



**Hewlett Packard
Enterprise**

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	6
Managing Local Users.....	10
Firmware Verification	13
Applying Web Proxy configuration	16
Connecting to HPE Compute Ops Management	18
Return to your HOL Horizon session.....	19
Secure Login Options for Enterprise IT Administrators	21
Establishing a connection from HPE iLO to HPE GreenLake	25
Configuring Server Groups and Applying Server Settings	32
Creating server groups and associating server settings	38
Advanced Security settings for iLO.....	48
iLO SSL Certificate Management.....	60
Deploying the Secure Gateway through VCenter	70
Configuring the Secure Gateway and connecting to COM	77
Connecting our HPE iLO to COM via the Secure Gateway	85

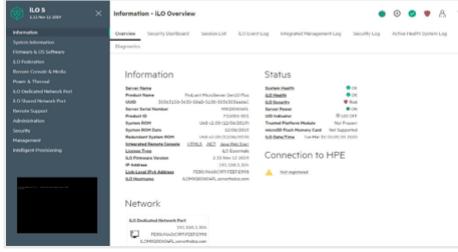
HPE ProLiant Security Experience

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

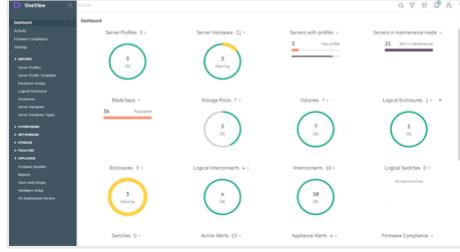
Embedded Server Management that enables you to securely configure, monitor and update your HPE server



HPE OneView

On-premises

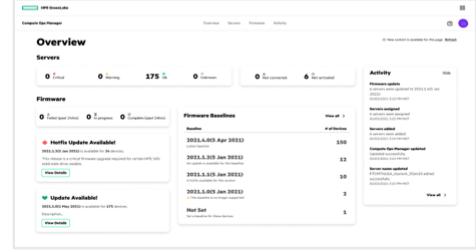
Infrastructure management software that provides composable solutions across compute, storage, and networking.



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.

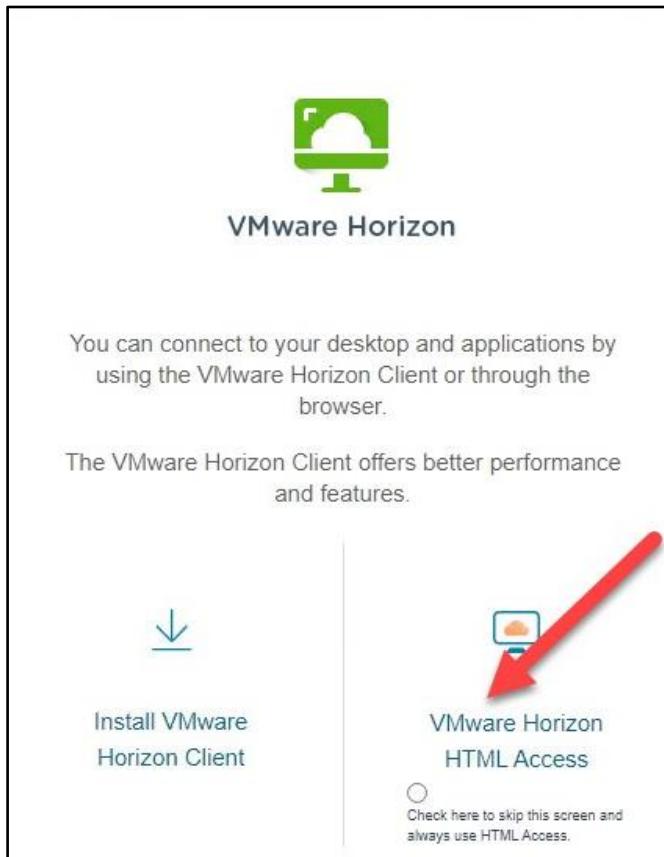
This HOL aims to take a technical approach to how these tools can be used to manage HPE ProLiant Servers with a strong focus around Security.

Connecting to the lab environment

Logging into Compute BU enablement environment.

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

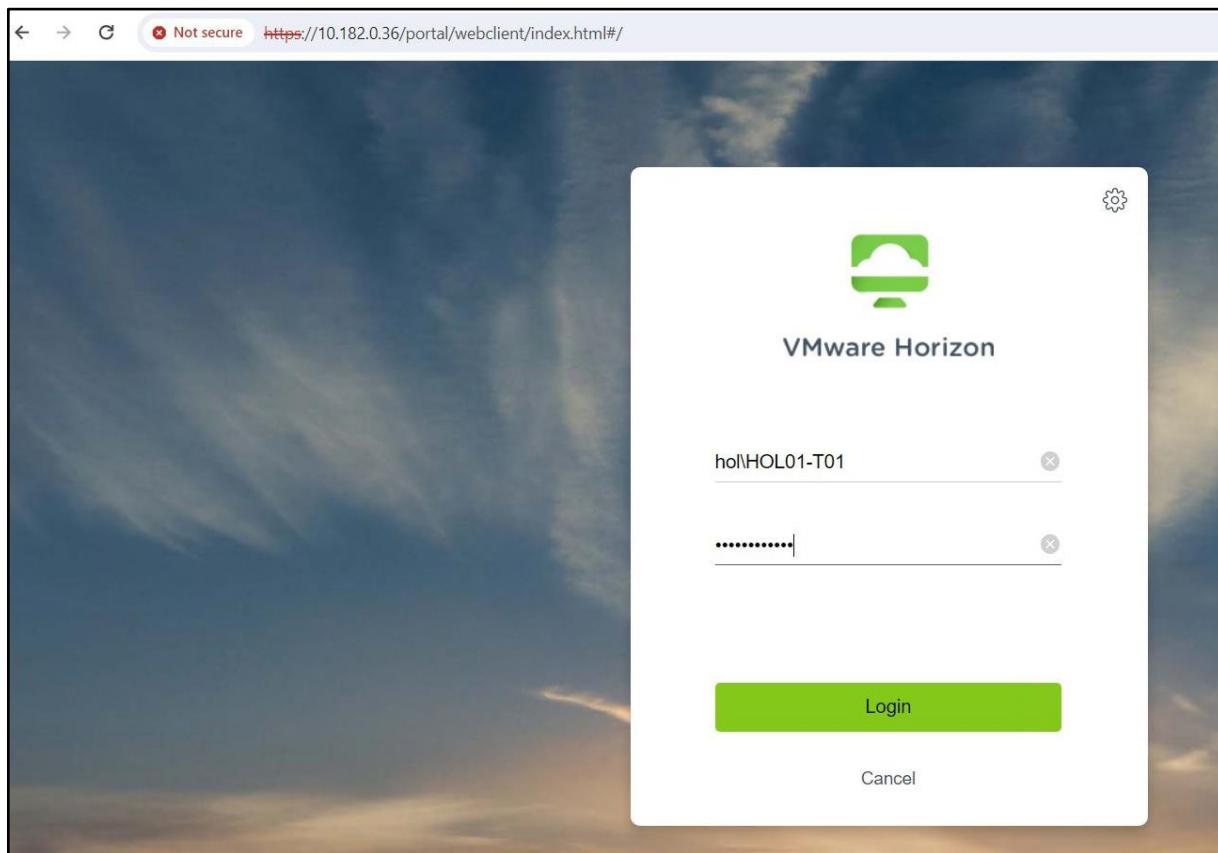
1. Using your Chrome browser, go to our Horizon based Compute Enablement access at: <https://16.103.2.129/>
2. At the VMware Horizon login screen, **click on the VMware Horizon HTML Access button**.



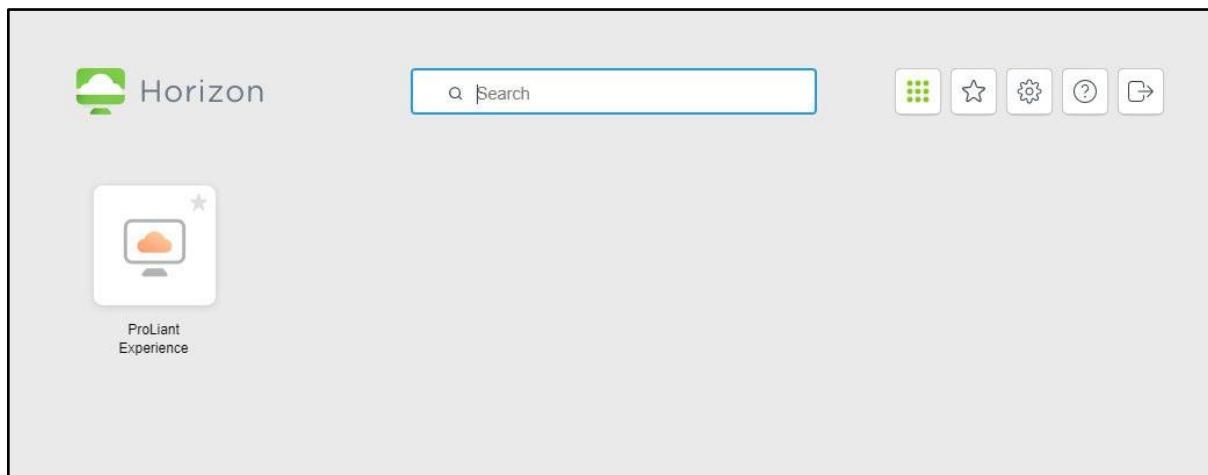
3. Enter the username and password supplied by your instructor and click the Login button.

Username: **HOL\HOL06-T01** through **HOL\HOL06-T25**, (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, make sure you use the logout button.



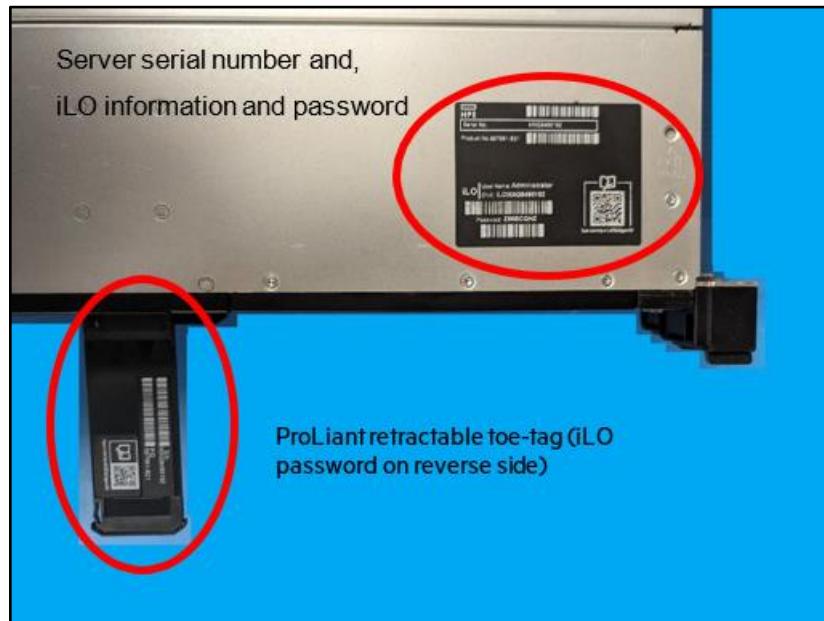
You are now in a VPN-enabled Chrome browser session. For these labs to work, you will need to stay within the context of this browser session. You have a secure connection to our remote lab in Houston, but it doesn't work like a traditional VPN session. Only what you launch from this browser session,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

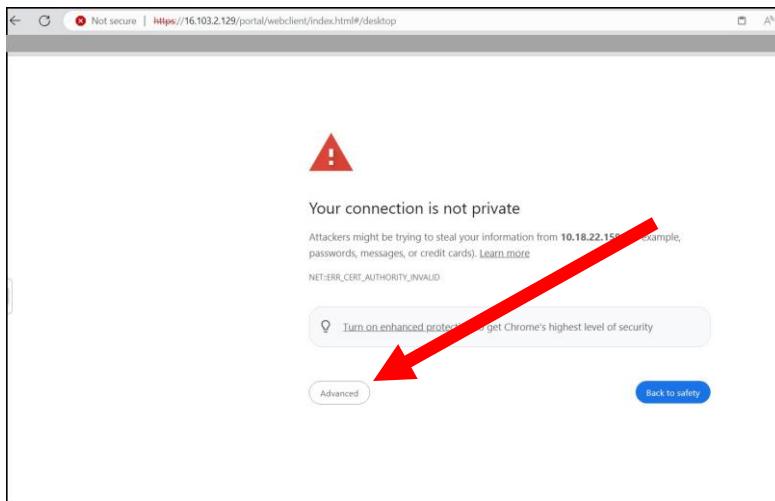
This portion of the lab exercises assumes the server has power, the iLO ethernet port is connected to a management network switch and the default password information has been gathered off the toe-tag on the front of the server.



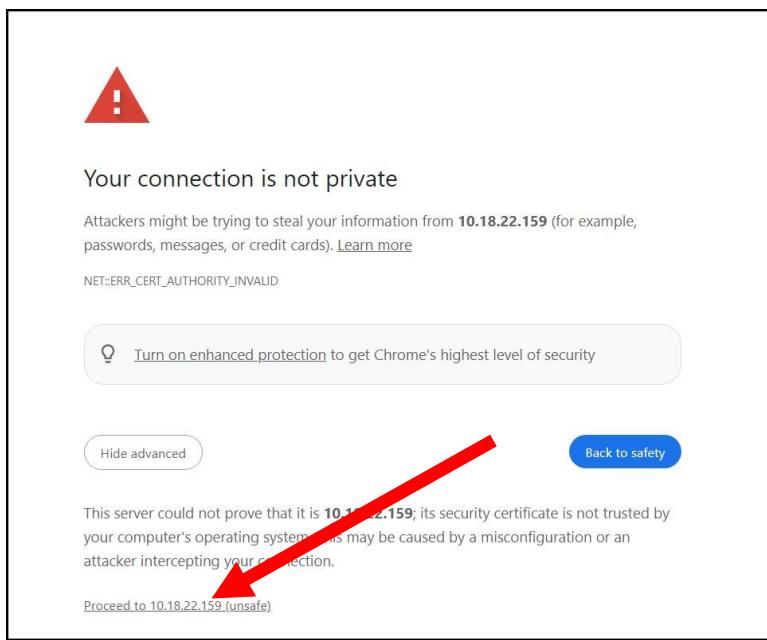
In this lab environment, a DHCP server is issuing IP addresses to known hosts using DHCP reservations. This ensures the lab unit you will access obtains the same IP address each time it boots after the lab is reset. Consult the table below for your team's name and number, and default Administrator credentials.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

Team Name & Number	iLO IP Address	Username	Default Factory Password
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	DPJDMMJ2
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**.

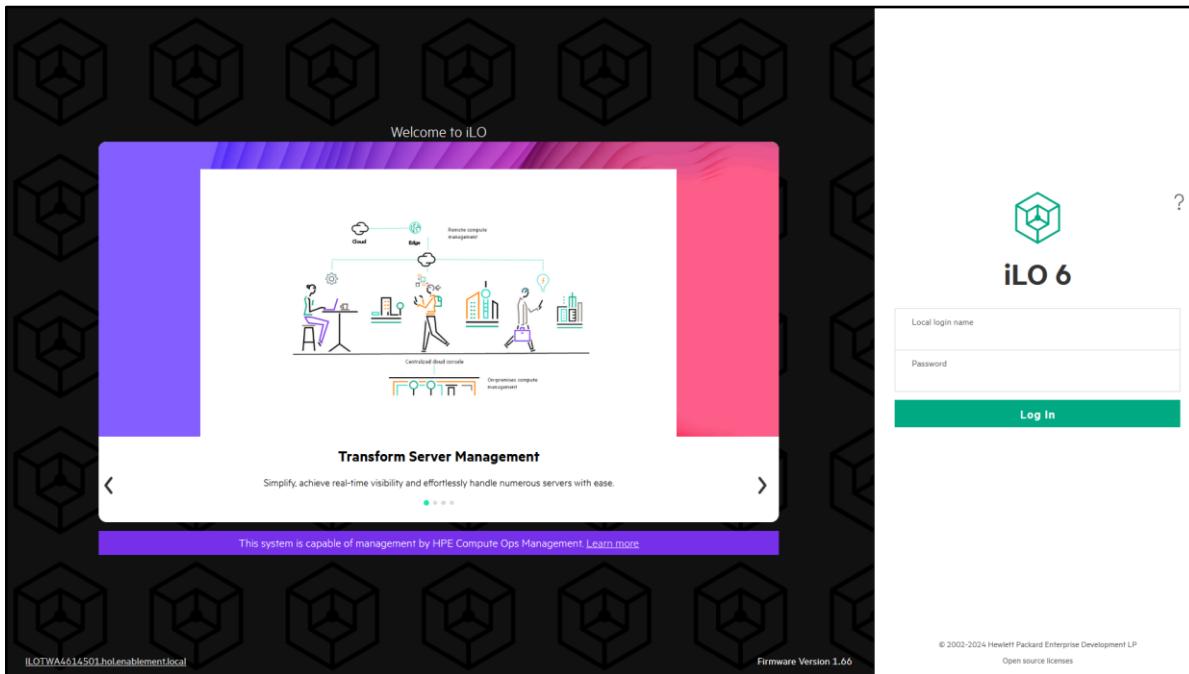


4. On the newly displayed prompt, **click on the Proceed to 10.18.22.xx** to continue to the iLO login screen.



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**.

The screenshot shows the iLO 6 administration interface. On the left, a sidebar lists various management categories. The 'Administration' category is selected and highlighted in green. The main content area is titled 'Administration - User Administration'. It contains two tables: 'Local Users' and 'Service'. The 'Local Users' table has columns for Login Name, User Name, and Status. It shows two entries: 'Administrator' (Status: Enabled) and 'TechEnablement' (Status: Enabled). Both users have checkmarks in all listed permissions. Below these tables are four buttons: 'New', 'Edit', 'Delete', and 'Enable'. The 'New' button is highlighted with a green border.

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.

Login Name	HPE_Admin
User Name	HPE Admin
New Password	hpent123
Confirm Password	hpent123
Role	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:	administrator
<input type="checkbox"/> Service Account	

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

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

Login Name	User Name	Status	Actions
<input type="checkbox"/> Administrator	Administrator	Enabled	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
<input type="checkbox"/> HPE_Admin	HPE Admin	Enabled	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✗

Login Name	User Name	Status	Actions
<input type="checkbox"/> TechEnablement	TechEnablement	Enabled	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓

New **Edit** **Delete** **Enable**

- Logout and then log back in with your newly created user.
- 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.
- Return to the Administration section in iLO and Click on the Directory Groups tab.

Group	SID	Actions
<input type="checkbox"/> Administrators		✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✗
<input type="checkbox"/> Authenticated Users	S-1-5-11	✓ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗

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

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.

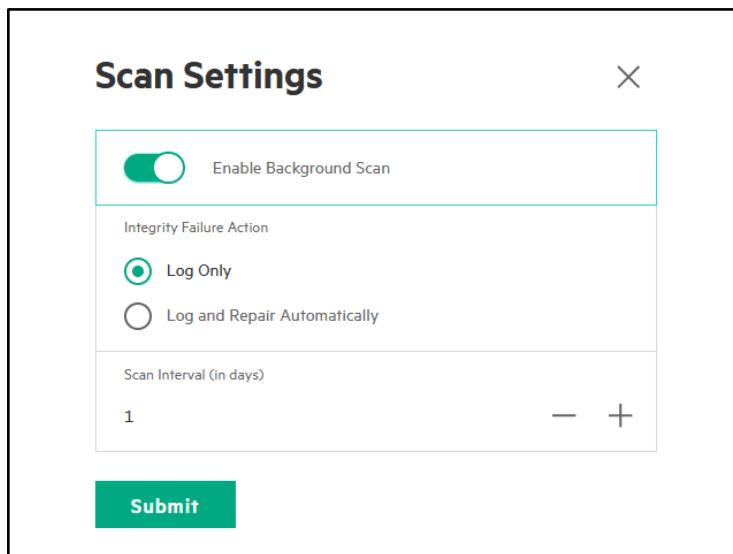
1. Click on the **Firmware Verification** tab to explore the iLO capability to manually scan the system firmware to check the validity and health of the firmware components.

The screenshot shows the 'Administration - Firmware Verification' interface. At the top, there are several icons: a power button, a circular arrow, a triangle, a sun, a gear, a hexagon, a shield, a person, and a question mark. Below the icons, a navigation bar includes links for User Administration, Directory Groups, Boot Order, Licensing, Key Manager, Language, and Firmware Verification (which is underlined). A green banner at the top displays a checkmark icon and the text 'Last scan result: OK' followed by 'Last scan time: 2025-03-05T06:31:22Z'. The main content area is titled 'Firmware Status' and contains a table with the following data:

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

At the bottom left are two buttons: 'Run Scan' and 'Send Recovery Event'. On the right side of the status table is a 'Scan Settings' button.

2. 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.



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

The page has a navigation bar with tabs: User Administration, Directory Groups, Boot Order, Licensing, Key Manager, Language, and Firmware Verification (which is active).

Alert messages:

- Last scan result: OK (Last scan time: 2025-03-05T06:31:22Z)
- Scan settings saved successfully

Firmware Status table:

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

Scan Settings button is located in the top right corner of the table area.

- 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 'Administration - Firmware Verification' page. At the top, there are several icons: a yellow circle with a dot, a blue gear, a yellow triangle, a green sun-like icon, a blue hexagon, a red shield, a person icon, and a question mark. Below the icons is a navigation bar with tabs: User Administration, Directory Groups, Boot Order, Licensing, Key Manager, Language, and Firmware Verification (which is underlined). A message box displays: 'Runtime Firmware Verification' and 'New scan in progress, please wait ...'. Below this is a 'Firmware Status' table with the following data:

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

At the bottom left are two buttons: 'Run Scan' and 'Send Recovery Event'. The 'Scan Settings' button is located at the top right of the table area.

- 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 [Not set]	Anonymous Data	Enabled	Global Component Integrity	Disabled
Server FQDN / IP Address		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) Port	22	iLO Web Interface	Enabled
		SNMP	Enabled	Remote Console Thumbnail	Enabled
		SNMP Port	161	Require Host Authentication	Disabled
		SNMP Trap Port	162	Require Login for iLO RBSU	Disabled
		Virtual Media	Enabled	Serial Command Line Interface Speed	9600
		Virtual Media Port	17988	Serial Command Line Interface Status	Enabled - Authentication Required
		Virtual Serial Port Log Over CLI	Disabled	Show iLO IP during POST	Enabled
		Web Server	Enabled	Show Server Health on External Monitor	Enabled
		Web Server Non-SSL Port Enabled	Enabled	VGA Port Detect Override	Enabled
		Web Server Non-SSL Port	80	Virtual NIC	Disabled
		Web Server SSL Port	443		
		Web Proxy	Disabled		
		Web Proxy Server	[Not set]		
		Web Proxy Port	1		
		Web Proxy Username	[Not set]		
		Update Service			
				Downgrade Policy	Allow downgrades
				Accept 3rd Party Firmware Update Packages	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 text "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. The main content area is divided into several sections:

- Getting Started**: Contains two cards: "Find Services" (Discover and launch services from our catalog) and "Manage Workspace" (Set up this workspace, users, access and more). There is a "Dismiss" link next to the Manage Workspace card.
- Recent Services**: Shows a card for "Compute Ops Management" (Compute) with a "Launch" button. To the right, there is a "My Services" section with a list icon and a "Learn" button below it.
- Featured Services**: A section with a "View Catalog" button.
- Quick Links**: A sidebar on the right containing links to various management tools:
 - [Manage Workspace](#)
 - [Device Inventory](#)
 - [Service Subscriptions](#)
 - [User Management](#)
 - [Locations](#)
 - [Switch Workspace](#)
 - [Reporting](#)
 - [Feedback](#)
 - [Support Hub](#)

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.

Team Number	GreenLake Username	User password
Team-001	comholuser+1@gmail.com	TechPr02025!
Team-002	comholuser+2@gmail.com	TechPr02025!
Team-003	comholuser+3@gmail.com	TechPr02025!
Team-004	comholuser+4@gmail.com	TechPr02025!
Team-005	comholuser+5@gmail.com	TechPr02025!
Team-006	comholuser+6@gmail.com	TechPr02025!
Team-007	comholuser+7@gmail.com	TechPr02025!
Team-008	comholuser+8@gmail.com	TechPr02025!
Team-009	comholuser+9@gmail.com	TechPr02025!
Team-010	comholuser+10@gmail.com	TechPr02025!
Team-011	comholuser+11@gmail.com	TechPr02025!
Team-012	comholuser+12@gmail.com	TechPr02025!
Team-013	comholuser+13@gmail.com	TechPr02025!
Team-014	comholuser+14@gmail.com	TechPr02025!
Team-015	comholuser+15@gmail.com	TechPr02025!
Team-016	comholuser+16@gmail.com	TechPr02025!
Team-017	comholuser+17@gmail.com	TechPr02025!
Team-018	comholuser+18@gmail.com	TechPr02025!
Team-019	comholuser+19@gmail.com	TechPr02025!
Team-020	comholuser+20@gmail.com	TechPr02025!
Team-021	comholuser+21@gmail.com	TechPr02025!
Team-022	comholuser+22@gmail.com	TechPr02025!
Team-023	comholuser+23@gmail.com	TechPr02025!
Team-024	comholuser+24@gmail.com	TechPr02025!
Team-025	comholuser+25@gmail.com	TechPr02025!

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

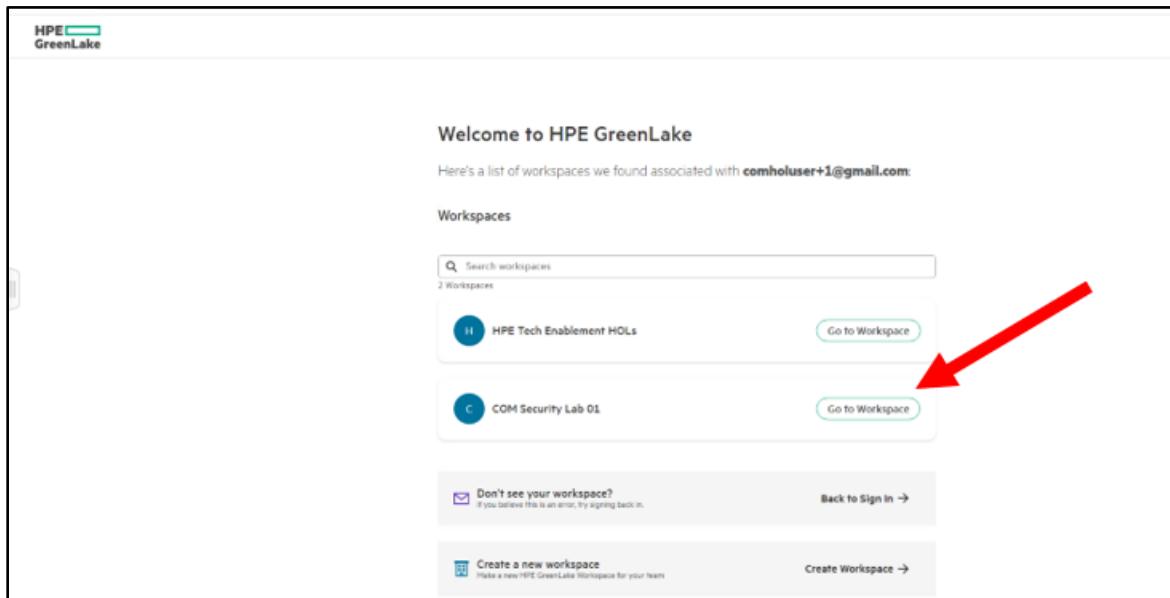
OR

Sign in with SSO

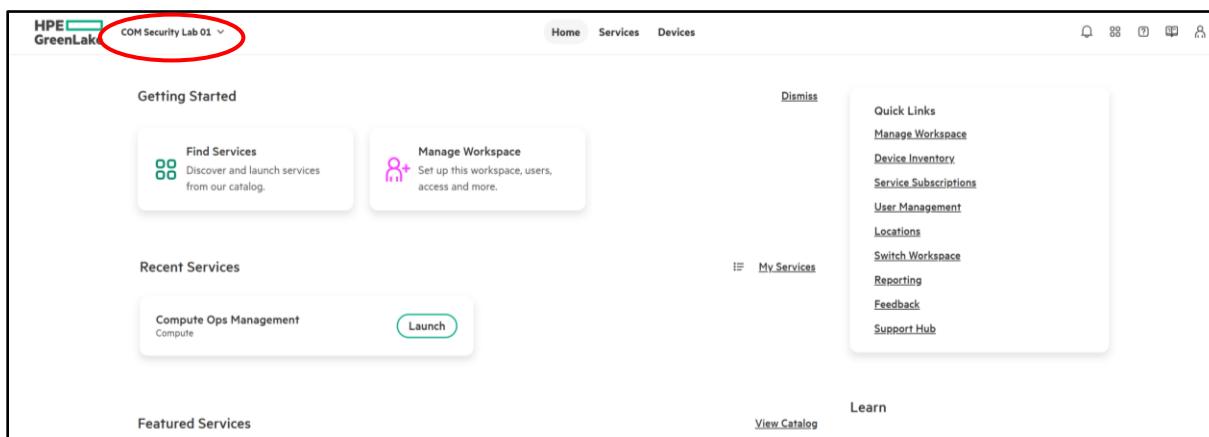
[Need help signing in?](#)

2. Click **Next** to be prompted for a password.
3. Type in the password of **TechPr02025!** (or the password supplied by your instructor) and press the **Enter** key or click **Sign In**.

4. When presented with a choice of workspaces, choose **COM Security Lab XX** (where XX is your Team Number) and **Go to Workspace**.



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



This concludes this section of the lab.

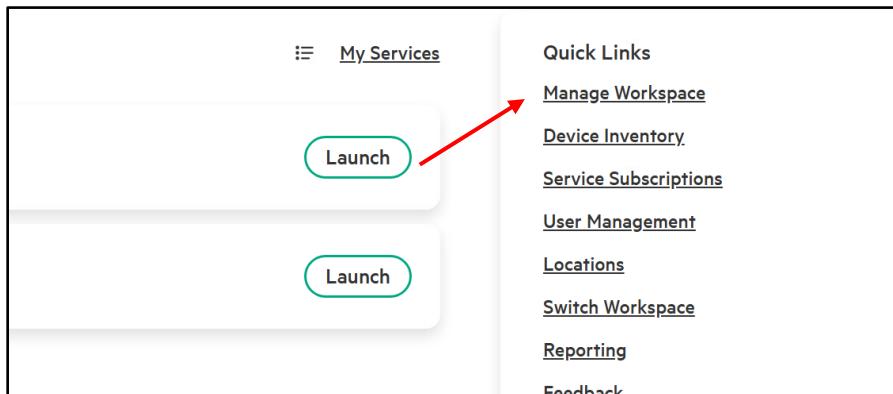
Secure Login Options for Enterprise IT Administrators

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.

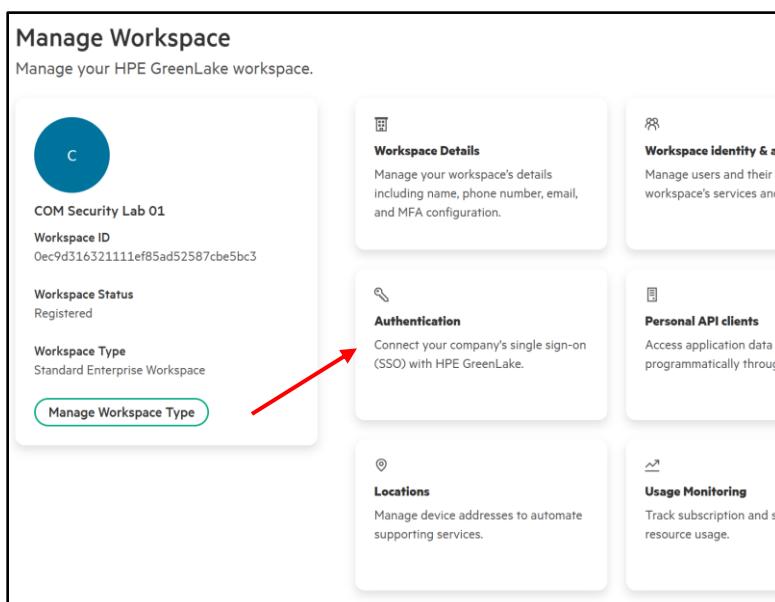
Our HPE GreenLake Cloud Platform supports Multi-Factor Authentication as well as SAML SSO which combining both together, can go a long way to ensuring any bad actors do not access your IT Estate, especially through Compute Ops Management.

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. From here, you can then navigate to the **Authentication** tile.



3. It's here that you would then look to configure your SAML SSO access to HPE GreenLake.

The screenshot shows the 'Authentication' page within the 'Manage Workspace' section of the HPE GreenLake interface. The page title is 'Authentication'. Below it, a sub-section titled 'SAML' is described: 'HPE GreenLake supports SSO by SAML only. Alternatively, users can authenticate with an HPE GreenLake username and password, including optional MFA.' A green shield icon with a plus sign is displayed next to the 'Configure SAML SSO access to HPE GreenLake here.' link.

For more information on setting up and configuring SAML SSO authentication with your enterprise, you can consult the blog: [Configuring-HPE-GreenLake-SSO-SAML-Authentication-with-ADFS](#)

4. Now navigate back to **Manage Workspace** by clicking the left arrow.

The screenshot shows the same 'Authentication' page as before, but with a red arrow pointing to the 'Manage Workspace' backlink located above the main content area.

5. Select the **Workspace Details** tile.

The screenshot shows the 'Manage Workspace' interface. On the left, there's a circular profile picture with a 'C' and some basic workspace information: 'COM Security Lab 01', 'Workspace ID' (0ec9d31632111ef85ad52587cbe5bc3), 'Workspace Status' (Registered), and 'Workspace Type' (Standard Enterprise Workspace). A green button labeled 'Manage Workspace Type' is at the bottom. In the center, there are four tiles: 'Workspace Details' (selected, highlighted with a red arrow), 'Authentication' (with a magnifying glass icon), 'Personal API clients' (with a document icon), and 'Workspace identity & access' (with a user icon). The 'Workspace Details' tile contains text about managing workspace details including name, phone number, email, and MFA configuration.

6. Navigate to the **Security** tab.

The screenshot shows the 'Workspace Details' page under the 'Manage Workspace' header. On the left, there's a circular profile picture with a 'C'. Below it are two tabs: 'Workspace Details' (selected) and 'Security' (highlighted with a red arrow). The main content area is titled 'Workspace Details' and describes managing workspace details including name, phone number, email, and MFA configuration. To the right, there's a 'Workspace Information' section with a table:

Workspace Information	
Manage your workspace's general information.	
Workspace Icon	--
Workspace Name	COM Security Lab 01
Address	United States
	1701 E Mossy Oaks

7. 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.

Workspace Details

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

Workspace Details **Multi-Factor Auth**

Security

Configure multi-factor authentication using Google Authenticator. MFA enforcement is applied to all login attempts, including local and SSO-enabled workspaces.

Multi-Factor Authentication (MFA) Disabled

Edit Details

Workspace Details

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

Workspace Details **Multi-Factor Auth**

Security

Configure multi-factor authentication using Google Authenticator. MFA enforcement is applied to all login attempts, including local and SSO-enabled workspaces.

Multi-Factor Authentication (MFA) Enabled with Google Authenticator

Cancel **Save Changes**

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.

Com Holuser
comhol...+19@gmail.com

Quick Links

- Manage Workspace
- Device Inventory
- Service Subscriptions
- User Management
- Locations

HPE User Account Details ←

HPE GreenLake Preferences
Visit hpe.com
Sign out of HPE

My HPE Account

This concludes this section of the lab.

Establishing a connection from HPE iLO to HPE GreenLake

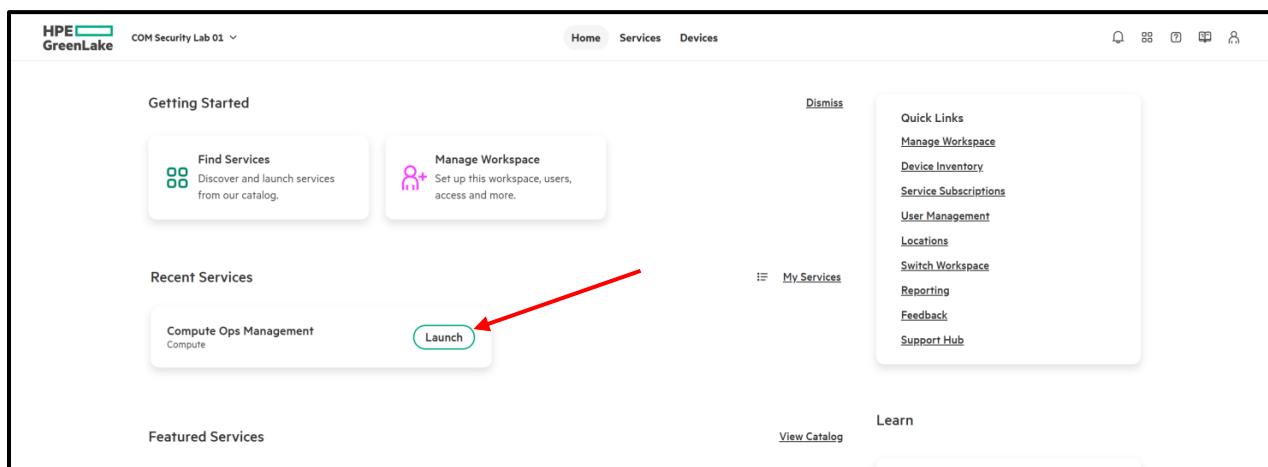
For our lab purposes, the HPE GreenLake Workspace company in this environment is called *COM Security Lab XX*.

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.

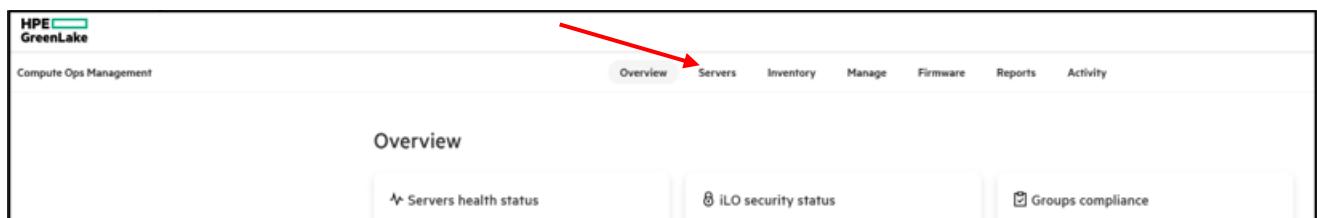
For more information regarding the security protocols and firewall requirements, consult the [HPE Compute Ops Management security guide](#).

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

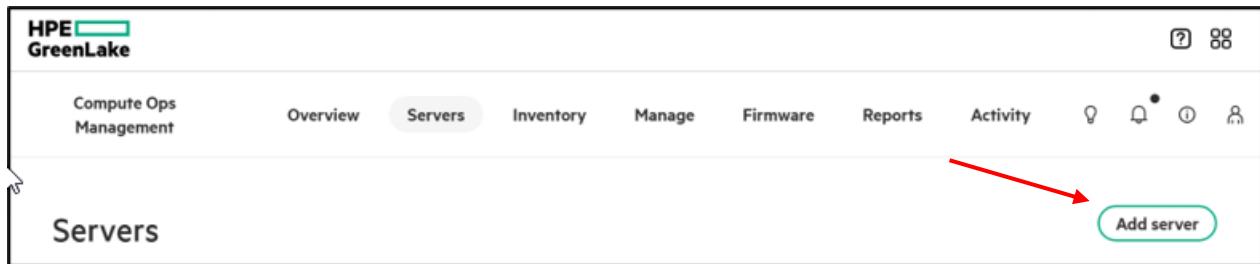
1. From the HPE GreenLake Recent Services section, choose the **Compute Ops Management Launch** button to connect to HPE Compute Ops Management main menu.



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



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



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

The screenshot shows the 'Add server' wizard, Step 1 of 3. The title is 'Connection type'. There is a note: '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.' A callout box contains the note: '⚠ Ensure that your HPE GreenLake Platform application role includes **edit** permissions for **Devices** and **Subscription Service**.'. Below this, there is a section for 'Server connection type' with two options: 'Direct connect' (selected) and 'Secure gateway'. At the bottom right is a 'Next' button.

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

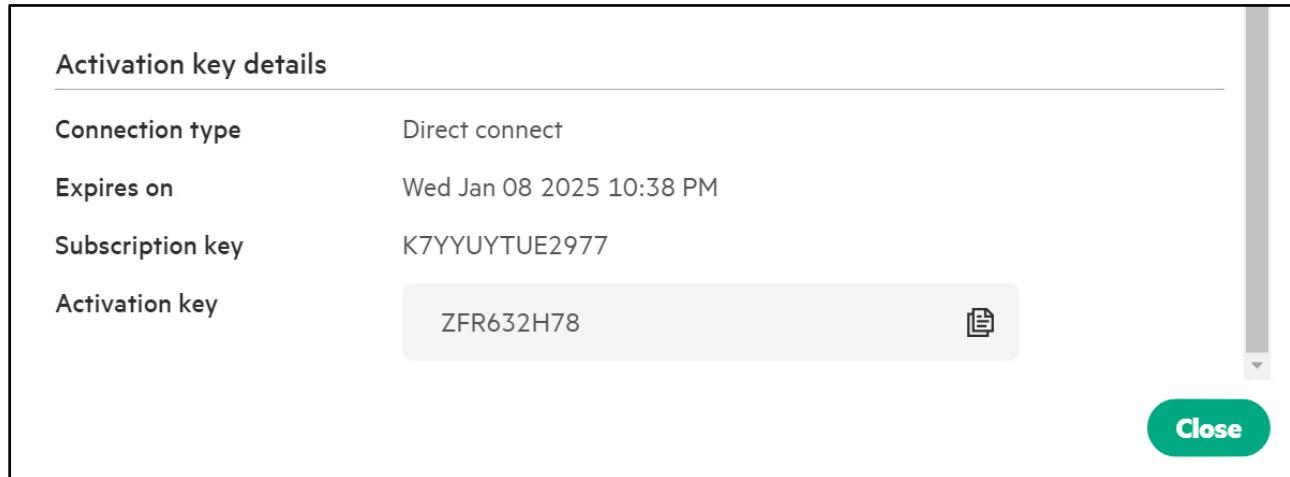
Review

Activation key details

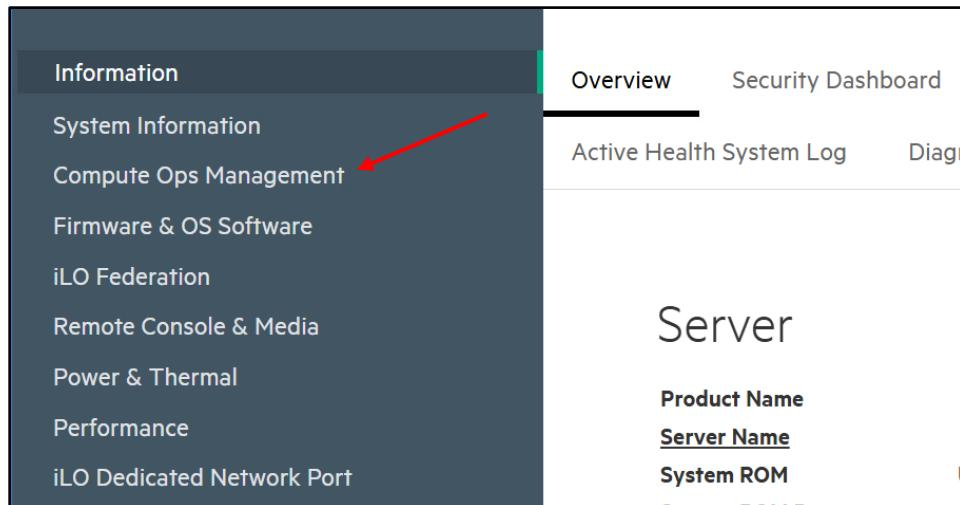
Connection type	Direct connect
Expiration	Wed Jan 08 2025 10:36 PM
Subscription key	K7YYUYTUE2977

Finish and generate activation key

7. 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.



8. 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.

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

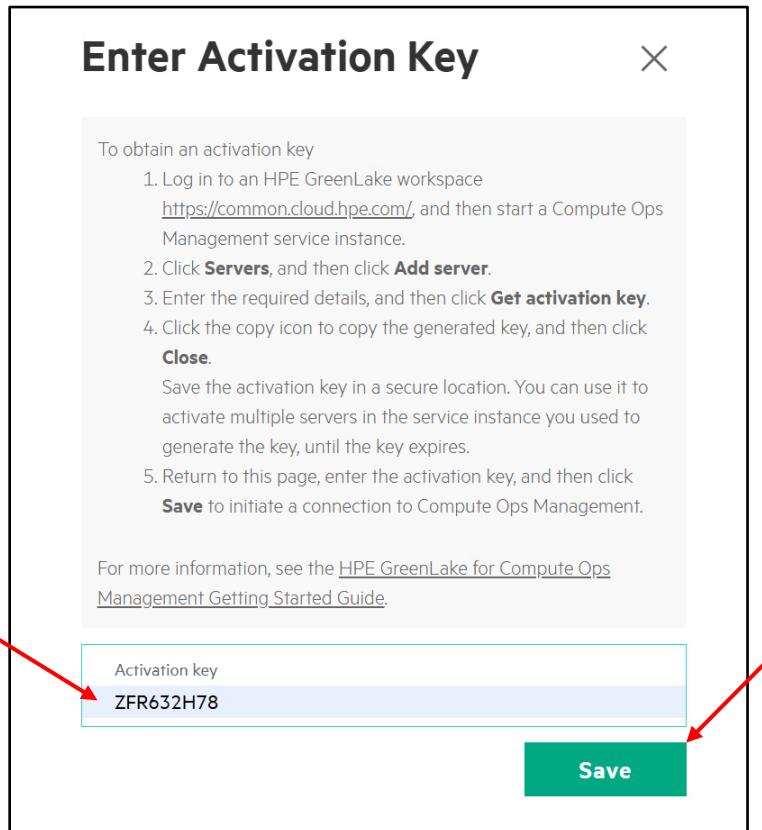
Recommendations([View a video tutorial](#)):
An activation key is required for iLO to connect to HPE Compute Ops Management. To obtain an activation key

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**.



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

The screenshot shows the 'Compute Ops Management' interface. At the top, it displays 'Connection Status' as 'Connected' with a green checkmark icon. Below that, 'HPE GreenLake Workspace ID' is listed as '04ac5888d75a11ef908216479ea8874e'. Under 'Connection Type', it says 'Direct'. A central box contains instructions: 'Use HPE Compute Ops Management to perform some next actions:' followed by two bullet points: 'Subscribe to email notification for real time health issues' and 'Assign location to automatically create a support case when hardware fails'. At the bottom left is a 'Edit Settings' link, and at the bottom right is a green 'Launch HPE GreenLake' button.

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.

The screenshot shows the 'Servers' page of the HPE Compute Ops Management interface. At the top, there's a navigation bar with tabs: Overview, Servers (which is selected and highlighted in blue), Inventory, Manage (with a red arrow pointing to it), Firmware, Reports, and Activity. Below the navigation is a section titled 'Servers' with three summary cards:

- Servers health status:** Shows 1 server with 1 warning (yellow circle).
- ILO security status:** Shows 1 server with 0 issues (grey circle).
- Needs attention:** Shows None.

Below the cards are search and filter tools, including a search bar, a dropdown for 'All servers', and icons for sorting and filtering. A table lists the server details:

Health	Name	Serial	ILO security	State	Baseline	Group	Power	Model
▲	localhost.management.hpe...	TWA4614501	Unknown	Retrieving server storage information in progress	--	--	On	ProLiant DL145 Gen11

On the right side, there's an 'Activity' sidebar with a log of recent events:

- Server health: localhost.management.hpe.local storage health changed to OK (3/5/2025 5:44:44 PM)
- Server health: localhost.management.hpe.local processors health

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**
Manage metrics data collection settings used for utilization reporting including sustainability.
- 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 when iLO indicates a hardware related service event
- Aruba Central integration**
Set up integration with Aruba Central to view server network adapter to switch connectivity.

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

[Create setting](#)

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 with a table of existing settings. A red arrow points to the 'Create setting' button at the top right of the table.

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

Activity

- Server disconnected
2M294600B1 disconnected from Compute Ops Management
8/26/2024 12:10:32 PM
- Server power
2M294600B1 powered on
8/26/2024 9:45:30 AM
- Server power
2M294600B1 powered off
8/26/2024 9:45:17 AM
- Group firmware compliance
Team06 firmware compliance state changed to Compliant
8/26/2024 9:13:52 AM
- Server automatic configuration
2M294600B1 automatic configuration is complete
8/26/2024 9:12:53 AM

[View all activity](#)

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 reference Patch 2024.04.00.01 + SPP
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 iLO5 3.04 along with support for RHEL 9.4.

[Learn more](#)

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 reference Patch 2024.04.00.01 + SPP
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

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 reference Patch 2024.04.00.01 + SPP
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 iLO5 3.04 along with support for RHEL 9.4.

[Learn more](#)

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

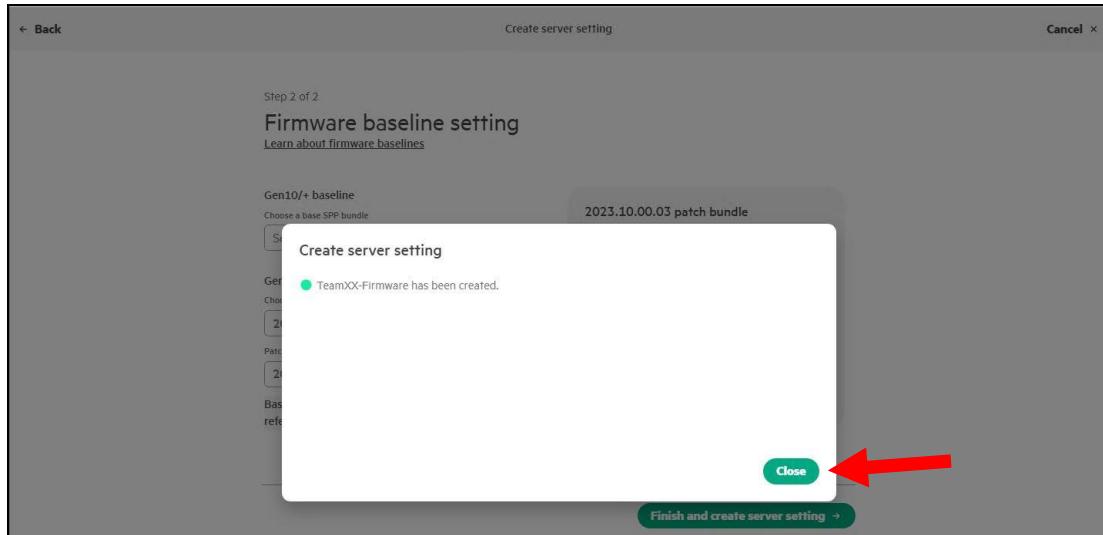
Baseline reference Patch 2024.04.00.01 + SPP
2024.04.00.00 (27 May 2024)

2024.04.00.01 patch bundle

Released: 27 May 2024
Base SPP of patch: 2024.04.00.00

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.

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	1 ...
Low Latency	BIOS/Workload profile	HPE pre-defined	0 ...
Mission Critical	BIOS/Workload profile	HPE pre-defined	0 ...
Team01/Firmware	Server firmware	User defined	1 ...
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 ...

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:

[Settings](#)

iLO settings enabled for security

Details

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
Type	HPE pre-defined

iLO settings

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.

1. 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 a red arrow. Other sections visible include 'Settings', 'Email notification policy preference', 'Metrics data collection', 'Data Services Cloud Console integration', 'ServiceNow integration', and 'Aruba Central integration'.

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

The screenshot shows the 'Groups' page in the HPE Compute Ops Management interface. It features a heading 'Let's get started by creating a group.' and a prominent green 'Create a group' button, which is also highlighted with a red arrow.

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*

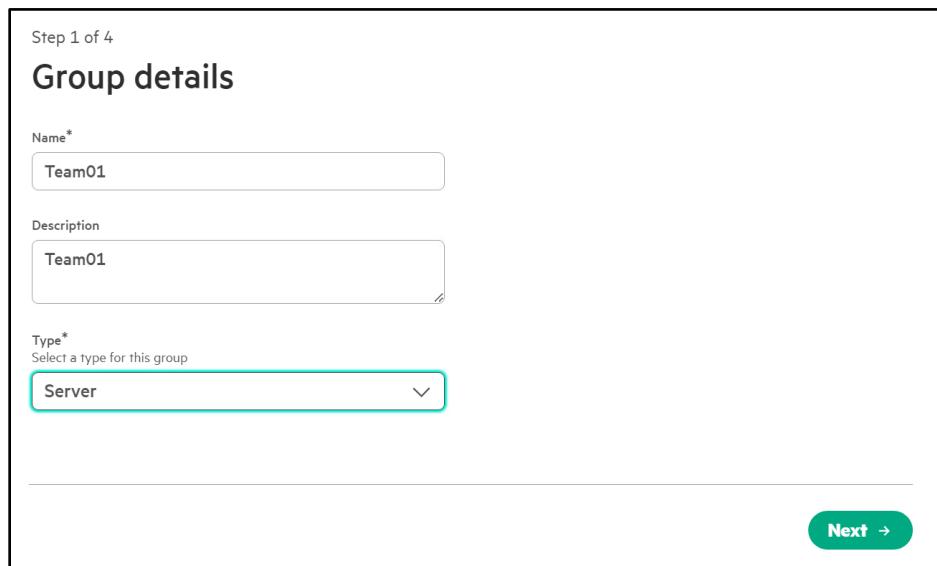
Description

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

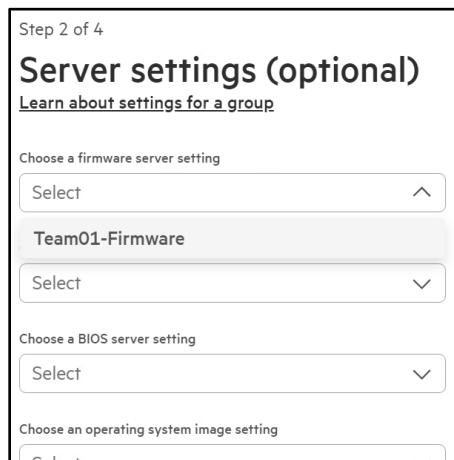
Select

Choose a BIOS server setting

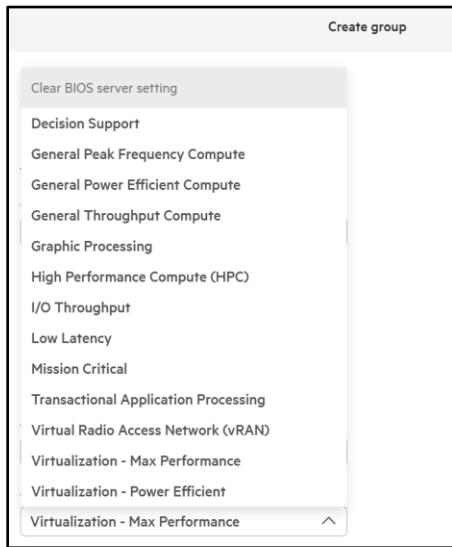
Select

Choose an operating system image setting

Select



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**.

Step 2 of 7

Server settings (optional)

[Learn about settings for a group](#)

Choose a firmware server setting

Team01-Firmware

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

Choose an internal storage server setting

Select

Choose a BIOS server setting

Virtualization - Max Performance

Choose an operating system image setting

Select

Choose an iLO server setting

iLO settings enabled for security

Choose an external storage server setting

Select

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](#)

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.

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

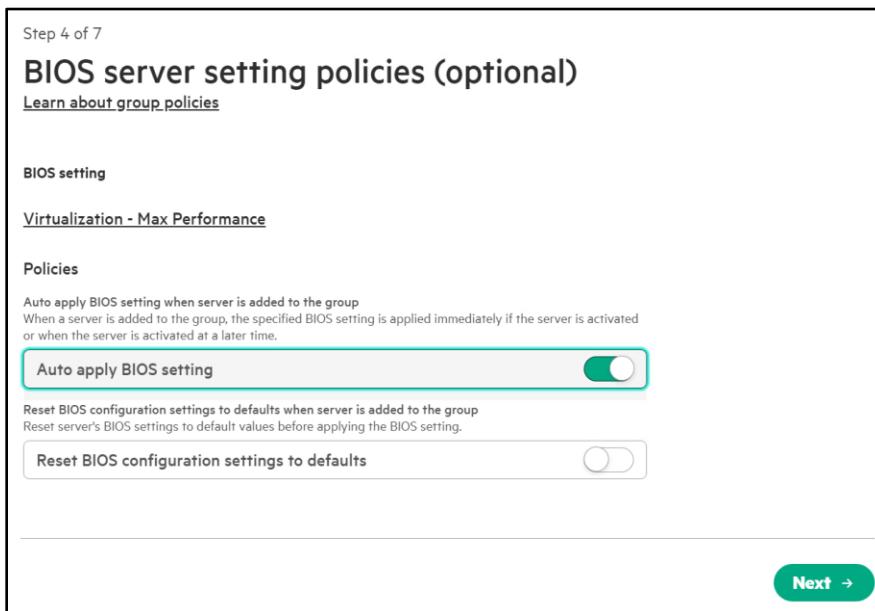
Auto apply BIOS setting when server is added to the group
When a server is added to the group, the specified BIOS setting is applied immediately if the server is activated or when the server is activated at a later time.

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

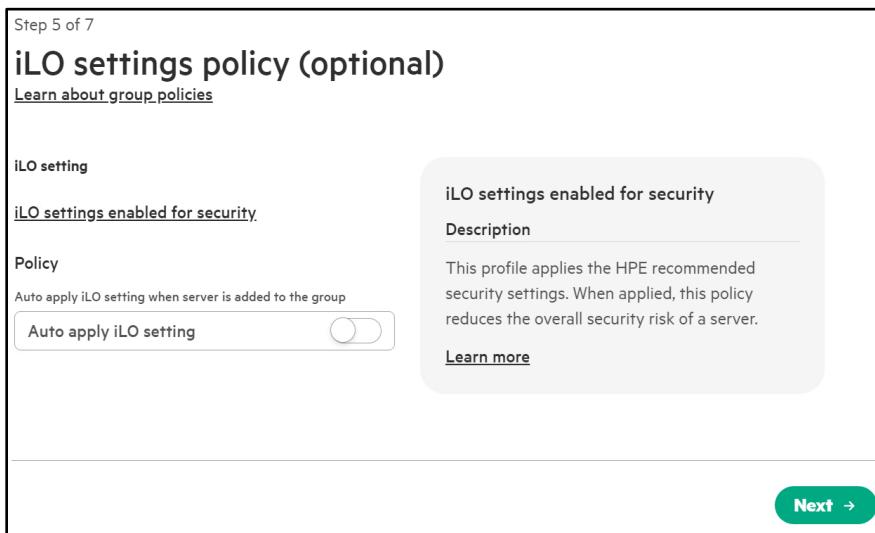
iLO settings enabled for security

Description

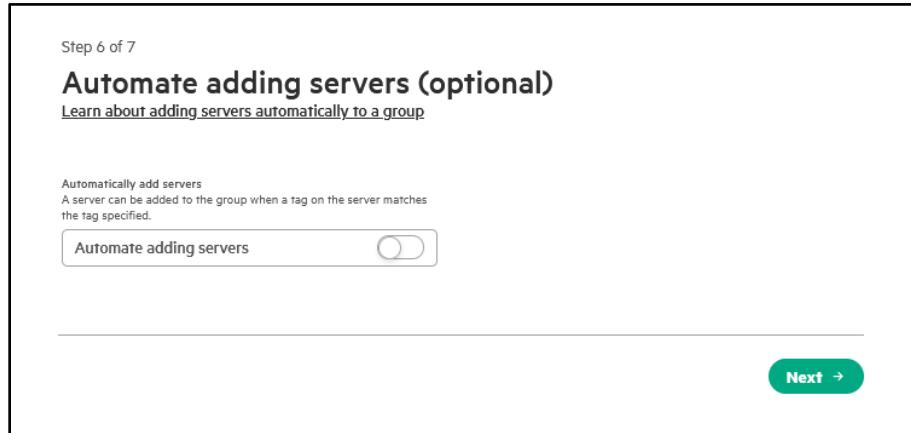
This profile applies the HPE recommended security settings. When applied, this policy reduces the overall security risk of a server.

[Learn more](#)

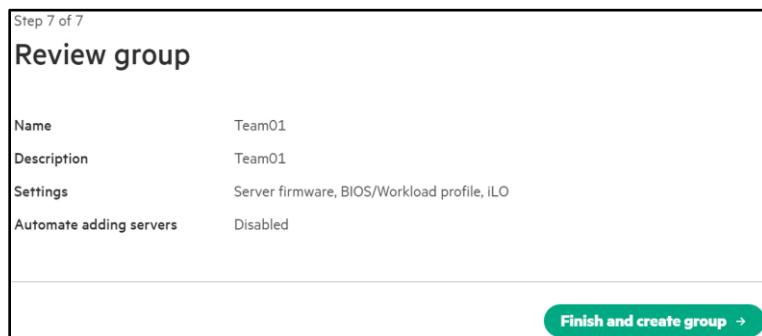
Next →



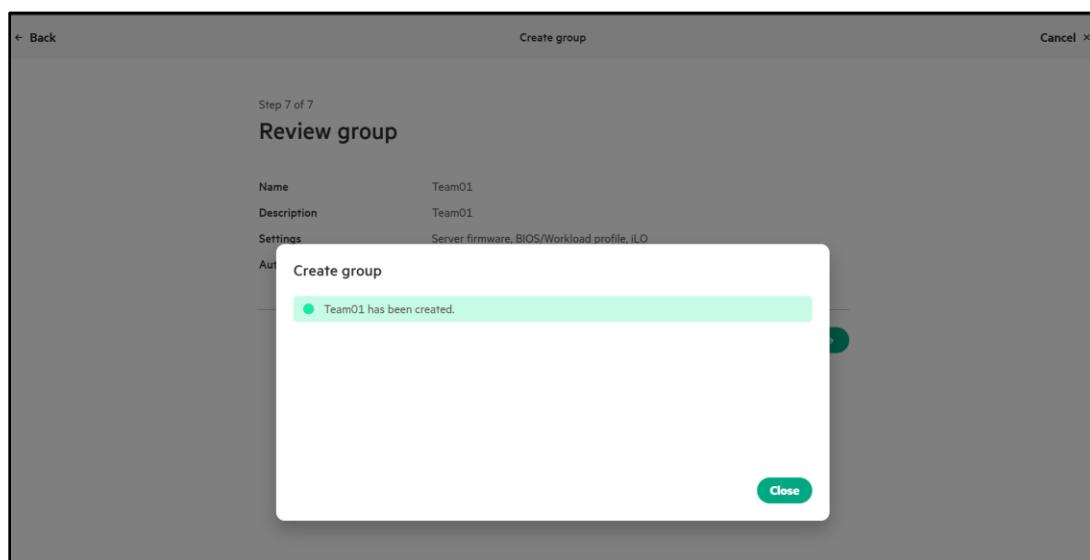
12. For the question of how we are adding our servers to the group, we are going to setup the group for manual addition of servers to the group. Select **Next** to move to the finish.



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	Team01-Firmware
BIOS/Workload profile	Virtualization - Max Performance
iLO	iLO settings enabled for security

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	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

Actions ▾

- Edit
- Delete
- Add servers**
- View servers
- Group: **Team01**
- Group: [Remove servers](#)
- Manager: [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](#)

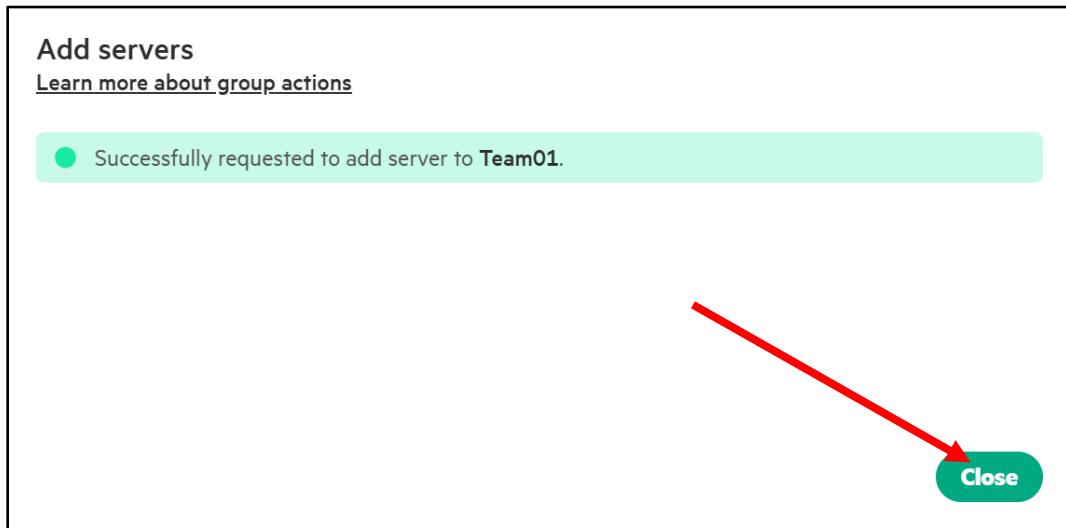
You are adding **1** server:

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.

The screenshot shows the 'Team01' server group details page. On the left, there are sections for '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), and 'Scheduled actions'. On the right, there is a 'Recent group activity' pane listing four items: '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), and 'Server automatic configuration' (2M2946009Z automatic configuration is complete, 1/28/2025 12:42:33 PM). The 'BIOS settings' section is also visible at the bottom of the pane.

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. Features 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 iLO 6 Security Dashboard. At the top, it displays the overall security status as "Risk". Below this, a table lists various security parameters with their current state 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

Recommendation: Enable the "Global 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
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 executions for trusted signatures. This configuration breaks the chain of trust established by iLO from power-on.
Recommendation: Enable the Secure Boot setting in the UEFI System Utilities.

Ignore - 0

Configure iLO ignore risk setting Cancel

4. 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"/>
SNMPv1	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.

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

ILO security status

Recommendation: Enable the "Global 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 System 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 firmware, and other system software executables for trusted signatures. This configuration breaks the chain of trust established by iLO from power-on.
Recommendation: Enable the Secure Boot setting in the UEFI System 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, 2:11 PM CDT

Configure iLO ignore risk setting **Cancel**

6. 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

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

SNMP Alerts

Trap Source Identifier
<input checked="" type="radio"/> ILO Hostname
<input type="radio"/> OS Hostname
<input checked="" type="checkbox"/> SNMPv1 Request
<input checked="" type="checkbox"/> SNMPv1 Trap
<input type="checkbox"/> SNMPv3 Request
<input checked="" type="checkbox"/> SNMPv3 Trap
<input checked="" type="checkbox"/> Cold Start Trap Broadcast
Periodic HSA Trap Configuration
Disabled

SNMPv3 Settings

Send Test Alert **Apply**

Apply

7. 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

SNMPv3 Trap

Cold Start Trap Broadcast

Periodic HSA Trap Configuration

Disabled

Send Test Alert **Apply**

8. Click the **Apply** button.
9. 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"/>
SNMPv1	OK	Disabled	<input type="radio"/>
Last Firmware Scan Result	OK	OK	<input type="radio"/>

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

The screenshot shows the 'Compute Ops Management' interface. On the left, a server named 'com-team20.hol.enablement.local' is selected. The main panel displays various server details like Health (OK), State (Connected), Group (Team20-COMAVC), Model (PHILIP DL365 Gen11), and ILO security status (At Risk). A red box highlights the 'iLO security status' section, which shows 'OK - 7'. Below this, several security configurations are listed: Authentication Failure Logging (Enabled), IPMI/DCMI Over LAN (Disabled), Last Firmware Scan Result (Passed), Minimum Password Length (Set to 8 characters), Require Host Authentication (Enabled), SNMPv1 (Disabled), and Security Override Switch (Disabled). At the bottom of the red box are two buttons: 'Configure iLO ignore risk setting' and 'Cancel'.

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](#).

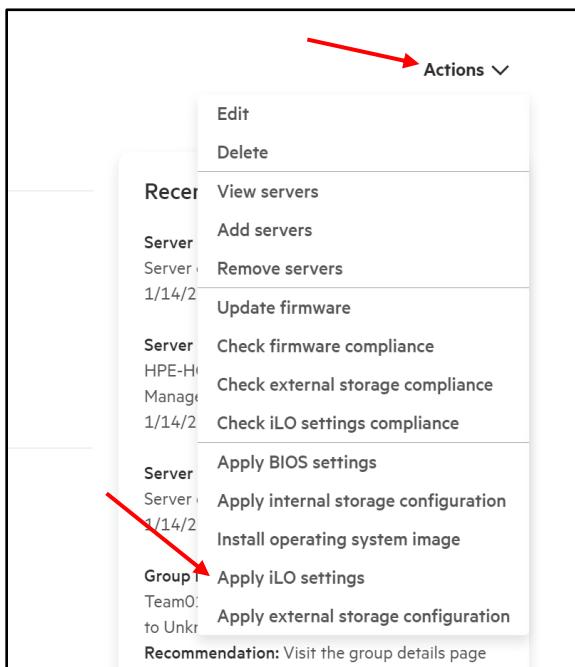
11. We will now utilize Compute Ops Management to push out all the recommended iLO Security Settings to our assigned Server. Let's click on **Manage** and then **Groups**.

The screenshot shows the 'Manage' section of the HPE GreenLake Compute Ops Management interface. The top navigation bar has tabs for Overview, Servers, Inventory, Manage (which is highlighted with a red arrow), and Firmware. Below the navigation, there are two cards: 'Groups' and 'Settings'. The 'Groups' card is active, showing a brief description: 'Groups allow easier device management of server and OneView appliances.' The 'Settings' card shows a similar brief description: 'Settings allow consistent configuration management across devices in a group.'

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

1 item						
Health	Name	Type	Security	Devices	Settings	Comp
●	Team01	Server	At risk	1	3	Unkn

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



14. 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](#)

⚠ 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

15. 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.

16. Click the **X** to close this popup.

17. 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

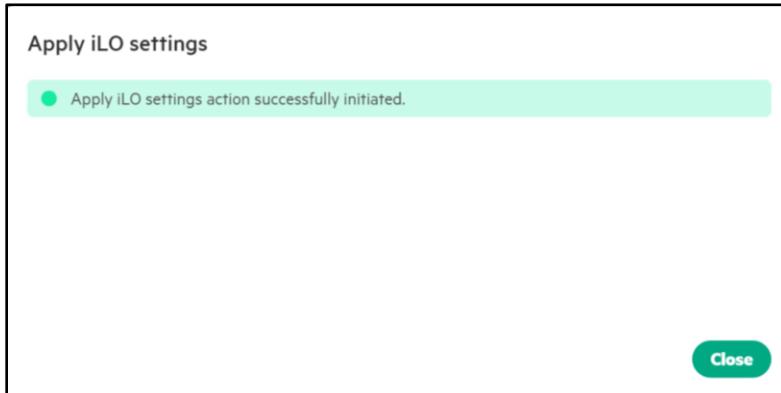
1 items

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

Next →

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

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

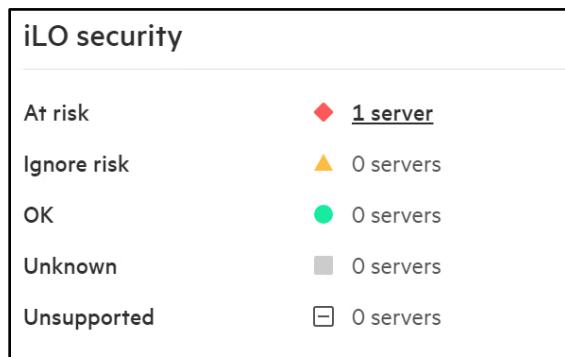


20. In the **Recent group Activity**, you should now see the **iLO settings being successfully applied** and the **settings compliance** changed to **Compliant**.

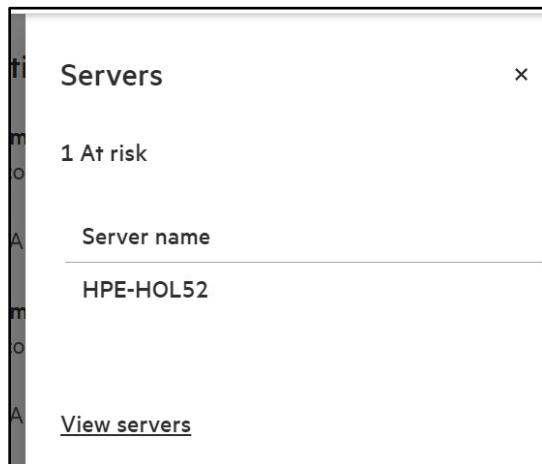
A screenshot of a "Recent group activity" section. It contains four log entries:

- 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

21. 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**.



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



23. 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			
Details							
State Connected							
Group	<u>Team01</u>						
Connection type	Direct						
Model	ProLiant DL325 Gen10 Plus						
Serial number	CN70461J1W						
iLO security status	◆ At risk	<u>Details</u>					
UUID	34383350-3737-4E43-3730-3436314A3157						
iLO IP address	<u>172.30.231.109</u>						
		<u>Remote console</u>					

24. 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
Default SSL Certificate In Use
Management processor's default self-signed certificate is in use.
Recommendation: Import a certificate signed by a trusted certificate authority.
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 executables for trusted signatures. This configuration breaks the chain of trust established by iLO from power-on
Recommendation: Enable the Secure Boot setting in the UEFI System Utilities.

25. 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**.

26. Return to the iLO web browser of your assigned Server.

The screenshot shows the iLO 5 web interface. The top bar displays the iLO 5 logo and the date 3.09 Oct 08 2024. The main title is "Information - iLO Overview". On the left sidebar, under the "Information" section, there are links for System Information, Compute Ops Management, Firmware & OS Software, and iLO Federation. The "Overview" tab is selected in the top navigation bar. The main content area displays the text "Server".

27. 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.

The screenshot shows the iLO 5 Administration - User Administration page. The top bar displays the iLO 5 logo and the date 3.09 Oct 08 2024. The main title is "Administration - User Administration". Under the "User Administration" tab, there is a table titled "Local Users" showing three entries: Administrator, TechEnablement, and ReadOnly. The "New" button is highlighted with a green border at the bottom of the table. The table columns include Login Name, User Name, Status, and several icons for managing users.

Local Users			
Administrator	Administrator	Enabled	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ X ✓
TechEnablement	TechEnablement	Enabled	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ X
ReadOnly	ReadOnly	Enabled	✓ ✓ X X X X X X X X X X

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

Login Name	HPE_Admin1
User Name	HPE Admin1
New Password	hpent123
Confirm Password	hpent123
Role	Administrator

The screenshot shows two side-by-side panels. The left panel is titled 'Add Local User' and contains a 'User Information' section with fields for Login Name (HPE_Admin1), User Name (HPE_Admin1), New Password (*****), and Confirm Password (*****). The right panel is titled 'User Permissions' and shows the 'Administrator' role selected. Under 'Privileges', several checkboxes are checked, including Login, Remote Console, Virtual Power and Reset, Virtual Media, Host BIOS, Configure iLO Settings, Administer User Accounts, Host NIC, Host Storage, and Recovery Set. A dropdown menu for IPMI/DCMI Privilege shows 'administrator'. At the bottom is a green 'Add User' button.

29. 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 screenshot shows a red error message box containing the text: "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." Below the message is a green 'Add User' button.

30. Set the password as **HPESecurePassw0rd!** 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 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.

So 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 certificate 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:

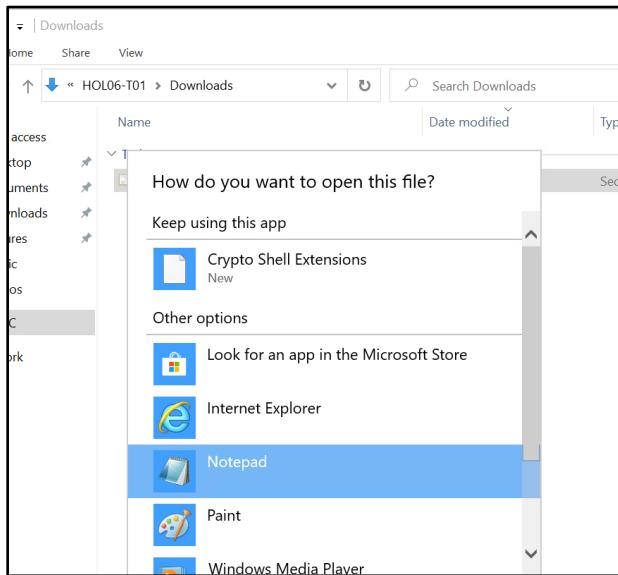
Current [HOLCA01-CA] ▾

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.

A screenshot of a Notepad window titled 'certnew - Notepad'. The window contains the full text of a certificate. The text starts with '-----BEGIN CERTIFICATE-----' and ends with '-----END CERTIFICATE-----'. The content is a long string of characters representing the certificate's data, including various identifiers, timestamps, and digital signatures. At the bottom of the Notepad window, the status bar shows '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/

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**.

SSL Certificate Information

SSL Certificate (2)

SSL Certificate Information

Issued To	CN = IL02M294600DF.hol.enablement.local, O = Hewlett Packard Enterprise, OU = ISS, L = Americas, ST = Houston, C = US
Issued By	CN = Default Issuer (Do not trust) , O = Hewlett Packard Enterprise, OU = ISS, L = Americas, ST = Houston, C = US
Valid From	Jan 28 17:26:14 2025 GMT
Valid Until	Jan 28 17:26:14 2040 GMT
Serial Number	6c83584cabcb2e4cb

Automatic Certificate Enrollment

Enrollment Service: Disabled

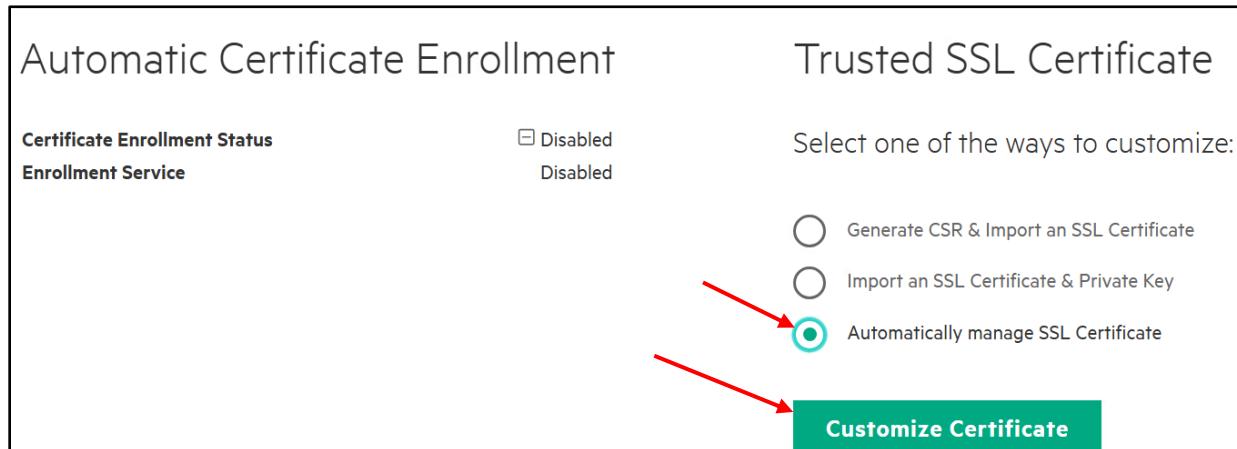
Trusted SSL Certificate

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

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)

Server URL	Country (C)
1 https://holca01.hol.enablement.local/certsrv/mscep/mscep.dll	US
Challenge Password	State (ST)
2 *****	Houston
CA Certificate Name	City or Locality (L)
/DC=local/DC=enablement/DC=hol/CN=HOLCA01-CA	Americas
CA Certificate	Organization Name (O)
3 DrDuMBAGCSsGAQQBgjcVAQODAgEAMA0GCSqGSIb3DQEBCwU AA4IBAQAP5SPNsy8P MWZ3ETgOfKSwC8BoKrsbfgsaS7tC6pSvQXUgWV33725WEthUSi XjoMs1tk2YEWba OJOXbJx9Vt2ldBnRTi6XYwHfXLFG2YS2bdCqtFeBe2F1LVKQv9 zoCgE31qxBne wjkFAa1p57EWCE9kEkofEibWvmb2TCb77DQU9WeGxmXnpts0Q WSsoqDZlBiXSeg I1/8mx93SV9iFMdexvgyH2ZhTGoZ3UOPRwMgXXO3R0NTz1CB/4 KY1Tx+eZkLVUS1 cfdyAOjywPjlJQlvymae12kiy6mYMTam2e2jY7xZ5ZJp8TjOpTeOku uZmAANDNG9 ZePebeHDi2Ne -----END CERTIFICATE-----	Hewlett Packard Enterprise
	Organizational Unit (OU)
	ISS
	Common Name (CN)
	ILO2M294600DF.hol.enablement.local
	<input checked="" type="checkbox"/> Include iLO IP Address(es)

12. Then click **Enable**.
13. To see the progress of the certificate enrollment status, refresh the page by clicking on the **SSL certificate** tab.

Information - Automatic Certificate Enrollment

Certificate Enrollment Status

Enrollment Service In Progress
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

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
171	⚠	Security Configuration	Unable to complete SSL certificate enrollment since validation of the issued certificate failed.	02/25/2025 14:33:56	1	Security, Administration, Configuration
170	⚠	Security Configuration	SSL certificate could not be imported since the input certificate has incorrect purpose.	02/25/2025 14:33:56	1	Security, Administration, Configuration
169	ⓘ	Security Configuration	Certificate enrollment service is enabled.	02/25/2025 14:33:56	1	Security, Administration, Configuration

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

X

Certificate Enrollment Status	◆ Failed ←
Enrollment Service	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://holcert01.hol.enablement.local/certsrv/mscep/mscep.dll</code>	Country (C) US
Challenge Password	State (ST) Houston
CA Certificate Name <code>/DC=local/DC=enablement/DC=hol/CN=hol-HOLCERT01-CA</code>	City or Locality (L) Americas
CA Certificate	Organization Name (O) Hewlett Packard Enterprise
	Organizational Unit (OU) <small>optional</small> Compute
	Common Name (CN) <code>ILO2M294600DF.hol.enablement.local</code>
	<input type="checkbox"/> Include iLO IP Address(es) <small>optional</small>

Update Disable ←

15. A successful Certificate Enrollment will show as:

SSL Certificate Information

Issued To	C = US, ST = Houston, L = Americas, O = Hewlett Packard Enterprise, OU = ISS, CN = ILO2M294600DF.hol.enablement.local
Issued By	DC = local, DC = enablement, DC = hol, CN = HOLCA01-CA
Valid From	Mar 4 05:31:41 2025 GMT
Valid Until	Mar 4 05:31:41 2026 GMT
Serial Number	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

Issued To	C = US, ST = Houston, L = Americas, O = Hewlett Packard Enterprise, OU = ISS, CN = ILO2M294600DF.hol.enablement.local
Issued By	DC = local, DC = enablement, DC = hol, CN = HOLCA01-CA
Valid From	Mar 4 05:31:41 2025 GMT
Valid Until	Mar 4 05:31:41 2026 GMT
Serial Number	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

Information - Security Log

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

Search

ID	Severity	Class	Description	Last Update	Count	Category
181	Info	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	Info	Security Configuration	SSL certificate enrollment is successful. Reset iLO to use the new certificate.	02/25/2025 14:51:19	1	Security, Administration, Configuration
179	Info	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

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

iLO Self-Test Results

ILO Health: ✓

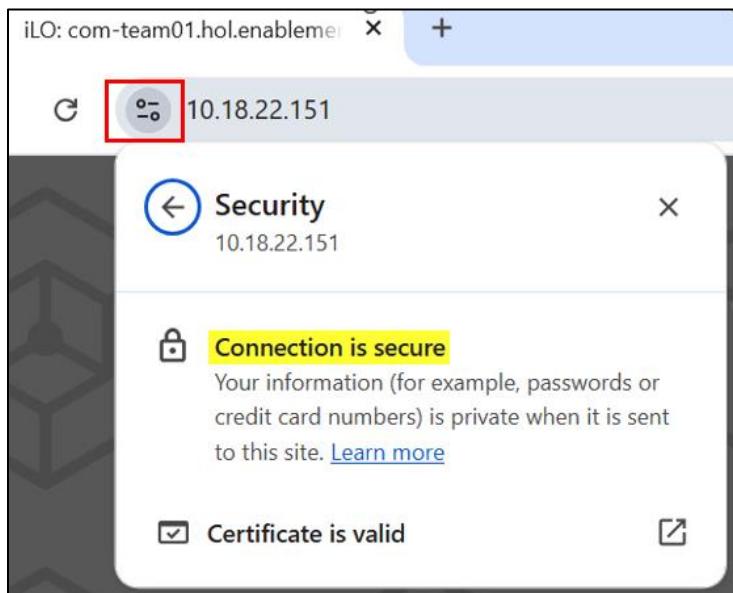
	↑ Status	Notes
Power Management Controller	○	Version 1.1.4
CPLD - PAL0	○	ProLiant DL160 Gen10 System Programmable Log
NVRAM data	●	
Embedded Flash	●	
EEPROM	●	Controller firmware revision 2.11.00
Host ROM	●	
Supported host	●	
ASIC Fuses	●	

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.



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**.

iLO security status

◆ At risk - 1

● OK - 10

Authentication Failure Logging
iLO is configured to log authentication failures in the event log.

Default SSL Certificate In Use
The Default SSL Certificate on security dashboard is OK.

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

HPE Compute Ops Management Secure Gateway

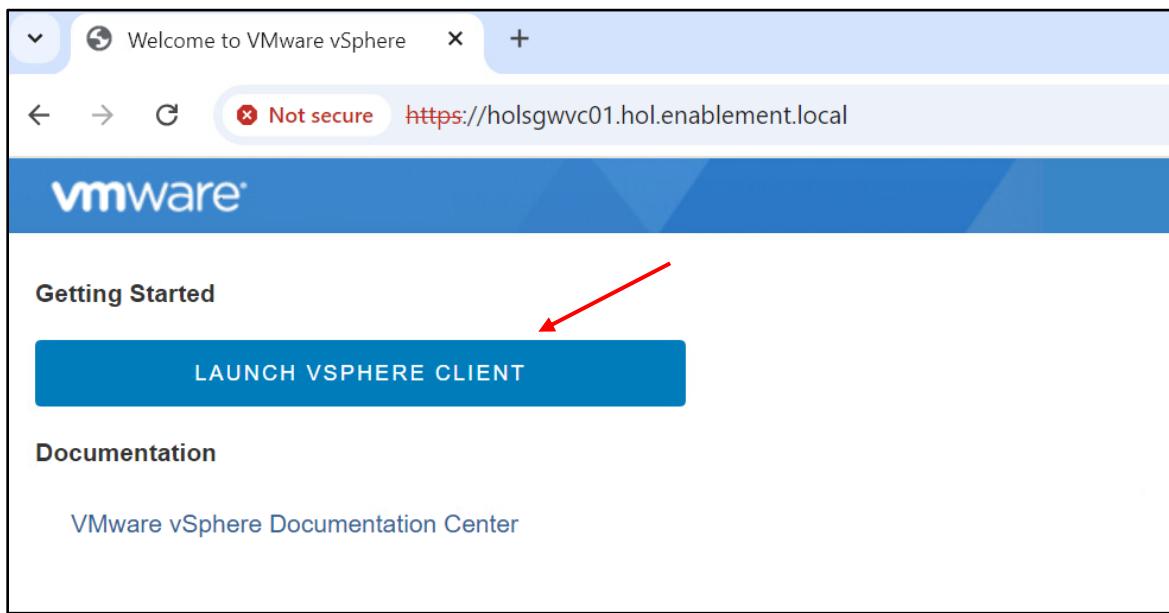
HPE Compute Ops Management customers can aggregate their on-premises HPE iLO connections over a single outbound connection to the management solution. Compute Ops Management secure gateway is an on-premises appliance deployed as a virtual machine.

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

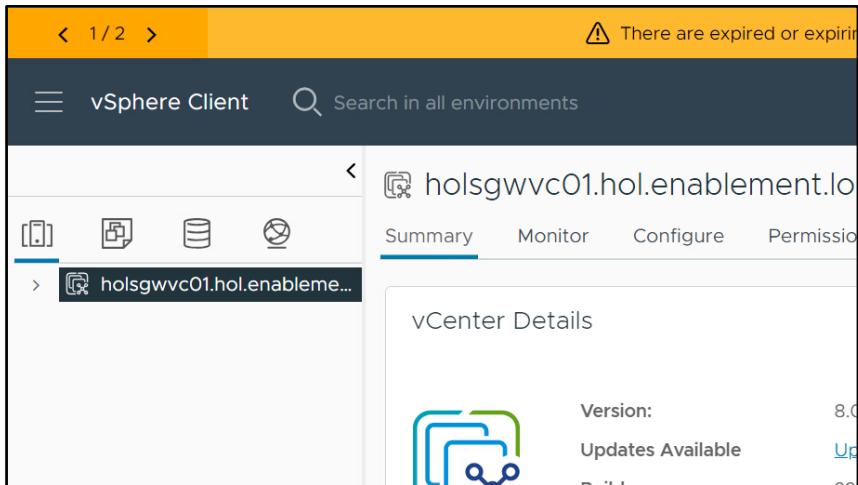
In this portion of the lab, we will focus on deploying an OVF Template supplied by HPE to provision the Virtual Machine Appliance which will function as the Secure Gateway for Compute Ops Management.

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**.

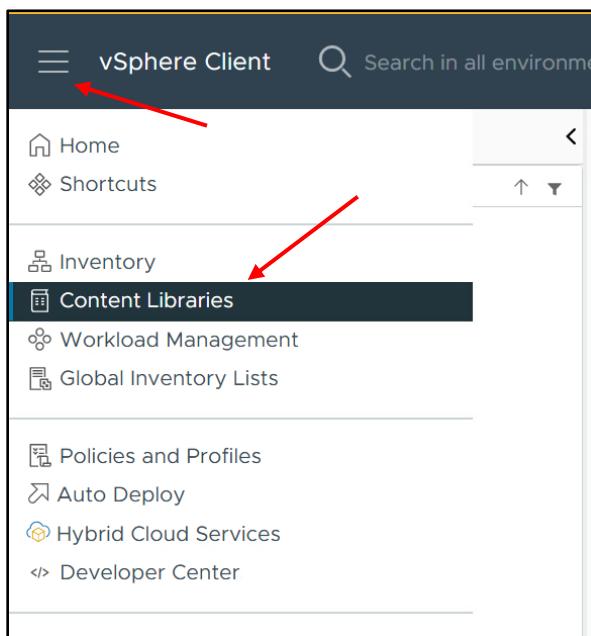


3. Use credentials **Administrator@vsphere.local** and **TechPr02025!** as the password.

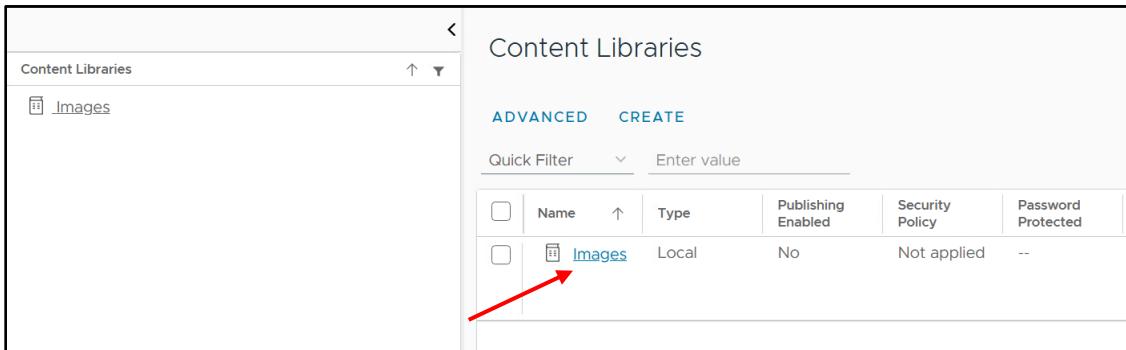
4. You should be now logged in to the vSphere Client



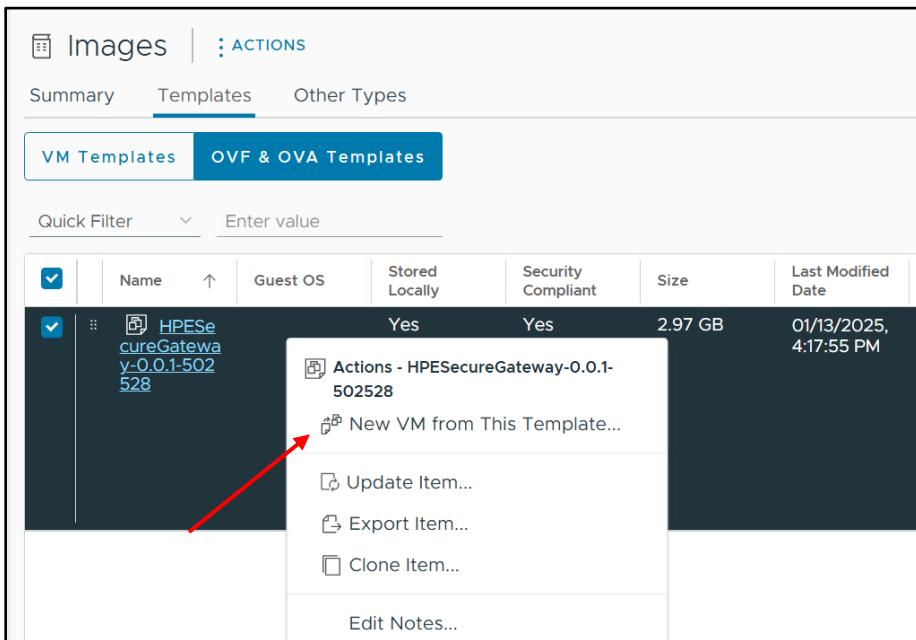
5. On the **left-hand side** of the screen, expand out the **vSphere Client menu**, and click on **Content Libraries**.



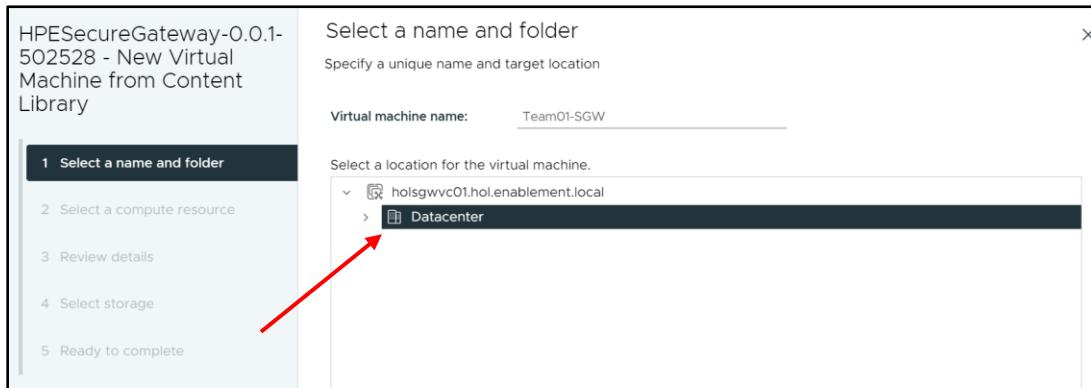
6. Click on **Images**.



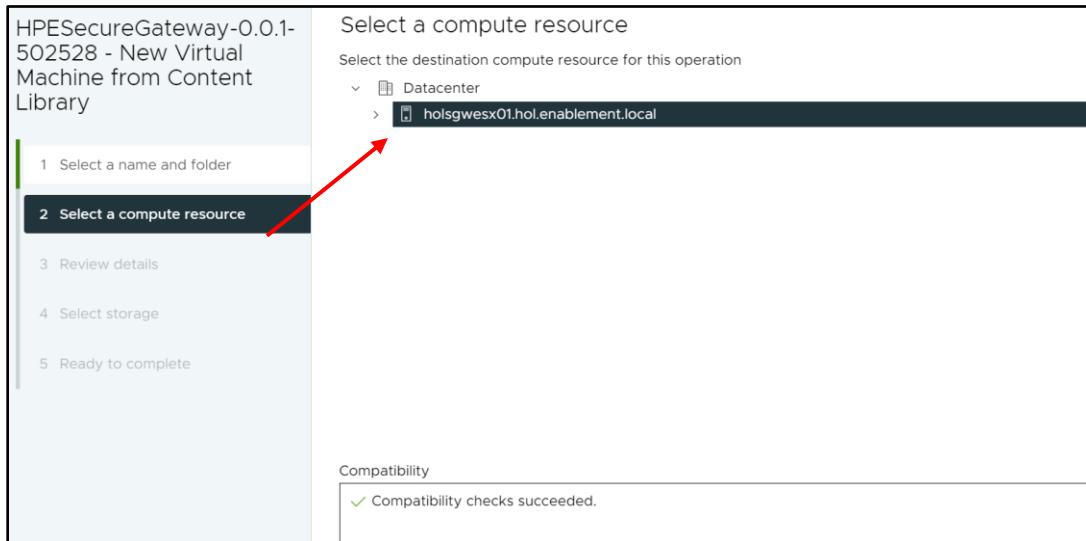
7. Right click on the **HPESecureGateway-X.X.X file** and select **New VM from This Template...**



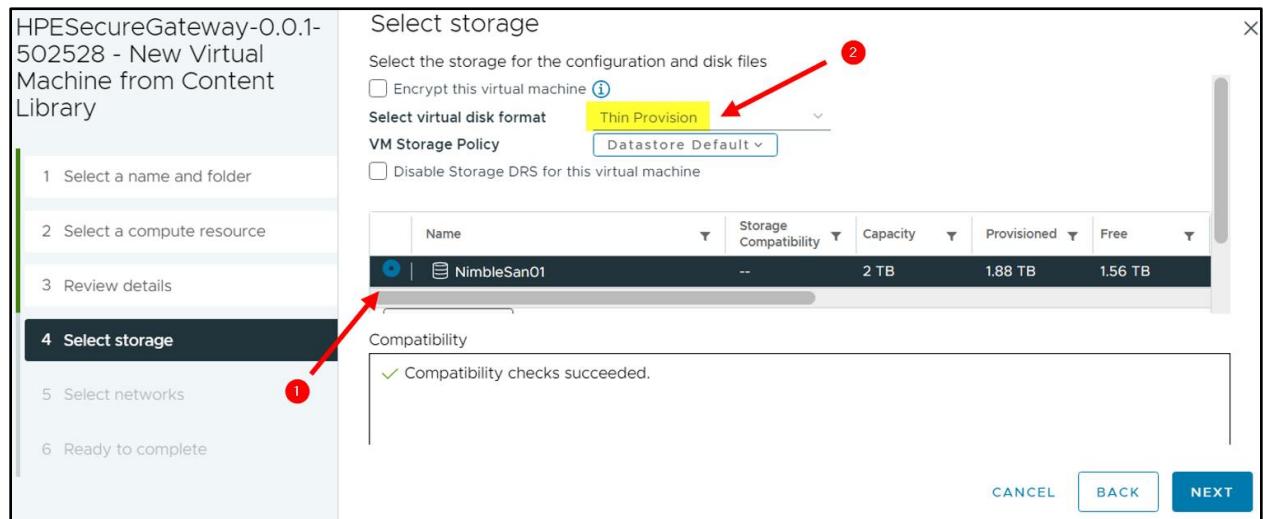
8. Set the Virtual Machine name as **TeamXX-SGW** where **XX** is your team number and select **Datacenter** as the location for the VM.



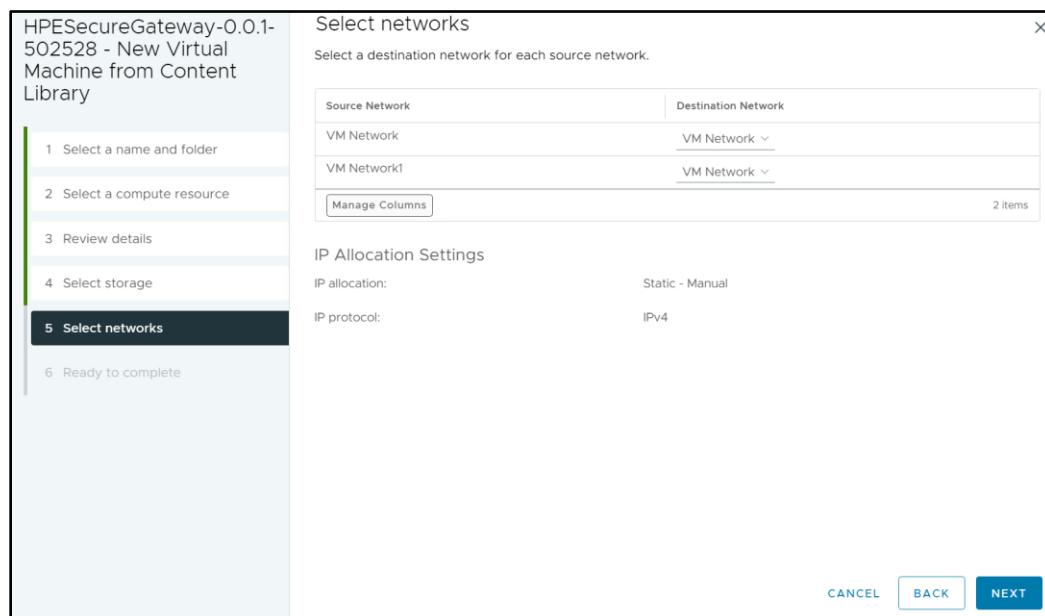
9. Click **holsgwesx01.hol.enablement.local** as the compute resource, then **Next** to proceed.



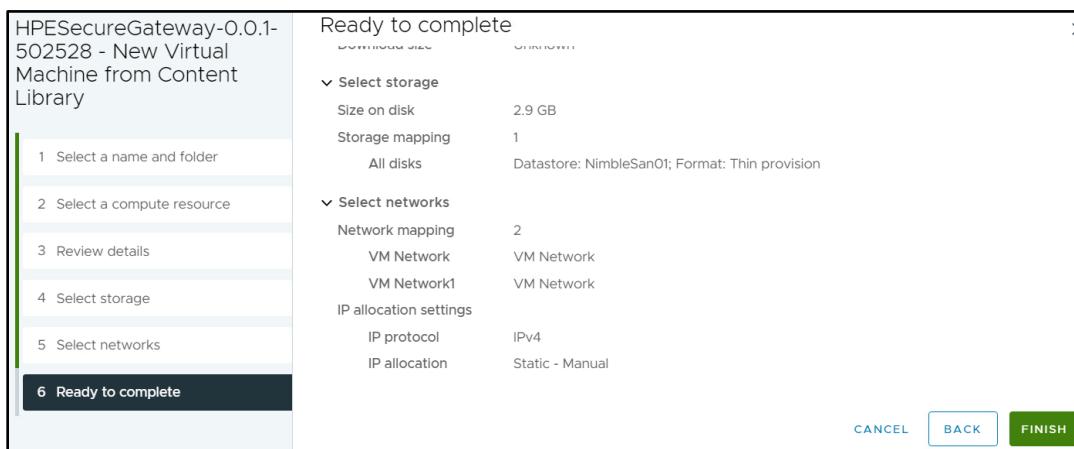
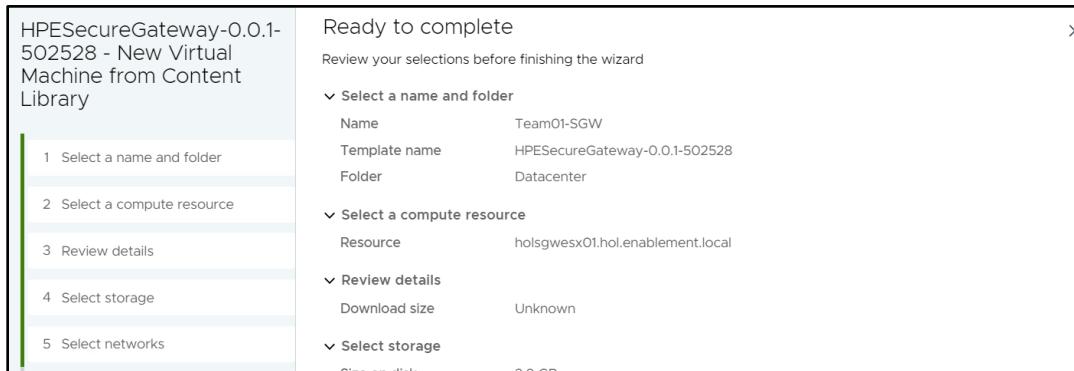
10. Click **Next** on **Review Details** and then for **Select Storage**, click **NimbleSan01**, change **Select virtual disk format** to **Thin Provision** and hit **Next**.



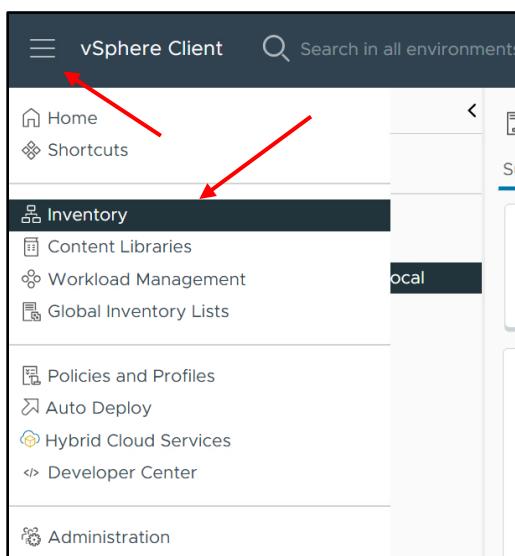
11. Leave the **defaults selected** for **Select Networks** and then **hit Next**.



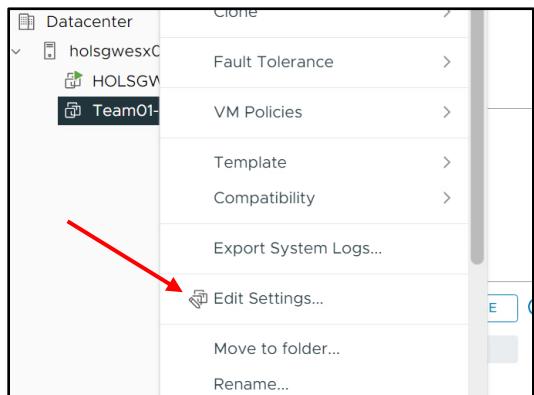
12. One last check and then hit **Finish** to complete the deployment.



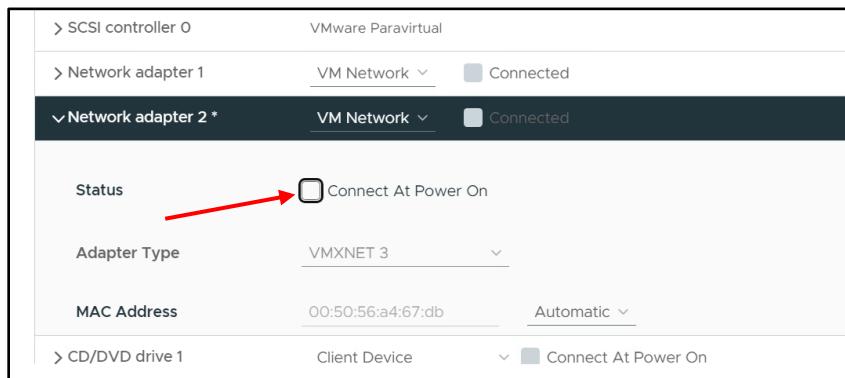
13. You can now navigate back to **Inventory Page** where you will see your **VM has been provisioned**.



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.



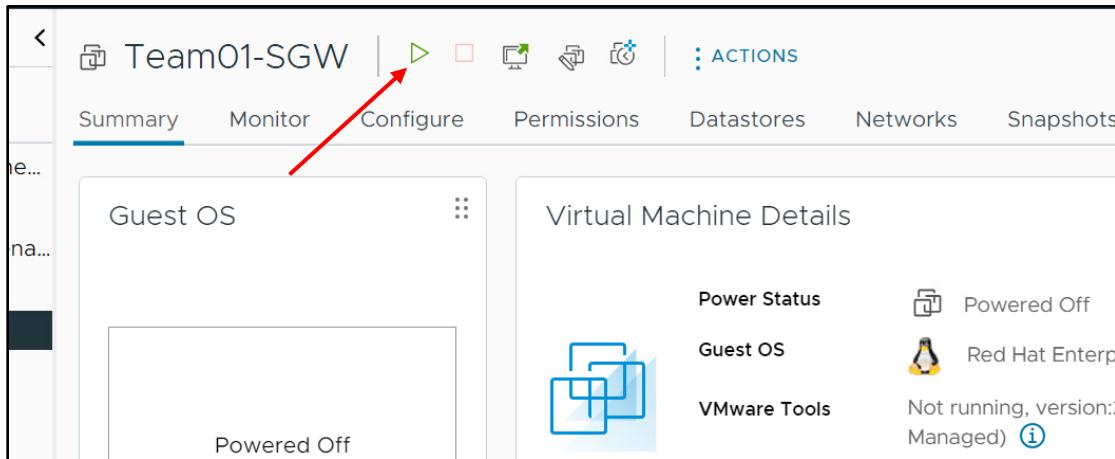
This concludes this section of the lab.



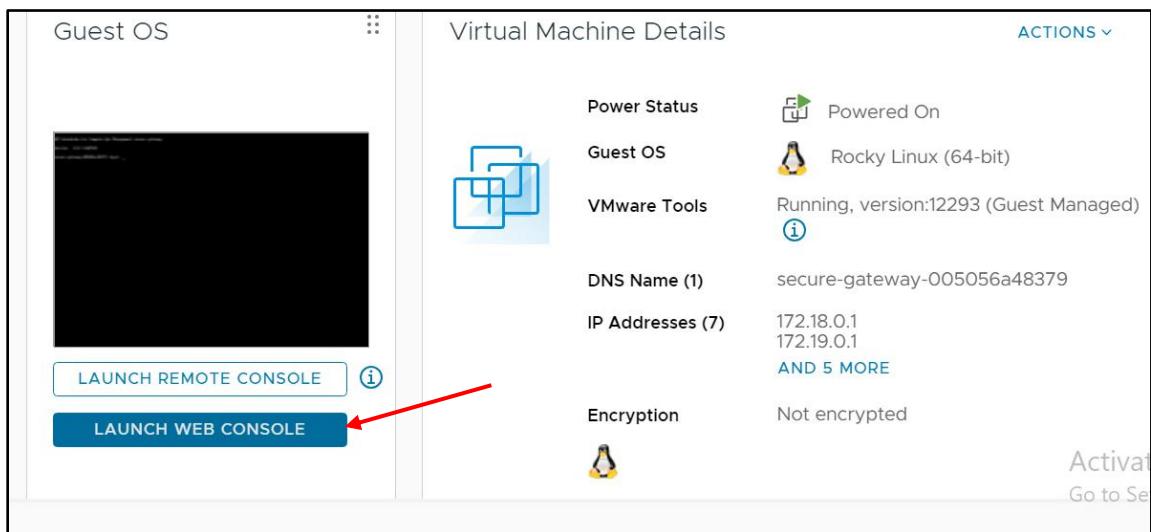
Configuring the Secure Gateway and connecting to COM

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.

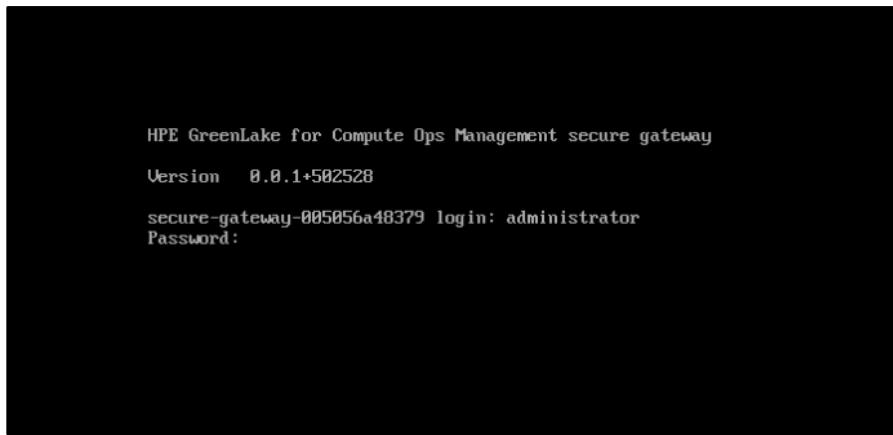
1. There are multiple ways to power on a VM, **click the Green Play button** or any alternative you prefer.



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 **HPESecurePassw0rd!** 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
team01-sgw.hol.enablement.local

IP address source

Team Number	Full qualified domain name	IP address
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**

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

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**.

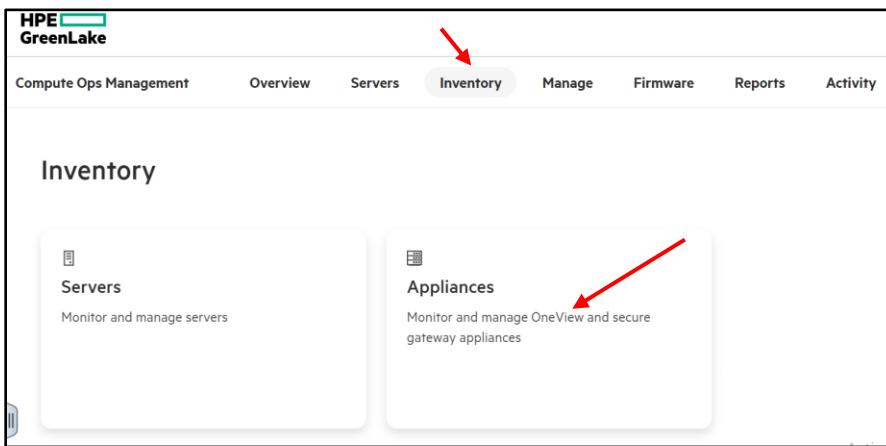
12. In the **DNS** Configuration area, enter **10.18.20.111** for the **Primary DNS Server**.

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

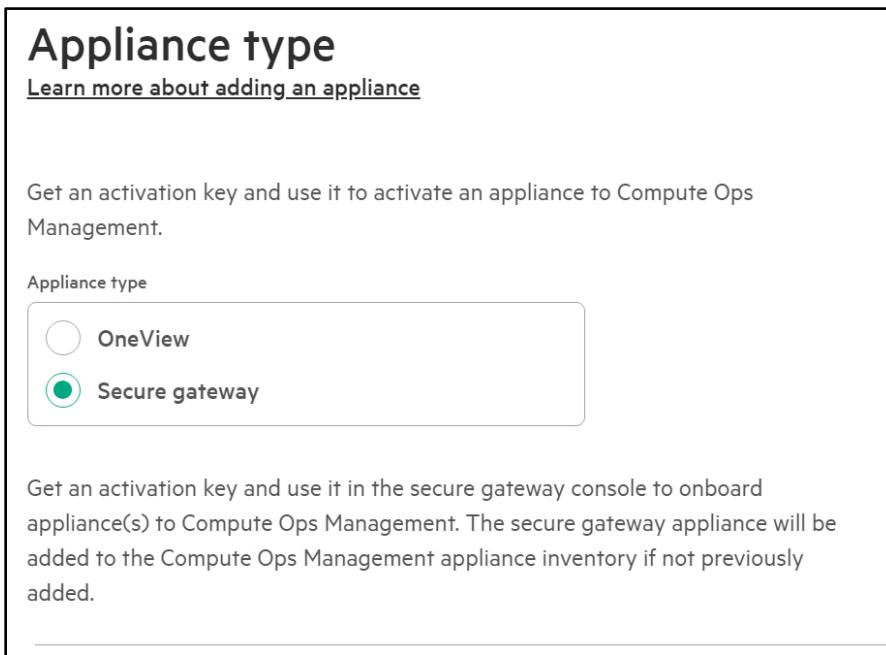
14. Once all entered correctly, select **Next** to proceed.

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
10.18.20.51
Prefix length
22
Gateway
10.18.20.1
Domain name server
Preferred DNS server (required)
10.18.20.111
Alternate DNS server (optional)
10.18.20.112
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**.



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



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**.

Step 3 of 3

Review

[Learn more about adding an appliance](#)

Activation key details

Appliance type Secure gateway

Expires on 1/10/2025 11:15 PM

[Finish and generate activation key](#)

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

Activation key

Use this activation key in the secure gateway console to onboard appliances(s) for Compute Ops Management. The same activation key can be used to onboard multiple secure gateway appliances. The secure gateway appliance will be added to the Compute Ops Management appliance inventory if not previously added.
[Learn more](#)

Activation key details

Appliance type Secure gateway

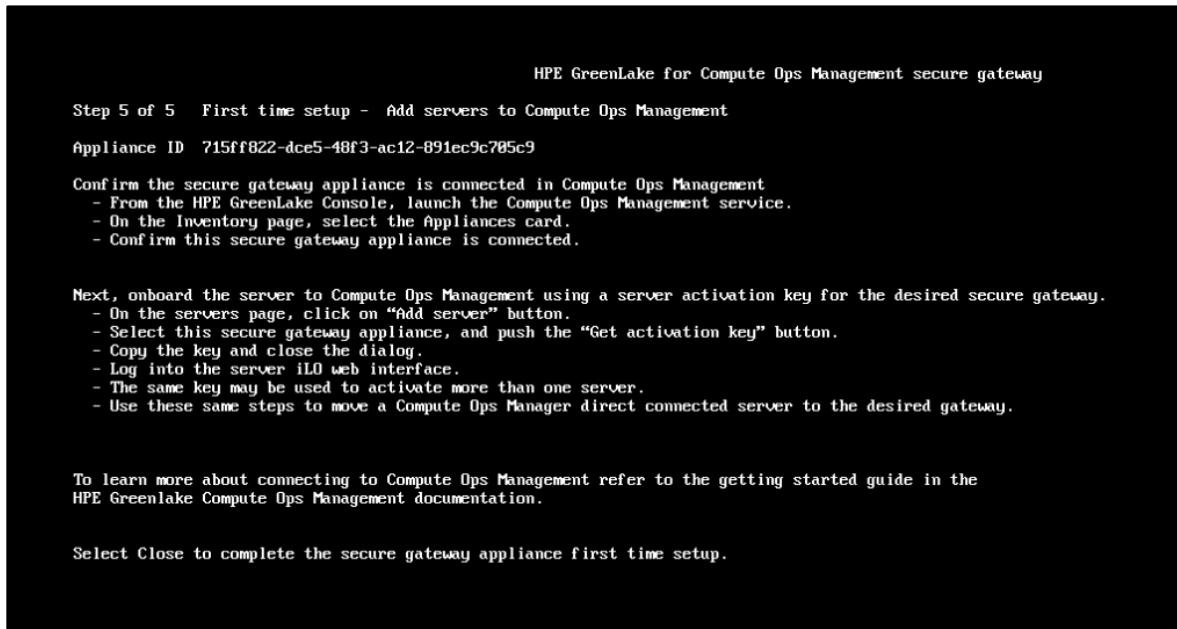
Expires on 1/10/2025 11:16 PM

Activation key

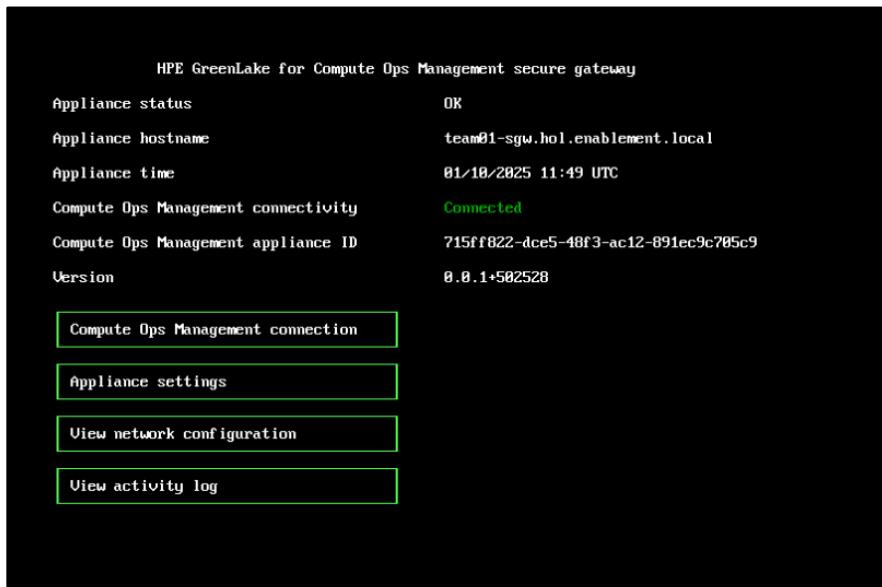
CF36327S2 

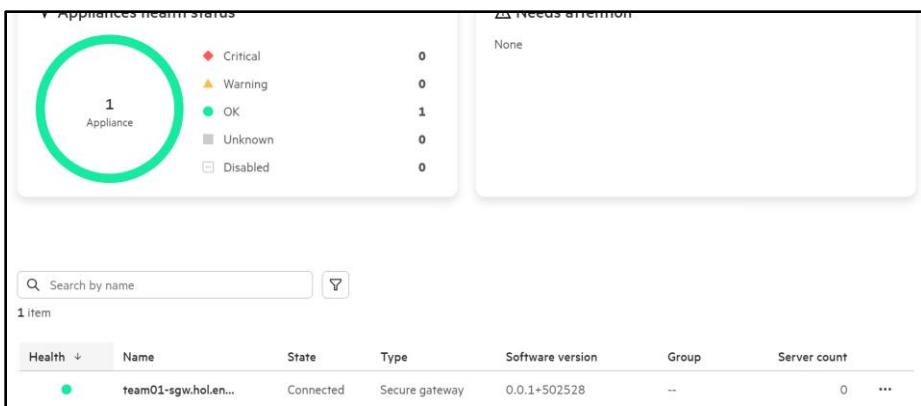
[Close](#)

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**, Firmware & OS Software, iLO Federation, Remote Console & Media, Power & Thermal, iLO Dedicated Network Port, and iLO Shared Network Port. The 'Compute Ops Management' item is highlighted with a teal bar at the bottom of the sidebar. The main content area is titled 'Compute Ops Management'. It displays the 'Connection Status' as 'Connected' with a green checkmark icon. Below it, the 'HPE GreenLake Workspace ID' is listed as '0ec9d316321111ef85ad52587cbe5bc3'. Under 'Connection Type', it says 'Direct'. At the bottom right of the main content area, there is a link labeled 'HPE GreenLake'. At the very bottom of the page, there is a navigation bar with icons for Home, Support, Documentation, and Contact.

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

The screenshot shows a 'Connection' settings dialog box. At the top, there is a toggle switch labeled 'HPE GreenLake for Compute Ops Management' which is currently turned off (gray). A red arrow points to this switch. Below the switch, there is a descriptive text block: 'HPE GreenLake for Compute Ops Management allows you to seamlessly monitor, manage, and gain real-time visibility of your distributed compute environment.' followed by a bulleted list of benefits. At the bottom of the dialog box, there is a checkbox labeled 'Yes, disable the connection to HPE GreenLake for Compute Ops Management.' with a checked green checkmark. A red arrow points to this checkbox. To the right of the checkbox is a green 'Save' button, which also has a red arrow pointing to it.

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

Server		Network	
Server Name	HPE-HOL52	Anonymous Data	Enabled
Server FQDN / IP Address	[Not set]	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]

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

5. 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**.

Web Proxy

Web Proxy Server
team01-sgw.hol.enablement.local

Web Proxy Port
8080

Web Proxy Username

Web Proxy Password

6. 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.

	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	ProLiz

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

Servers

Add server

_servers_health_status iLO_security_status

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.

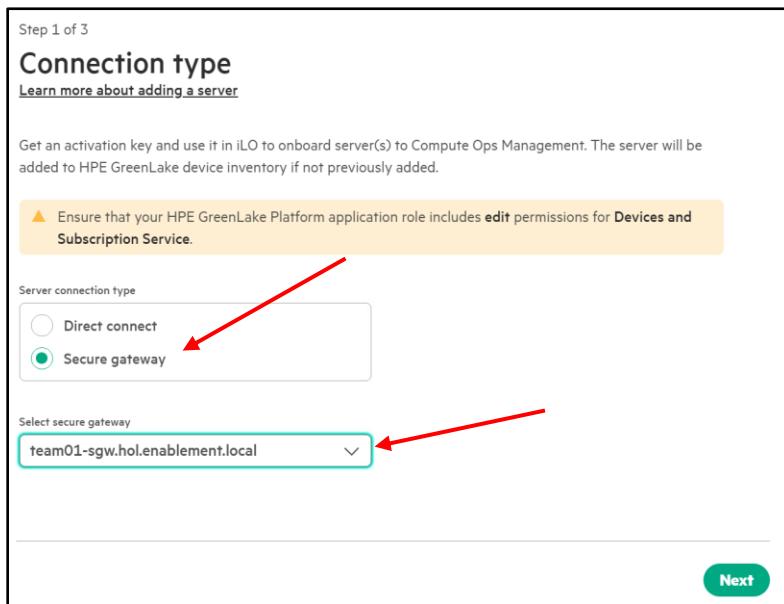
Server connection type

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

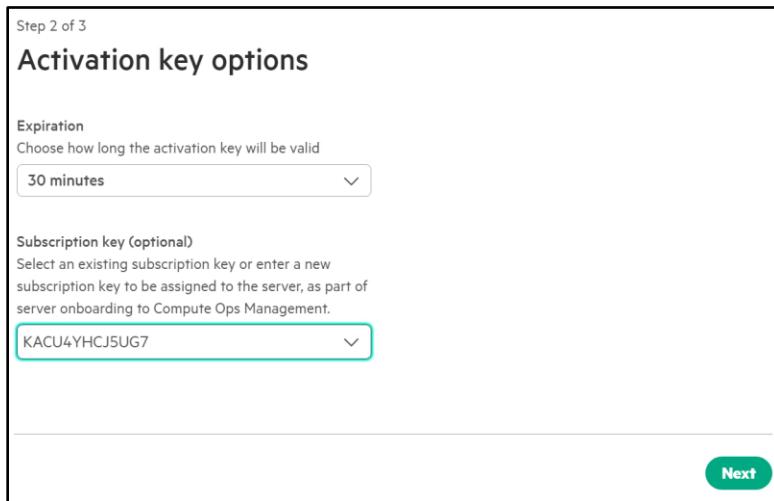
30 minutes

Subscription key (optional)

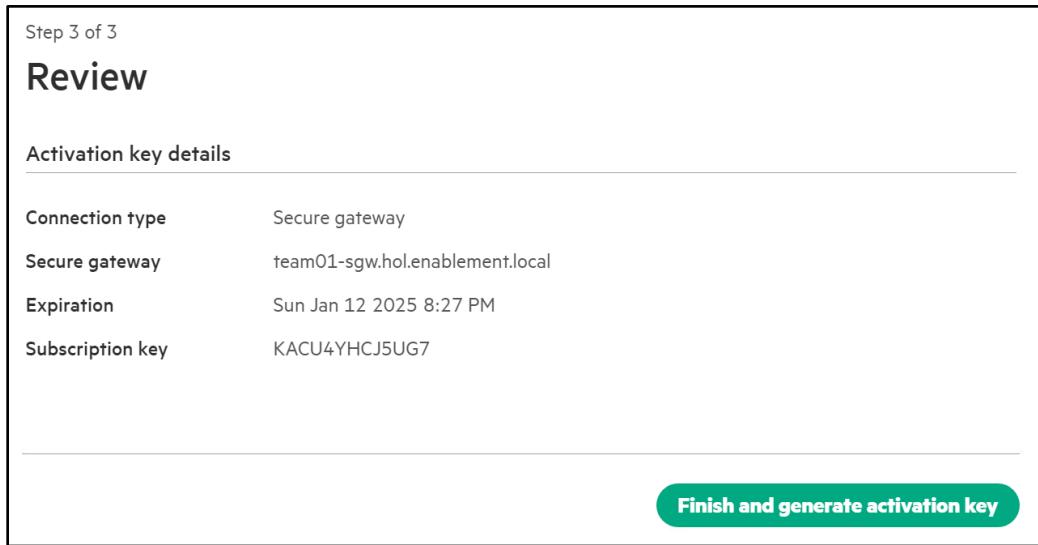
Select an existing subscription key or enter a new subscription key to be assigned to the server, as part of server onboarding to Compute Ops Management.

KACU4YHCJ5UG7

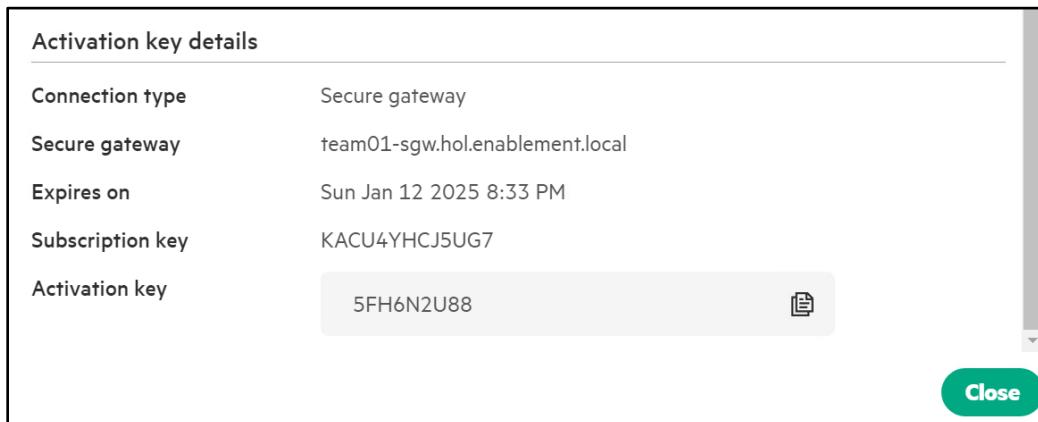
Next



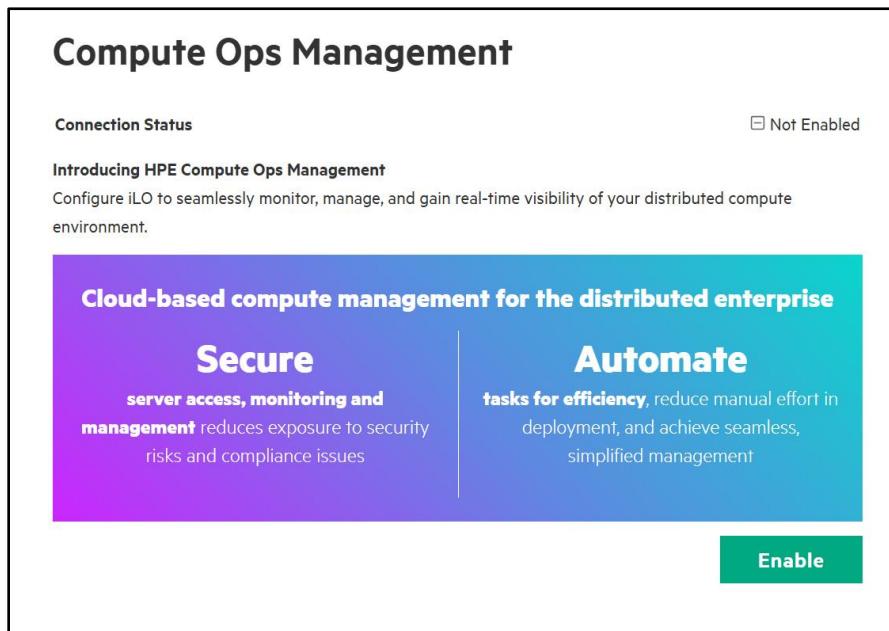
10. Review your Activation Key Details, then hit **Finish and generate activation key**.



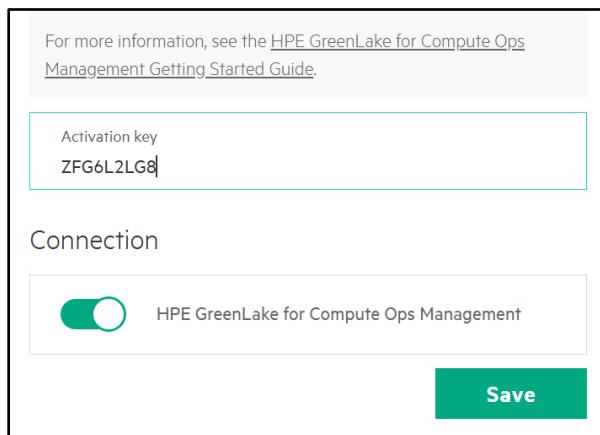
11. Take note of or **copy the Activation key**, then close the pop up.



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

Connection Status	Connected
HPE GreenLake Workspace ID	0ec9d316321111ef85ad52587cbe5bc3
Connection Type	Gateway
<u>Edit Settings</u>	<u>HPE GreenLake</u>

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 its inventory process.

Retrieving server driver and software inventory in progress

<input type="checkbox"/>	HPE-HOL52	CN70461J1W	At risk	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.

Summary Health Firmware Hardware Storage

Details

State	Connected	
Group	--	
Connection type	Secure gateway	
Appliance	<u>team01-sgw.hol.enablement.local</u>	Connected
Model	ProLiant DL325 Gen10 Plus	
Serial number	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 a Secure Gateway. 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	<u>1 server</u>

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: #Discover2024



LEARN MORE AT

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

