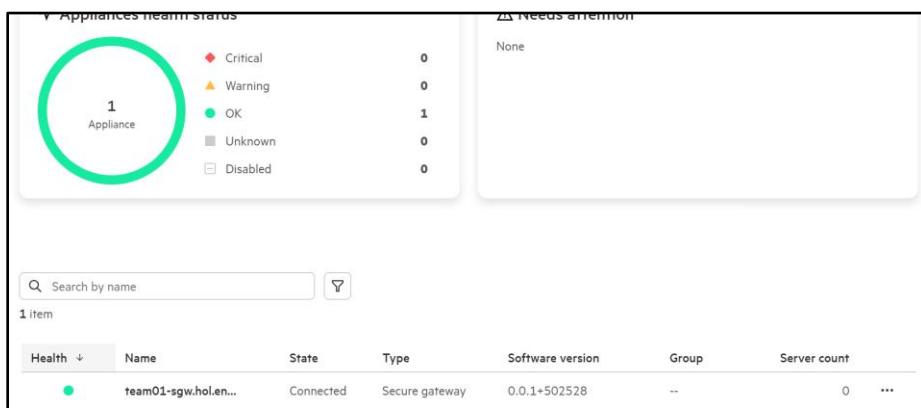
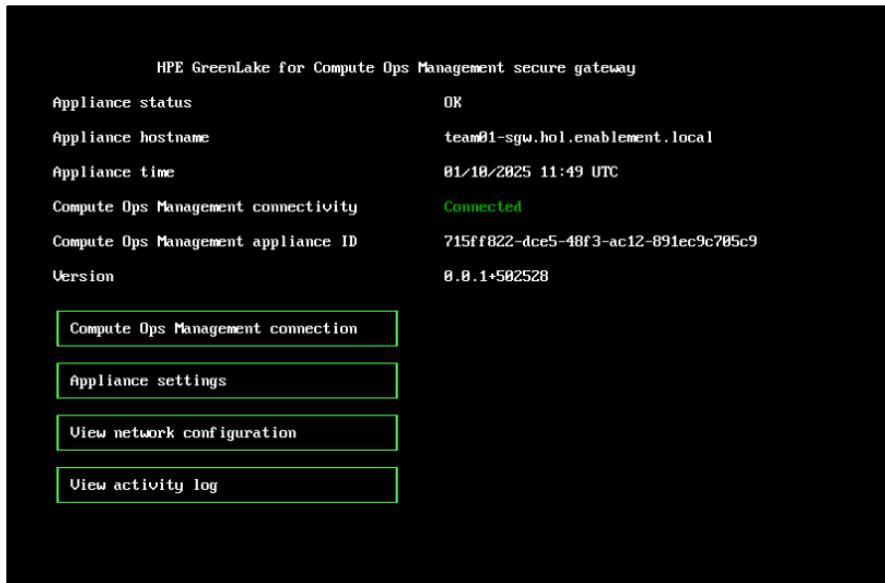
21. Take note of the **Activation Key** and then **type** this into the **TUI for the Secure Gateway Appliance**.



22. The Secure Gateway should now be **connected** and you can **Close** this last **informational** step.



23. The TUI and COM inventory page for **Appliances** should show your **Secure Gateway** as **Connected**.



This concludes this section of the lab.

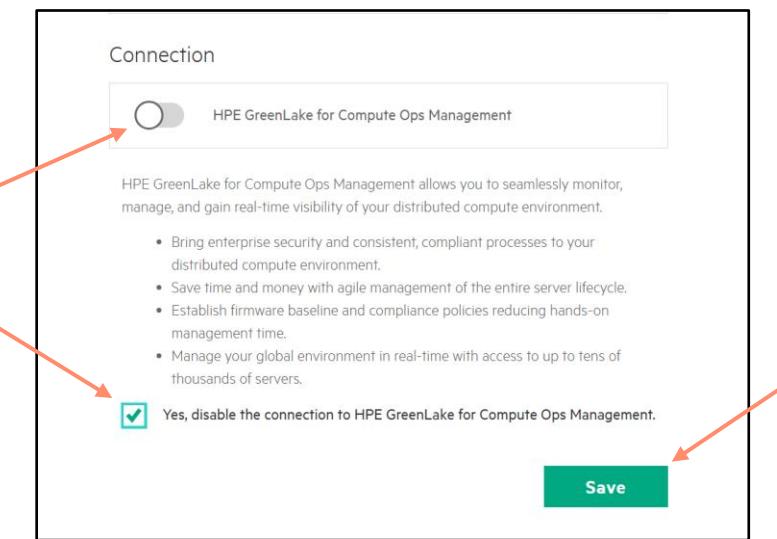
## Connecting our HPE iLO to COM via the Secure Gateway

In this portion of the lab, we will disconnect our existing iLO from COM, modify our Proxy details and then create a new Activation Key linking it to the Secure Gateway and apply this to our iLO.

1. Return to the **Web Browser** that's connected to your **HPE iLO** and navigate to **Compute Ops Management** section on the left-hand side.

The screenshot shows the HPE GreenLake for Compute Ops Management interface. On the left, there is a sidebar with the following menu items: Information, System Information, Compute Ops Management (which is selected), Firmware & OS Software, iLO Federation, Remote Console & Media, Power & Thermal, iLO Dedicated Network Port, and iLO Shared Network Port. The main content area is titled "Compute Ops Management". It displays the Connection Status as "Connected", the HPE GreenLake Workspace ID as "0ec9d31632111ef85ad52587cbe5bc3", and the Connection Type as "Direct". There are "Edit Settings" and "HPE GreenLake" buttons at the bottom. The top right corner has several status icons.

2. From here, click on **Edit Settings**, and **disable** the COM connection then click **Save**.



3. Then navigate to the **Security** section to update the **Web Proxy** details.

**Access Settings**

**Server**

Server Name	HPE-HOL52
Server FQDN / IP Address	[Not set]

**Network**

Anonymous Data	Enabled
Enhanced Download Performance	Enabled
IPMI/DCMI over LAN	Disabled
IPMI/DCMI over LAN Port	623
Remote Console	Enabled
Remote Console Port	17990
Secure Shell (SSH)	Enabled
Secure Shell (SSH) Port	22
SNMP	Enabled
SNMP Port	161
SNMP Trap Port	162
Virtual Media	Enabled
Virtual Media Port	17988
Virtual Serial Port Log Over CLI	Disabled
Web Server	Enabled
Web Server Non-SSL Port Enabled	Enabled
Web Server Non-SSL Port	80
Web Server SSL Port	443
Web Proxy	Enabled
Web Proxy Server	hpeproxy.its.hpecorp.net
Web Proxy Port	443
Web Proxy Username	[Not set]
Web Proxy Password	[Redacted]

4. Click the **pencil** next to the right of **Network** and scroll down to the **Web Proxy** information.

<input checked="" type="checkbox"/> Web Proxy
Web Proxy Server hpeproxy.its.hpecorp.net
Web Proxy Port 443
Web Proxy Username
Web Proxy Password

- Update the **Web Proxy Server** to the FQDN of your newly created Secure Gateway Appliance. Refer back to your assigned FQDN to know what to enter here. For this example, we will use "Team01". Additionally, set the **Web Proxy Port** to **8080**.

The screenshot shows a configuration form titled "Web Proxy". It contains the following fields:

- Web Proxy Server: team01-sgw.hol.enablement.local
- Web Proxy Port: 8080
- Web Proxy Username (empty)
- Web Proxy Password (empty)

- Find your **Web Browser** or **Tab** that's **connected to Compute Ops Management** and navigate to **Servers**. You will see your server showing it as **Reconnecting** or **Not Connected** depending on how fast you are.

<input type="checkbox"/>	Health	Name	Serial	iLO security	State	Baseline	Group	Power	Tags	Model
<input type="checkbox"/>		HPE-HOL52	CN70461J1W	At risk	Not connected	Patch 2023.09.00....	--	On	0	ProLiant Gen10

- Go ahead and click **Add server** at the top right area of this page.

The screenshot shows the "Servers" page with the following interface elements:

- A header bar with the title "Servers".
- Two status indicators below the header: "Servers health status" and "iLO security status".
- A prominent green button on the right labeled "Add server" with a red arrow pointing to it.

8. Change the **Server connection type** to **Secure gateway** and select your **assigned** secure gateway from the **drop-down menu**.

Step 1 of 3

## Connection type

[Learn more about adding a server](#)

Get an activation key and use it in iLO to onboard server(s) to Compute Ops Management. The server will be added to HPE GreenLake device inventory if not previously added.

⚠ Ensure that your HPE GreenLake Platform application role includes **edit** permissions for **Devices and Subscription Service**.

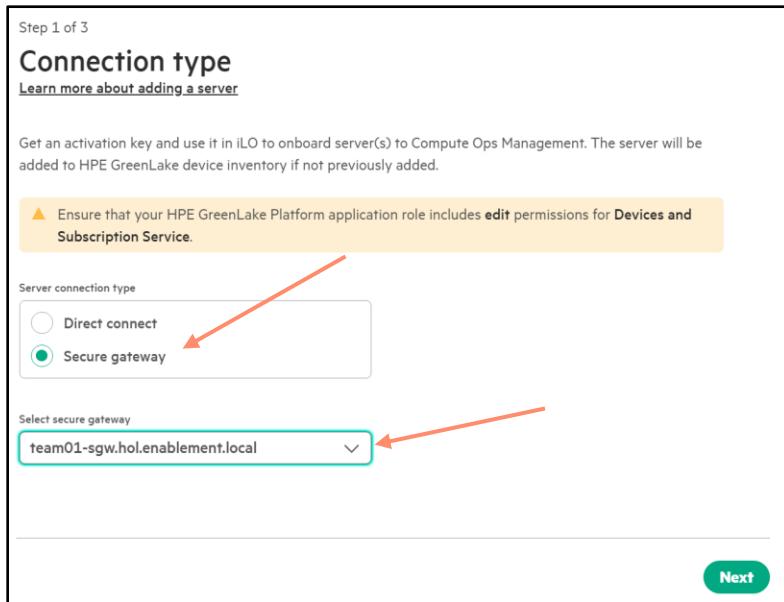
Server connection type

Direct connect  
 Secure gateway

Select secure gateway

team01-sgw.hol.enablement.local

**Next**



9. Change the Expiration to **30 minutes** and select an available **Subscription Key**.

Step 2 of 3

## Activation key options

Expiration

Choose how long the activation key will be valid

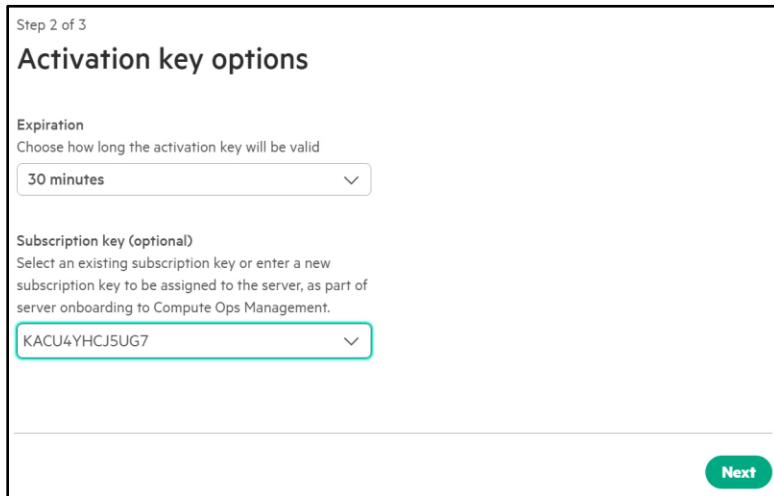
30 minutes

Subscription key (optional)

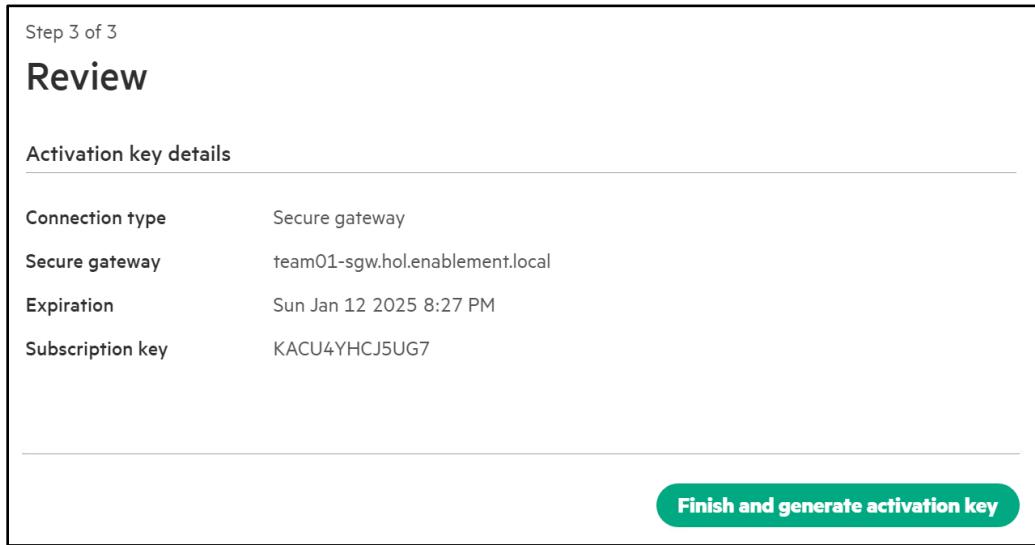
Select an existing subscription key or enter a new subscription key to be assigned to the server, as part of server onboarding to Compute Ops Management.

KACU4YHCJ5UG7

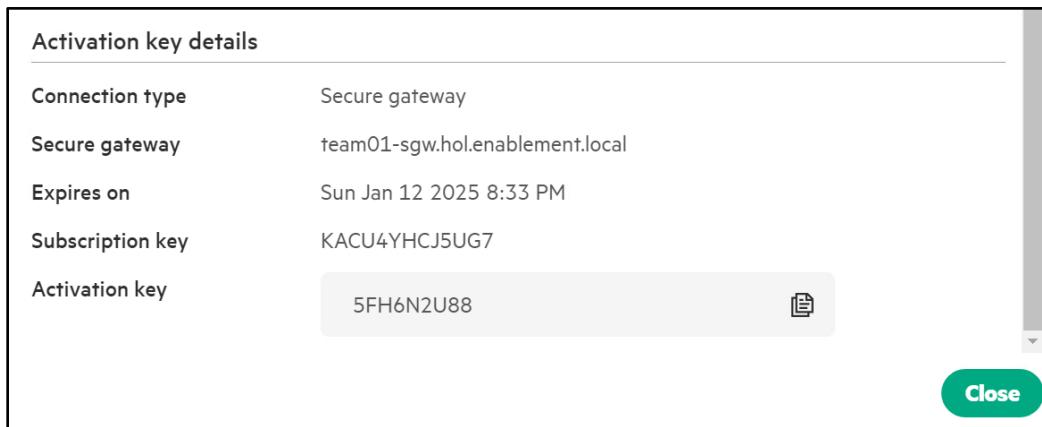
**Next**



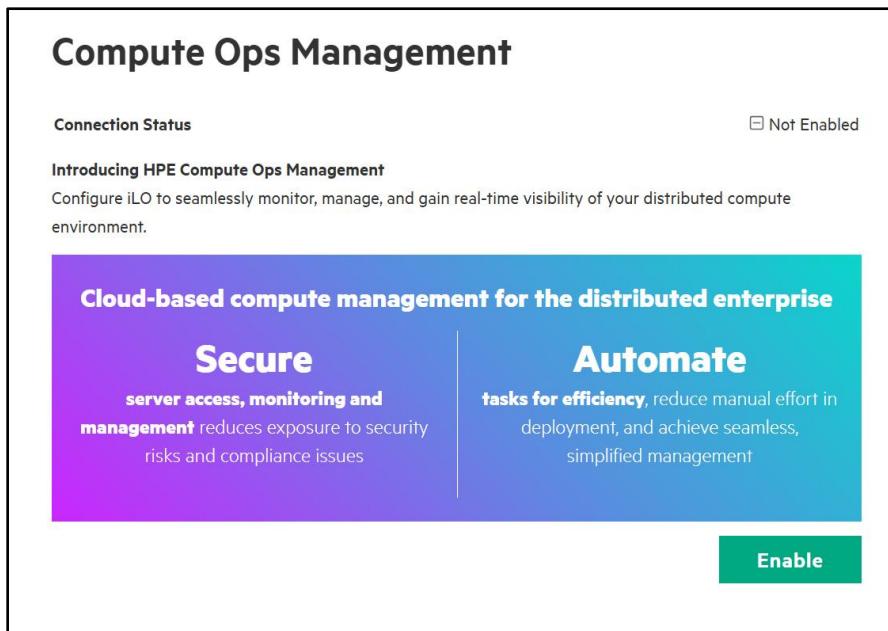
10. Review your Activation Key Details, then hit **Finish and generate activation key**.



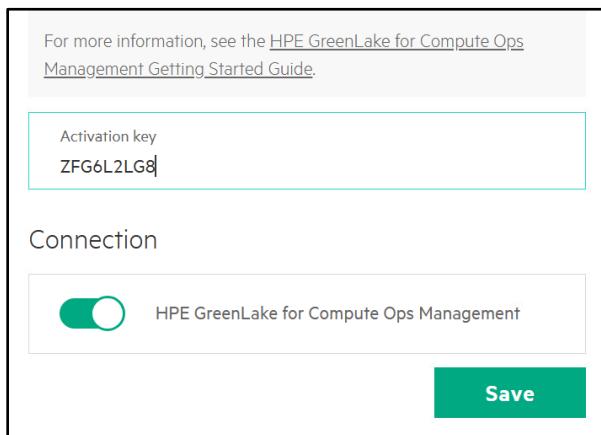
11. Take note of or **copy the Activation key**, then close the pop up.



12. Return to your **Web Browser** or **Tab** which is connected to your **Server's HPE iLO**, Click on **Compute Ops Management**.



13. **Click Enable**, enter the **Activation key** and hit **Save**.



14. Give it a few seconds and it should then return with a Connection Status of **Connected**, your **workspace ID** and **Connection Type Gateway**.

**Compute Ops Management**

<b>Connection Status</b>	Connected
<b>HPE GreenLake Workspace ID</b>	0ec9d31632111ef85ad52587cbe5bc3
<b>Connection Type</b>	Gateway
<a href="#"><u>Edit Settings</u></a>	<a href="#"><u>HPE GreenLake</u></a>

15. If we then navigate back to our Browser or Tab that's connected to COM, we will see our Server now Connected and going through it's inventory process.

<input type="checkbox"/>	HPE-HOL52	CN70461J1W	At risk	Retrieving server driver and software inventory in progress	Patch 2023.09.00....	--	On	0	ProLiant DL325 Gen10 F
--------------------------	-----------	------------	---------	---	----------------------	----	----	---	------------------------

16. If you go a step further and Click on the **Hostname of your Server** or at this point, possibly the two bolded dash lines --, you will get detailed information and see you are connected via the Secure Gateway.

<input type="checkbox"/>	Health	Name	Serial	iLO security	State	Baseline	Group	Power	Tags	Model
<input type="checkbox"/>	--	2M2946009Z	At risk	Connected	SPP 2024.11.00.00...	Team01	On	0	ProLiant DL160 Gen10	

**Details**

<b>State</b>	Connected	
<b>Group</b>	--	
<b>Connection type</b>	Secure gateway	
<b>Appliance</b>	<a href="#"><u>team01-sgw.hol.enablement.local</u></a>	<b>Connected</b>
<b>Model</b>	ProLiant DL325 Gen10 Plus	
<b>Serial number</b>	CN70461J1W	

17. You can also click on the **hyperlink** for your **Secure Gateway** to get **detailed information** for it as well.

The screenshot shows a web-based management interface for an HPE Secure Gateway Appliance. At the top left is a back arrow labeled "Appliances". The main title is "team01-sgw.hol.enablement.local". Below the title is a "Details" section. A table follows, listing the following information:

Health	OK
State	Connected
Appliance ID	715ff822-dce5-48f3-ac12-891ec9c705c9
Version	0.0.1+502528
Model	HPE Secure Gateway Appliance
Server count	1 server

You have accomplished what we wanted to show you in this HOL experience. We hope you get a lot out of it. Thank you for participating in the session.

This completes this HOL experience.

## Summary

In this lab, we explored the robust capabilities of HPE's integrated Lights-Out (iLO) management tools, specifically iLO5 and iLO6, within the ProLiant Gen10+ and Gen11 series. We also examined how HPE Compute Ops Management offers secure and efficient remote management of HPE servers, enabling administrators to access and control systems from virtually anywhere—provided the necessary security configurations are in place.

By implementing iLO security best practices—such as secure network access, strong authentication methods, and encryption—users can maintain a secure environment while remotely managing ProLiant servers. This applies across various environments, from remote offices and edge systems to large data centers. HPE's unified management strategy ensures consistency in system oversight, regardless of location.

Additionally, we demonstrated how HPE Compute Ops Management integrates seamlessly with a Secure Gateway, highlighting the ease and security of remote management. With HPE ProLiant Compute, HPE empowers IT administrators with both the flexibility and security needed to maintain full control of their hardware, no matter where it's located.

## Want more?

Back home, you can head to the HPE Demonstration Portal and request a time slot (<https://hpedemoportal.ext.hpe.com/>) to demonstrate these products

For COM Interest, request a 90-day evaluation  
(<https://www.hpe.com/us/en/compute/management-software.html?dmodal=modal-edbaf#>)

Pull out your phone and view HPE GreenLake and HPE Compute Ops Management, to move to the next step in a wholistic IT system management strategy.

**Login:** com.demouser@gmail.com

**Password:** 2025!Summ3r



## LEARN MORE AT

<https://hpe.com/us/en/compute/management-software.html>