Hewlett Packard Enterprise

HPE ProLiant Security Experience

Hands-On Lab

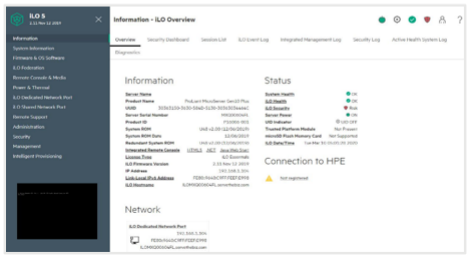
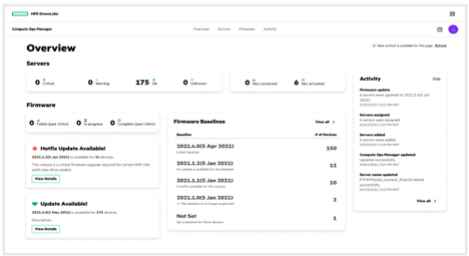
HPE ProLiant Servers differentiated by a security first focus

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	HPE OneView	HPE Compute Ops Management
Embedded	On-premises	SaaS
Embedded Server Management that enables you to securely configure, monitor and update your HPE server	Infrastructure management software that provides composable solutions across compute, storage, and networking.	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.

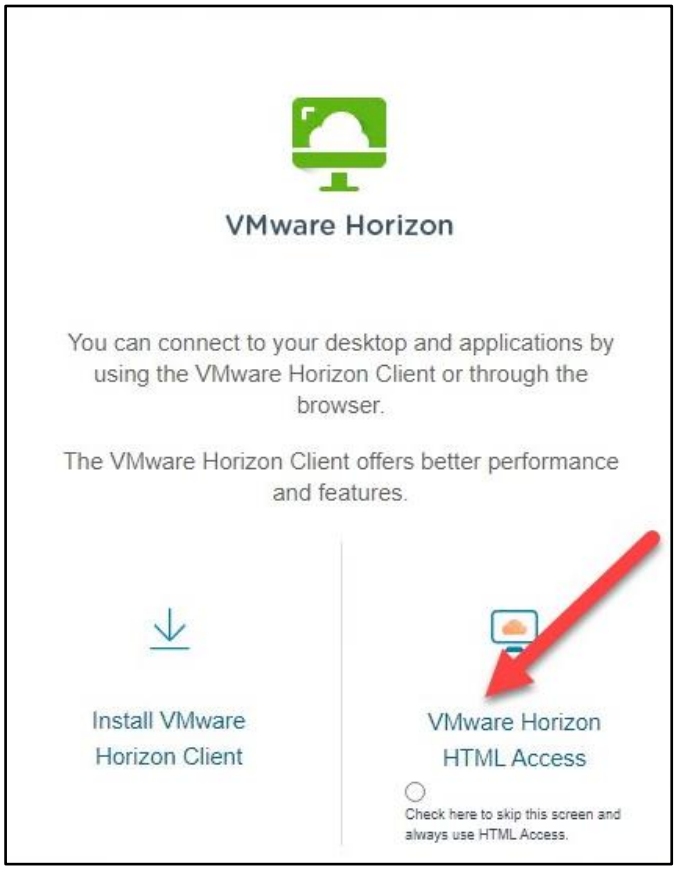
Connecting to the lab environment

Logging into Compute BU enablement environment.

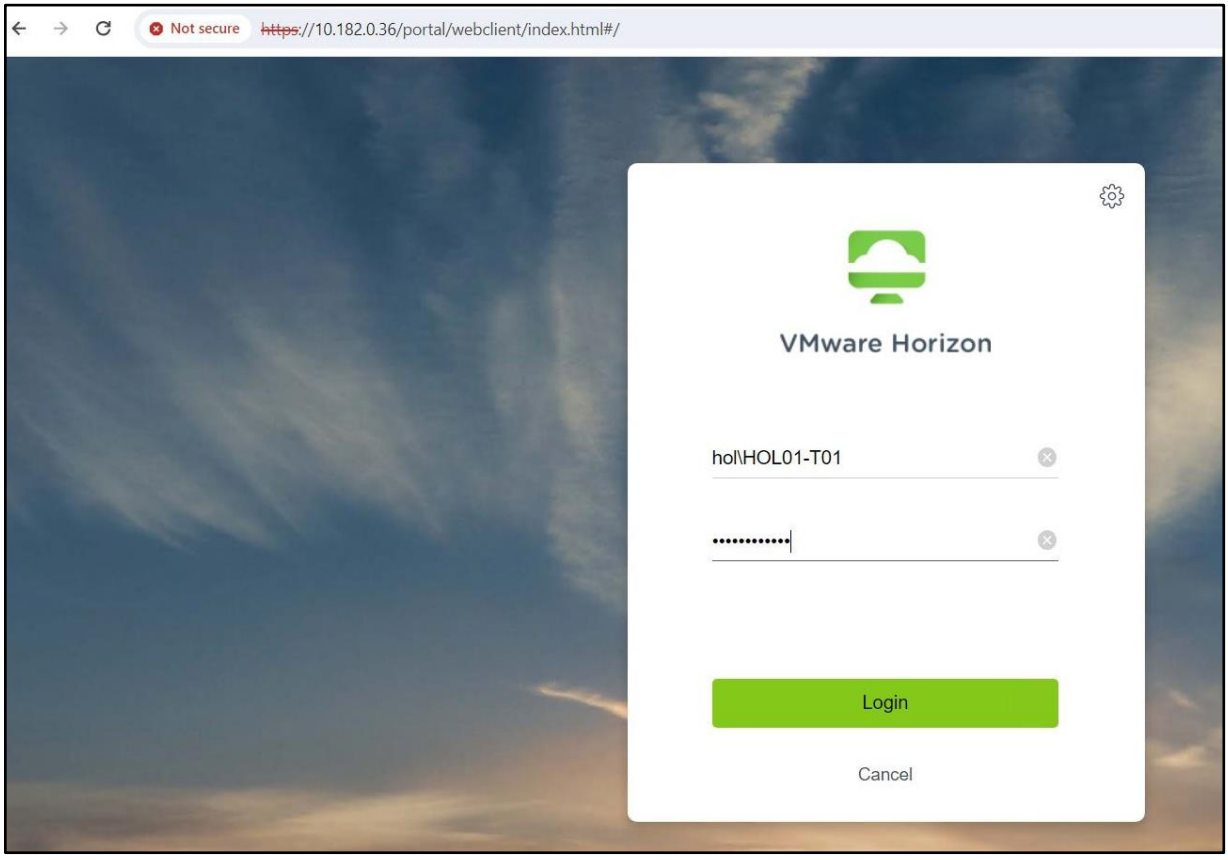
We will be using VMware Horizon to connect to our lab environment. To get to your Compute resources and view the server details page, follow the steps below.

1. Using your Chrome browser, go to our Horizon based Compute Enablement access at: **https://16.103.2.129/**

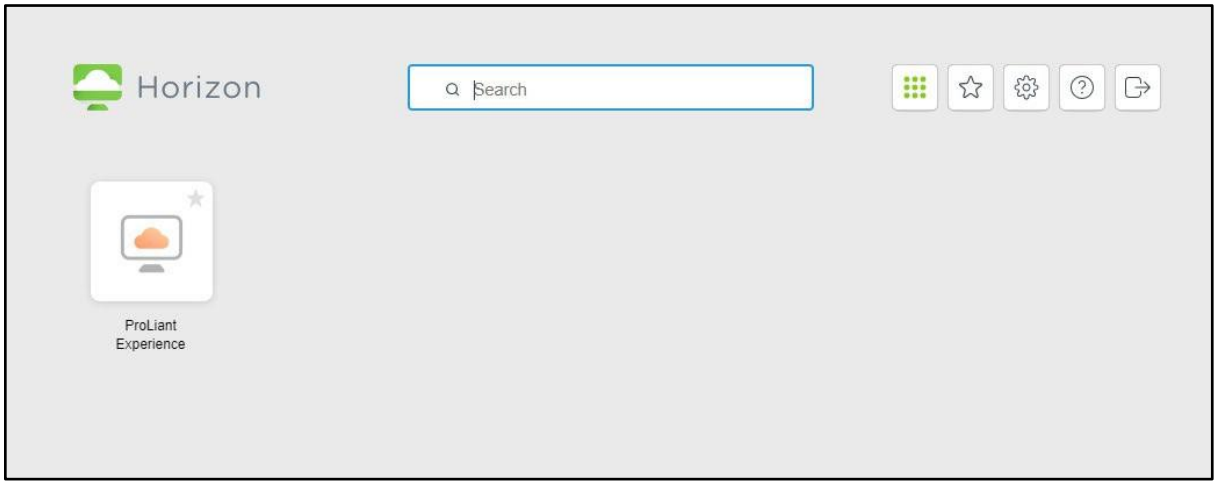
2. At the VMware Horizon login screen, **click on the VMware Horizon HTML Access button**.



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.



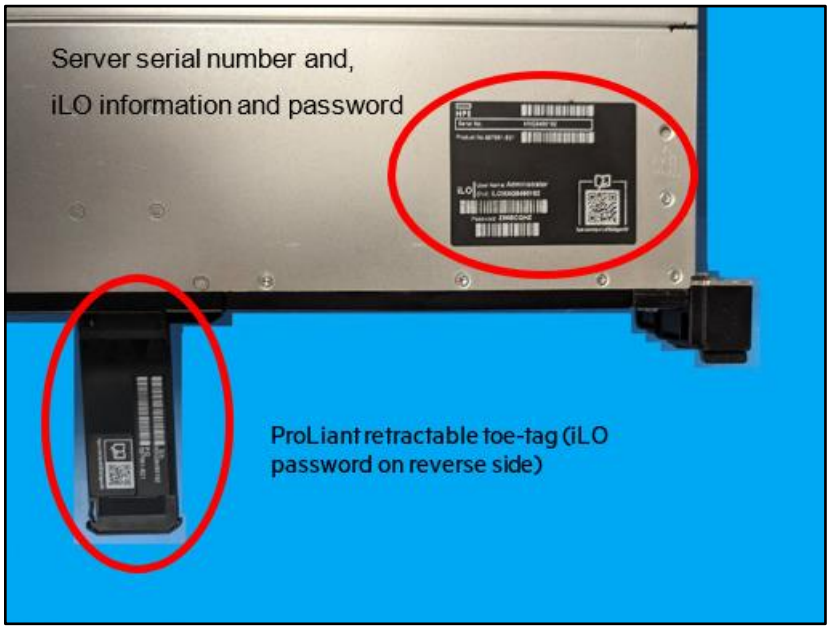
You are now in a VPN-enabled Chrome browser session. For these labs to work, you will need to stay within the context of this browser session. You have a secure connection to our remote lab in Houston, but it doesn't work like a traditional VPN session. Only what you launch from this browser session,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



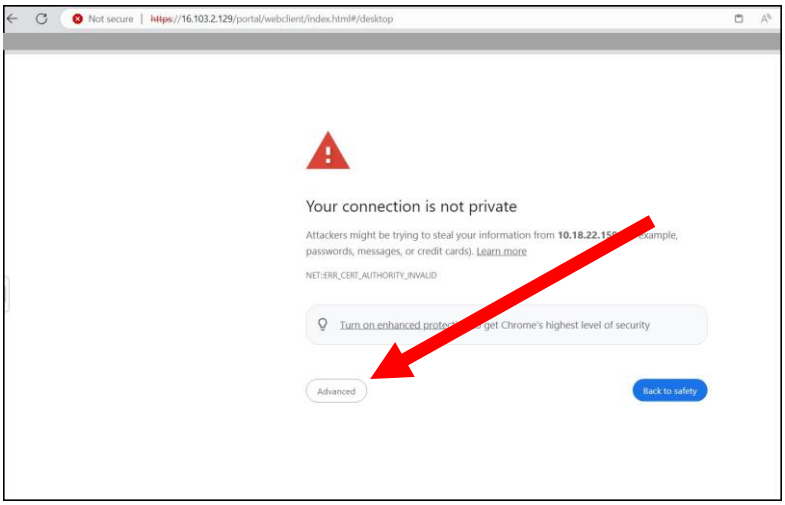
In this lab environment, a DHCP server is issuing IP addresses to known hosts using DHCP reservations. This ensures the lab unit you will access obtains the same IP address each time it boots after the lab is reset. Consult the table below for your team's name and number, and default Administrator credentials.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

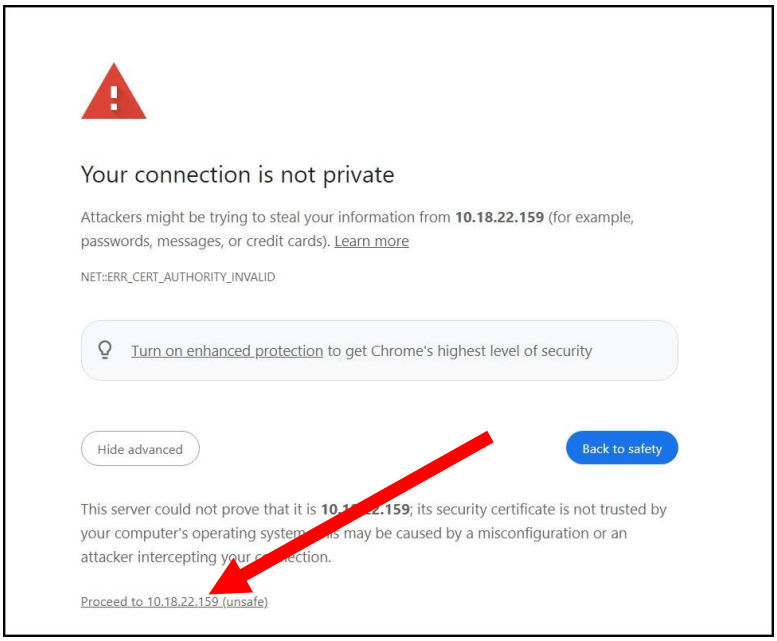
1. Use your Horizon enabled Chrome browser session that you connected with in the previous section. Remember that for these labs to work, you will need to stay within the context of this browser session.

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**.

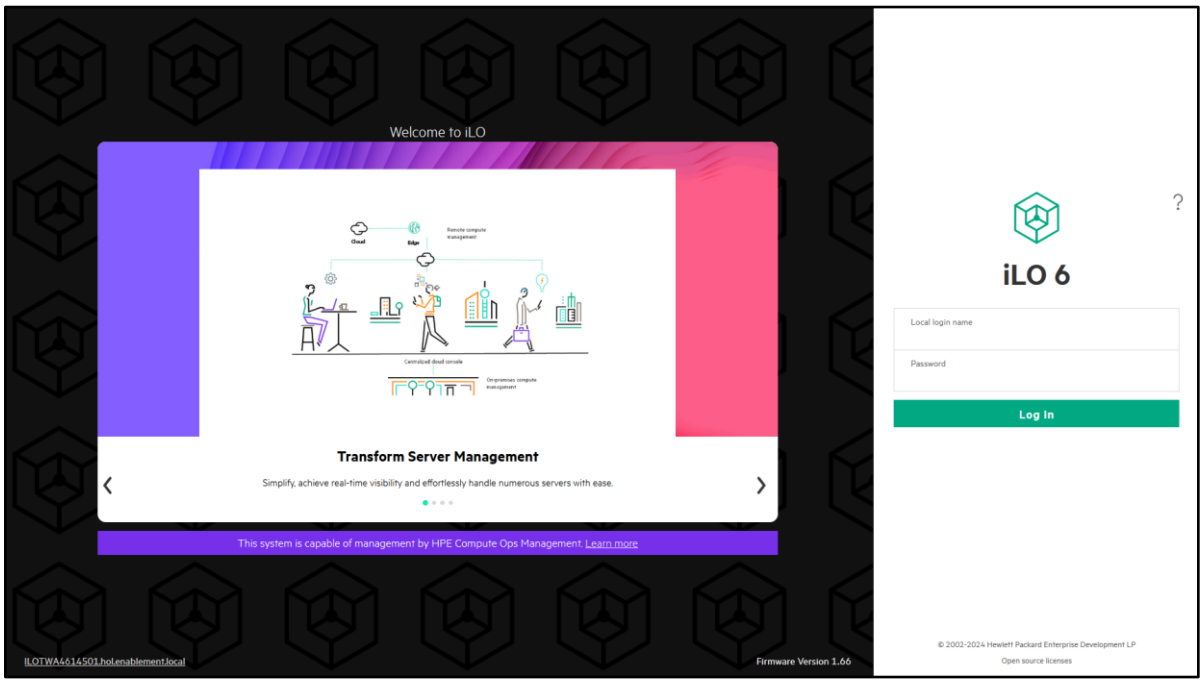


4. On the newly displayed prompt, **click on the Proceed to 10.18.22.xx** to continue to the iLO login screen.

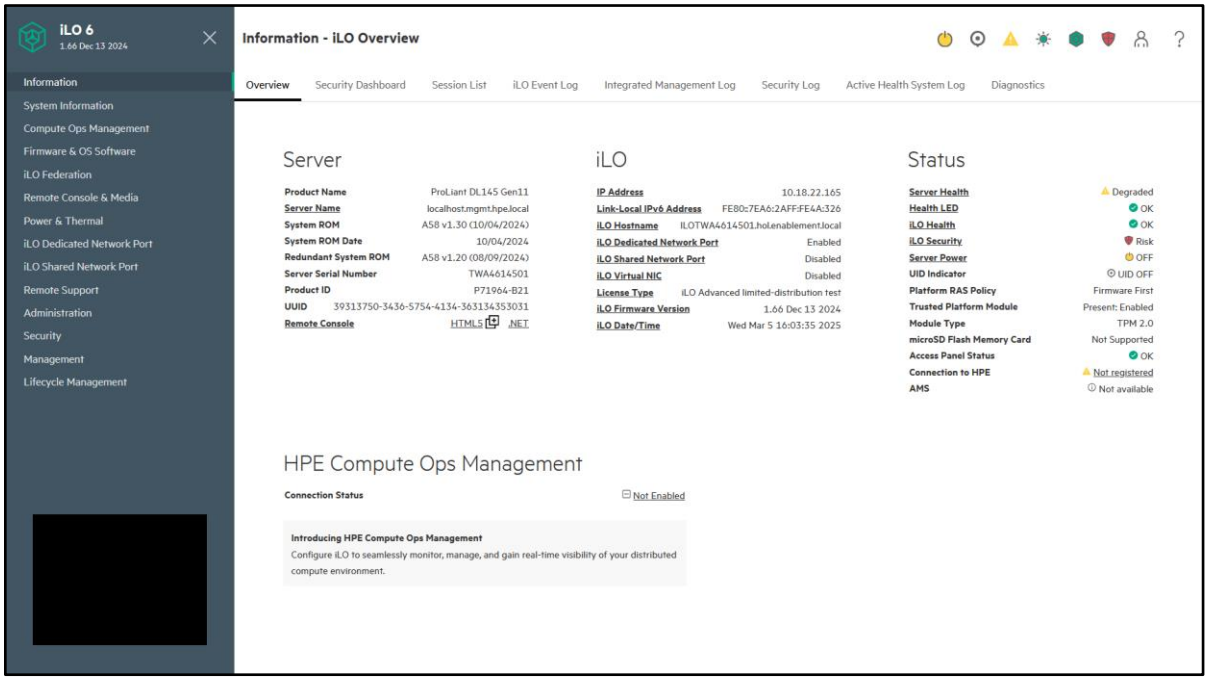


5. Now enter **Administrator** and the **password from the table above**, into the Local login name and Password fields.

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.

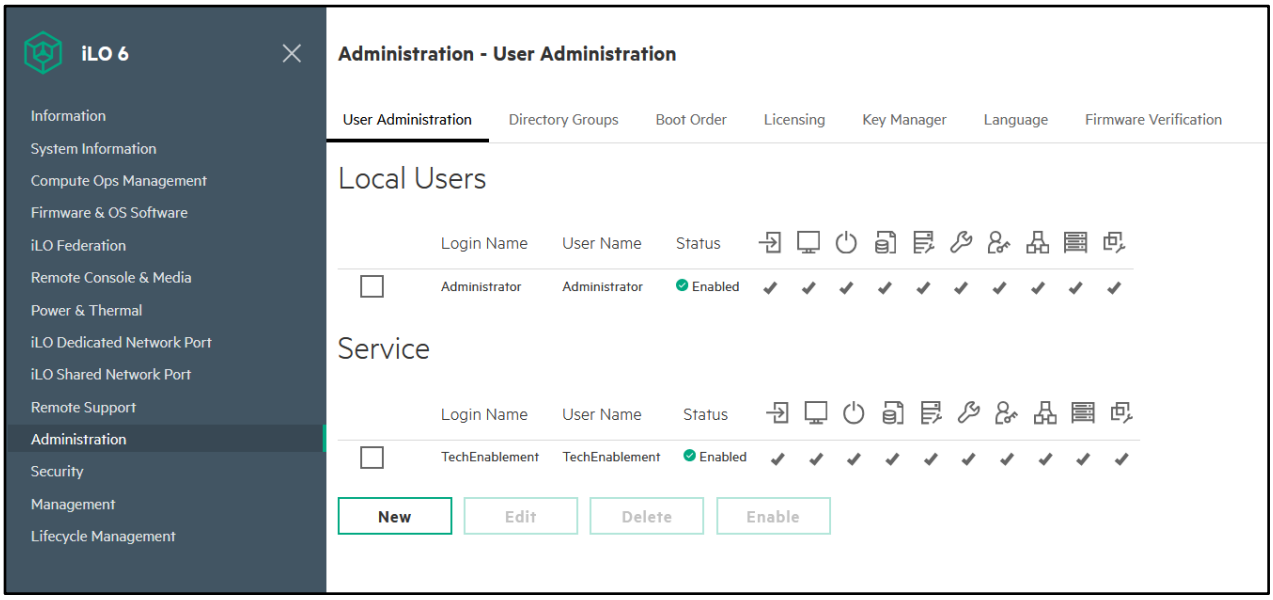


This concludes this portion of the lab.

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.

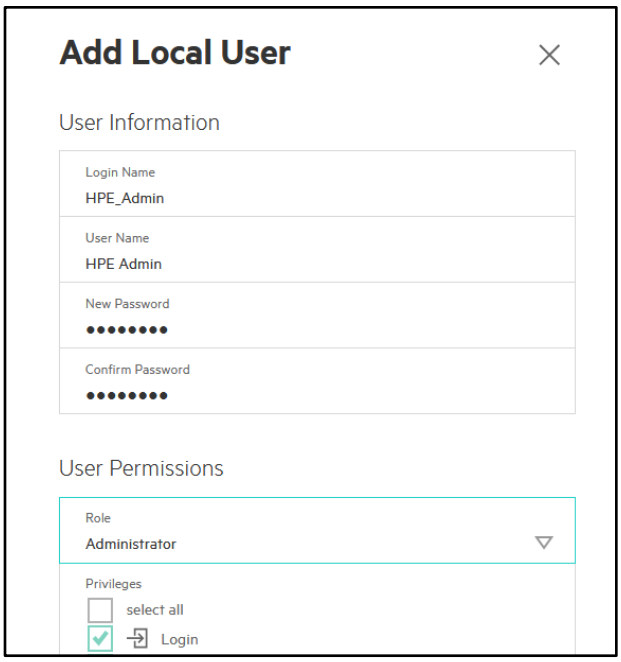
1. In the left-hand navigation pane of your iLO, click **Administration**.



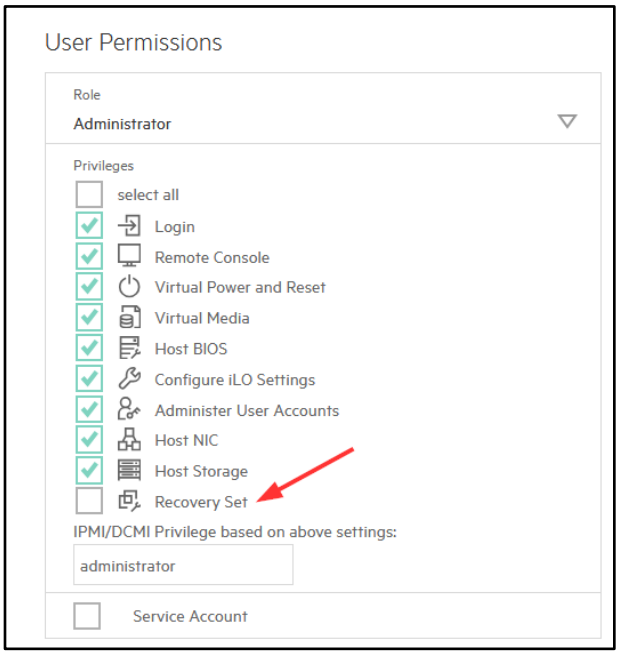
2. For the purposes of this lab, we will **leave the Administrator account with the default toe-tag password** and set up another administrative user account to access the iLO.

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

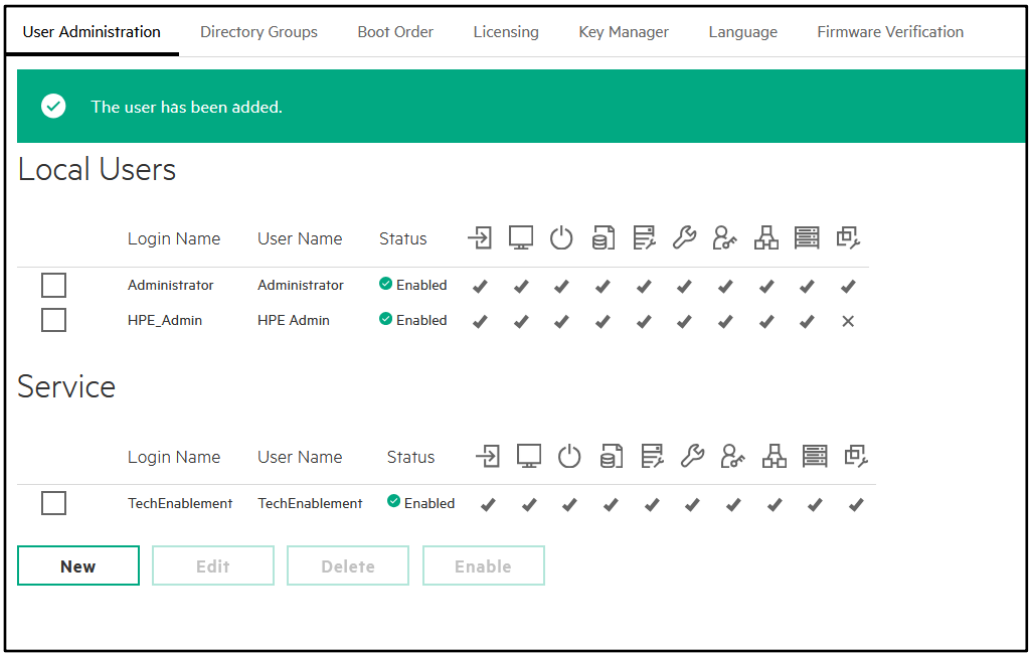


Optionally you can select Custom for the Role, which allows this user to be assigned the privilege to create iLO hosted firmware recovery sets. **Do not select** this choice for this lab.



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

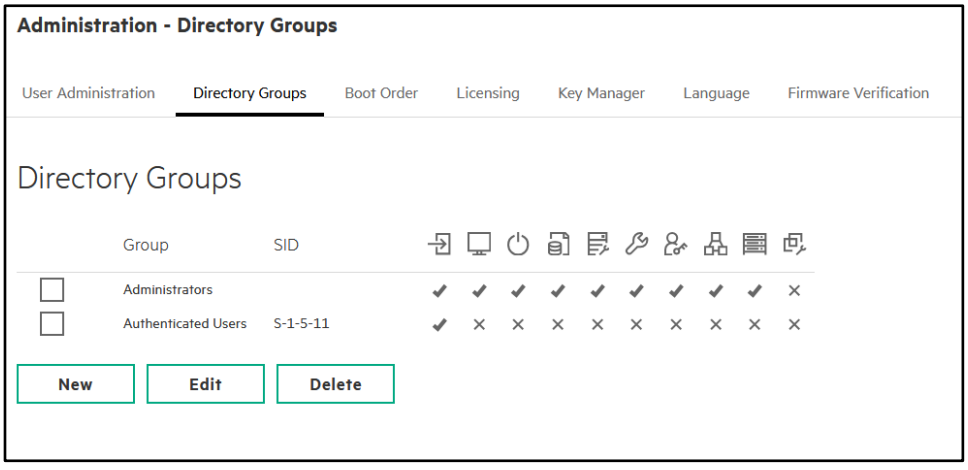
5. You should now see that the new user has been added to the User Administration list.



6. Logout and then log back in with your newly created user.

7. Take Note – You have just created a fully privileged Administrator account with a very simple password. We will circle back on this in a later part of the Lab.

8. Return to the Administration section in iLO and Click on the Directory Groups tab.



The 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/hpesc/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.

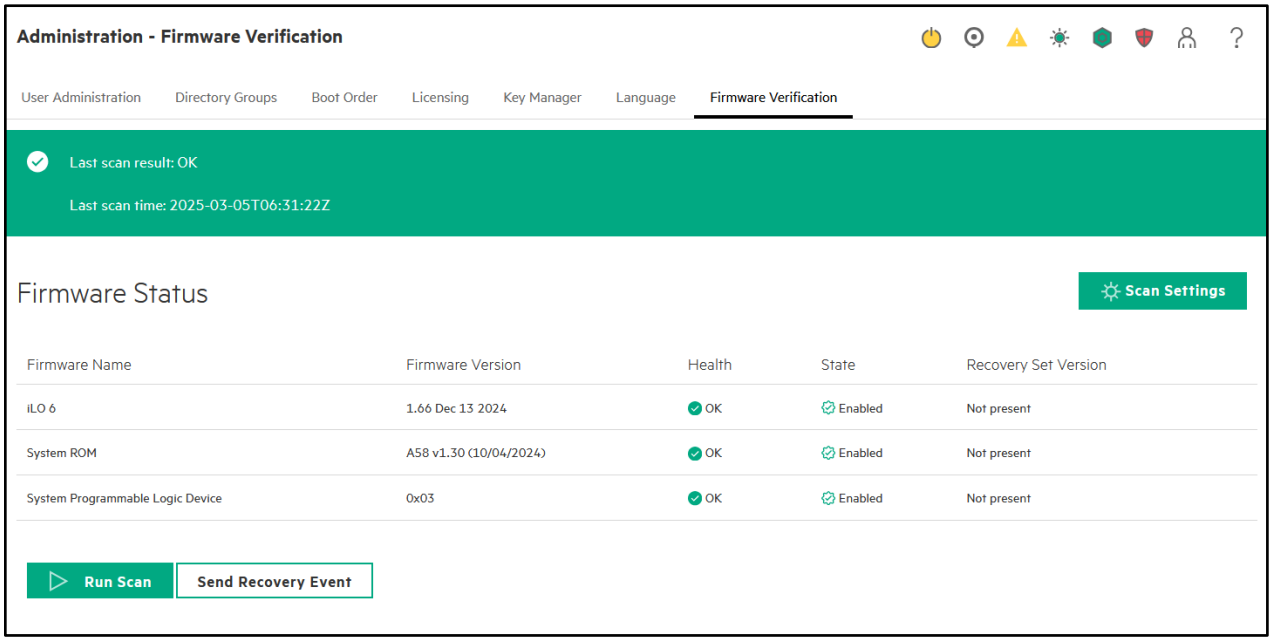
Depending on the scan results, information is logged in the Active Health System Log and the Integrated Management Log. The following firmware types are supported:

- 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)

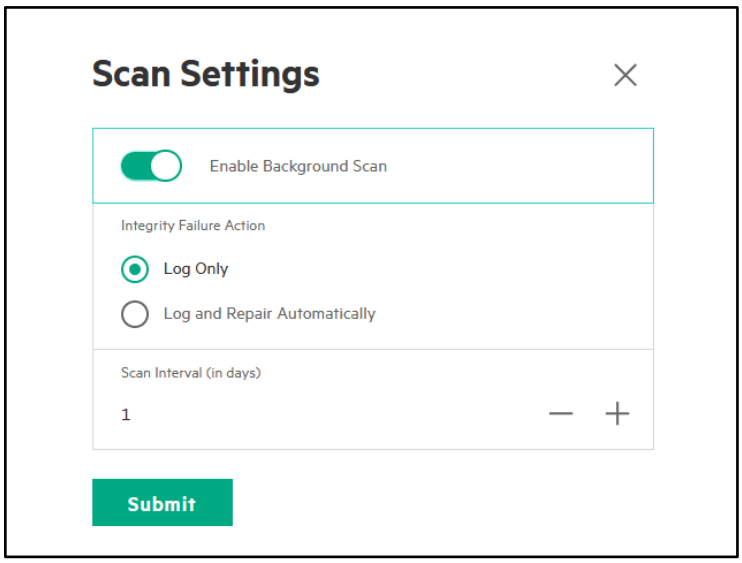
When a firmware verification scan is in progress, you cannot install firmware updates or upload firmware to the iLO Repository. If an invalid iLO or System ROM (BIOS) firmware file is detected, the invalid file is saved to a quarantine area in the iLO Repository. You can download the invalid file to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

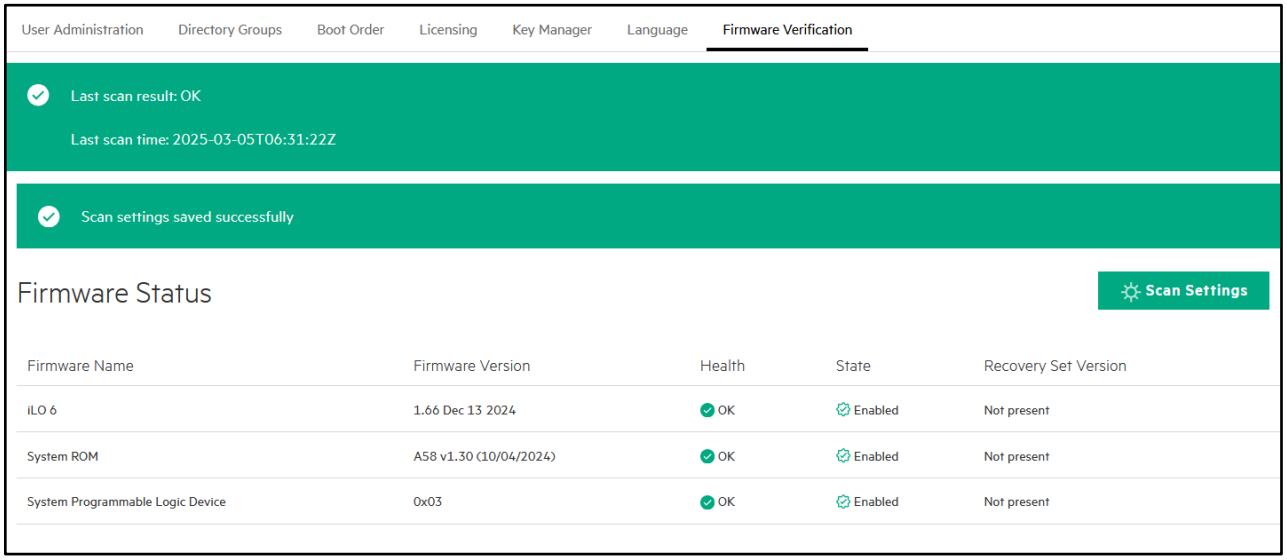
1. Click on the **Firmware Verification** tab to explore the iLO capability to manually scan the system firmware to check the validity and health of the firmware components.



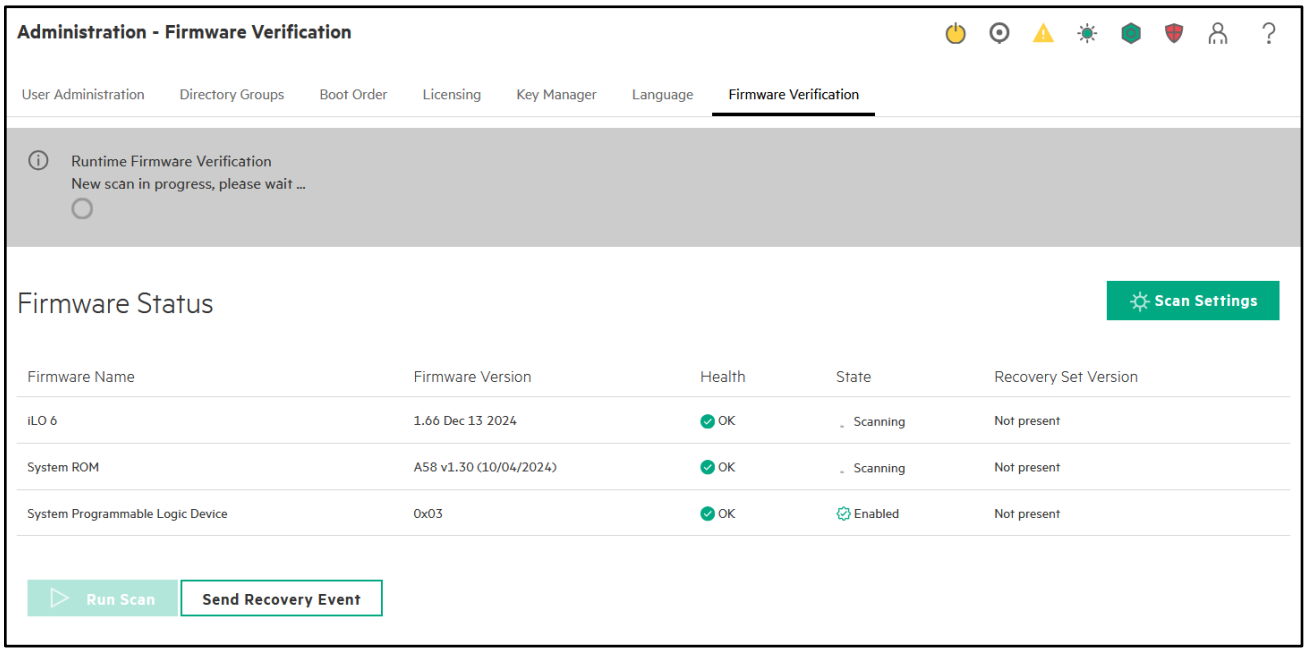
2. Click **Scan Settings** and **Enable Background Scan** with an Integrity Failure Action of **Log Only**. The default setting is 7 days, but for this lab, change the **Scan Interval** to 1.



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



4. 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.



5. Return to the iLO Information screen.

This concludes this portion of the lab.

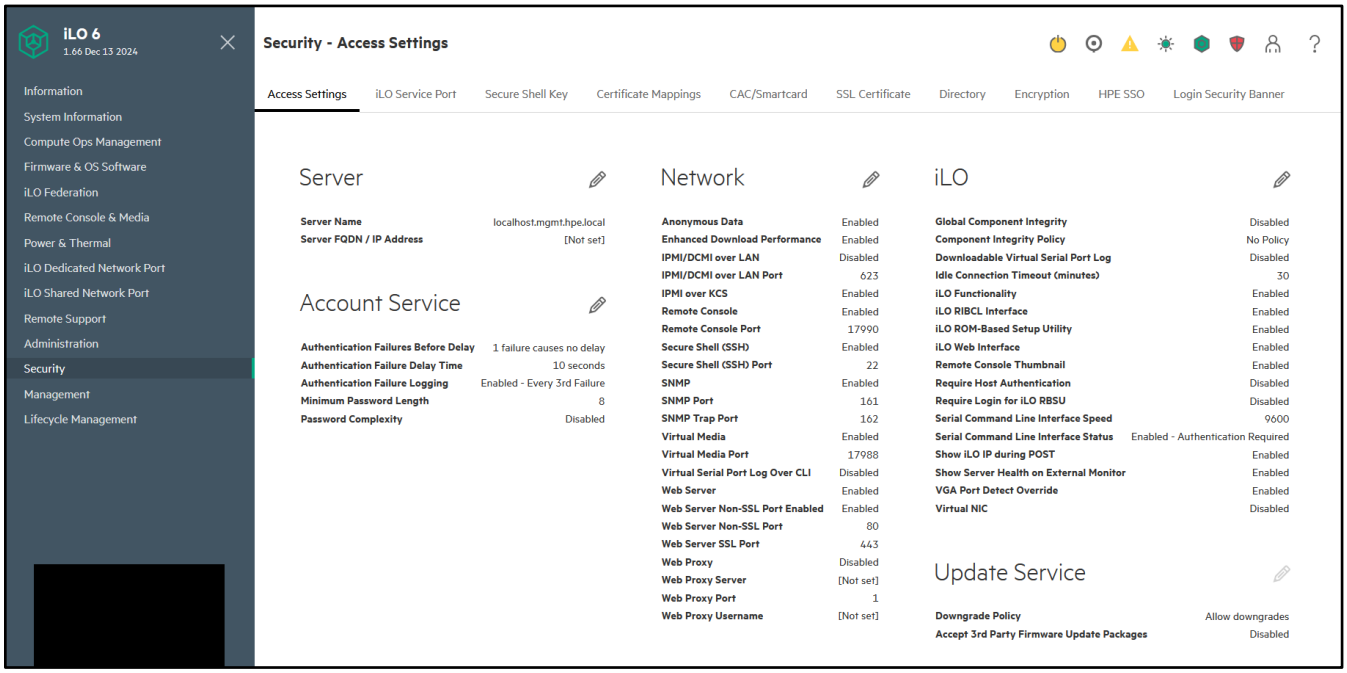
Applying Web Proxy configuration

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.



4. In the middle column, in the **Network** section, click the **edit** (pencil) icon.

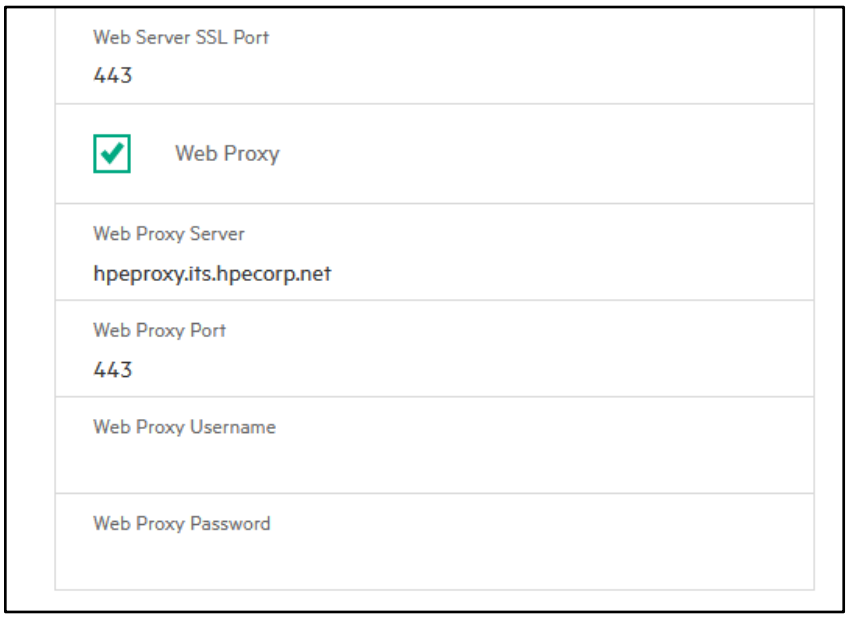
5. Now scroll down to the **Web Proxy** section.

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.



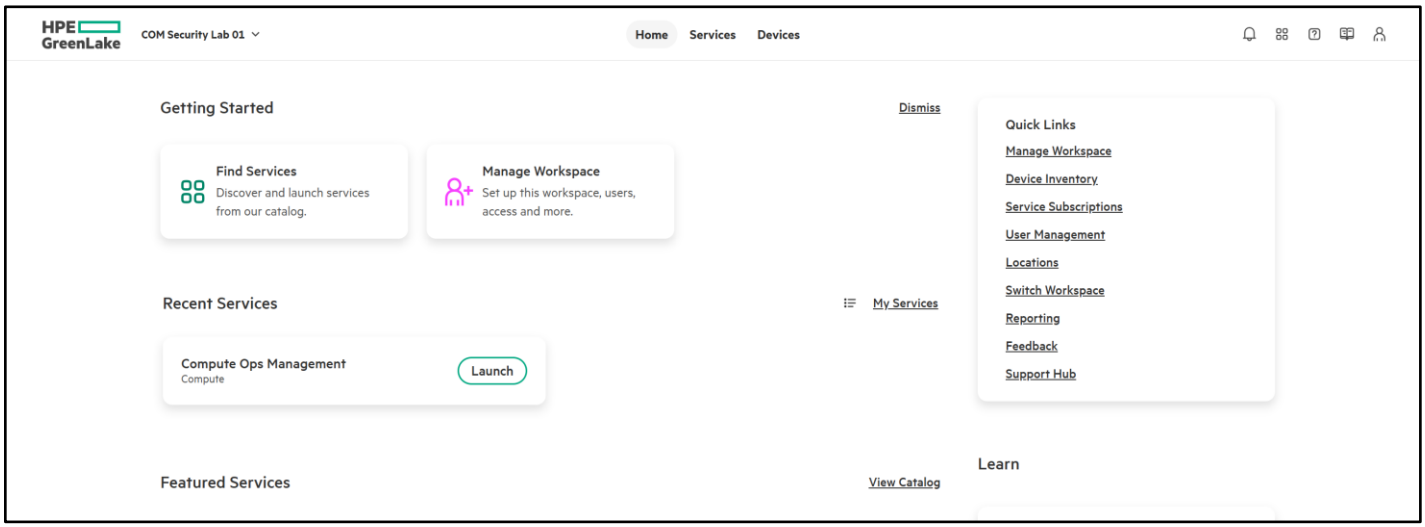
10. Click **OK** to save the changes you entered.

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.



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.

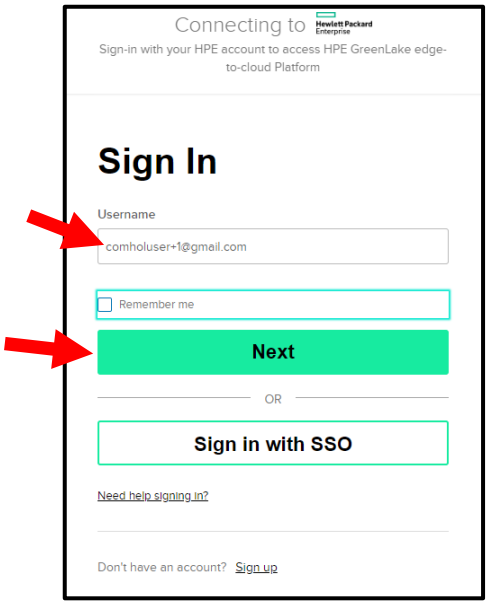
You will need to login to the GreenLake environment. For this portion of the lab, you will use a different username and password from what you used to start the labs. Your assignment is based on your team number and is in the table below.

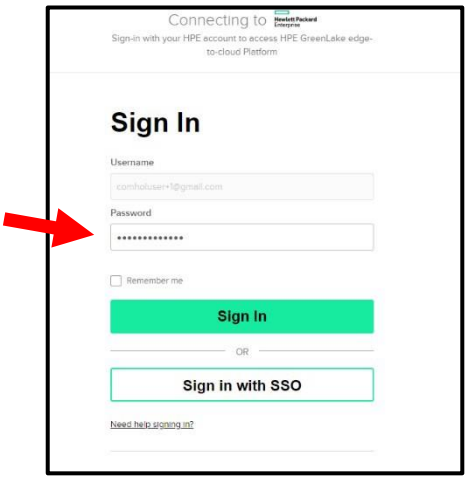
Once you have located your username and password, proceed to Step 1 of this lab.

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!

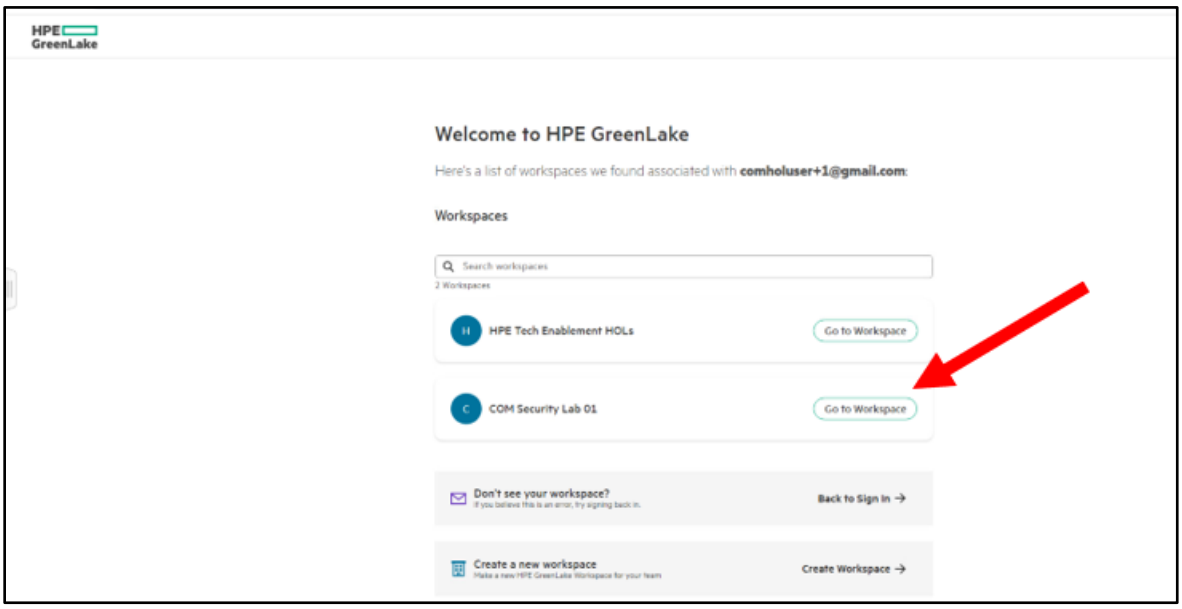




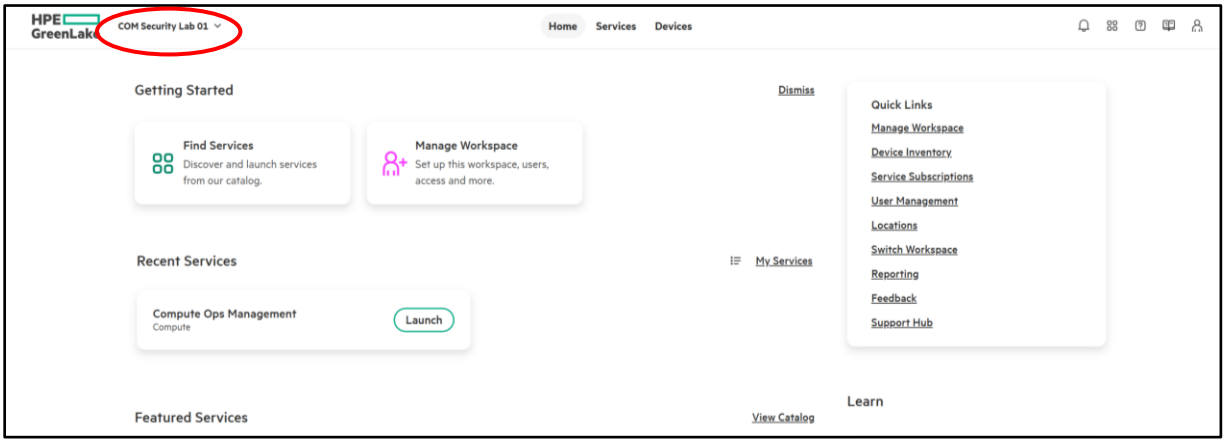
2. Click **Next** to be prompted for a password.

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.

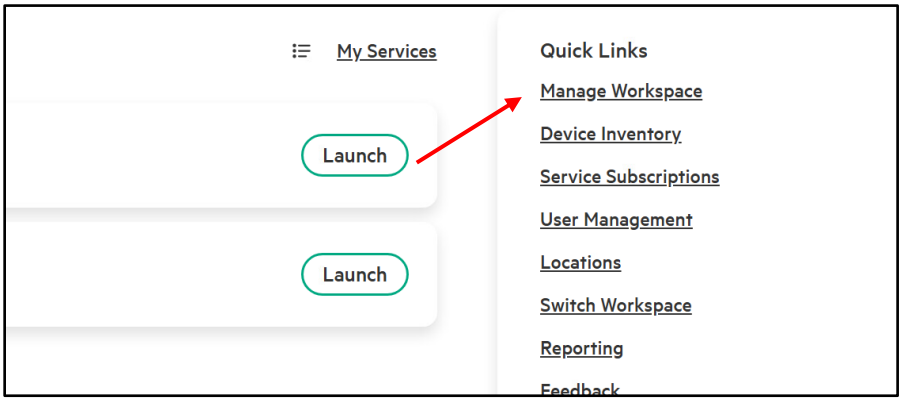
Secure Login Options for Enterprise IT Administrators

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.

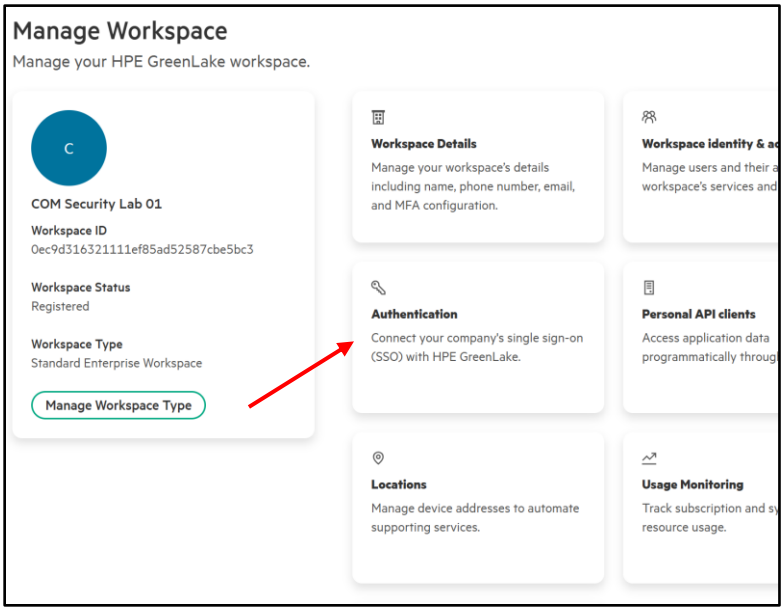
Our HPE GreenLake Cloud Platform supports Multi-Factor Authentication as well as SAML SSO which combining both together, can go a long way to ensuring any bad actors do not access your IT Estate, especially through Compute Ops Management.

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.

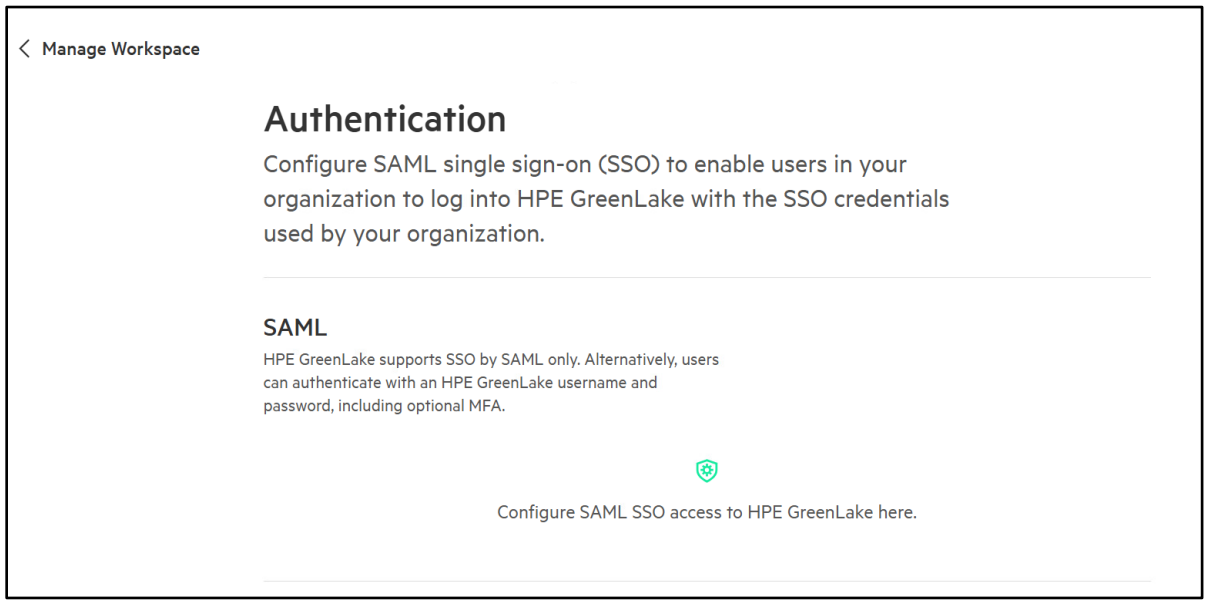
1. From the **Quick Links** on the right-hand side of the Home Page, click **Manage Workspace**.



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

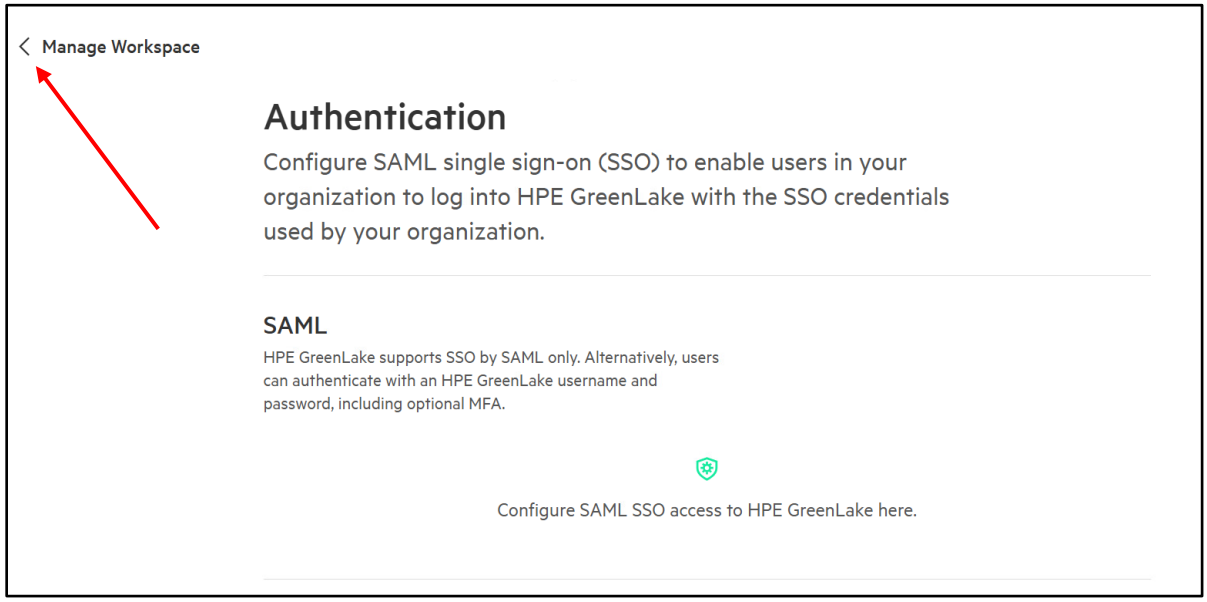


3. It's here that you would then look to configure your SAML SSO access to HPE GreenLake.

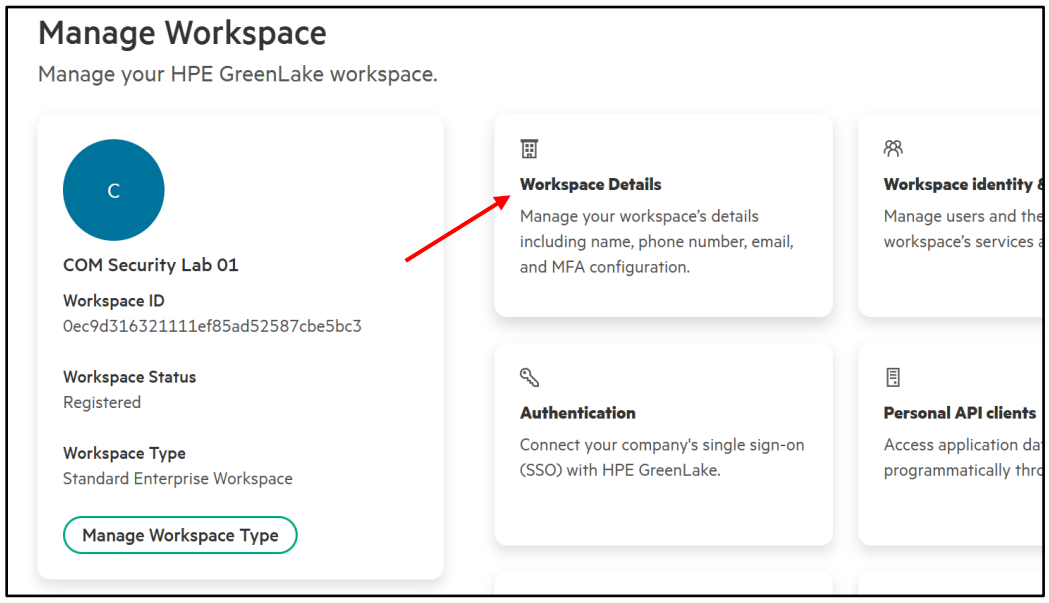


For more information on setting up and configuring SAML SSO authentication with your enterprise, you can consult the blog: Configuring-HPE-GreenLake-SSO-SAML-Authentication-with-ADFS

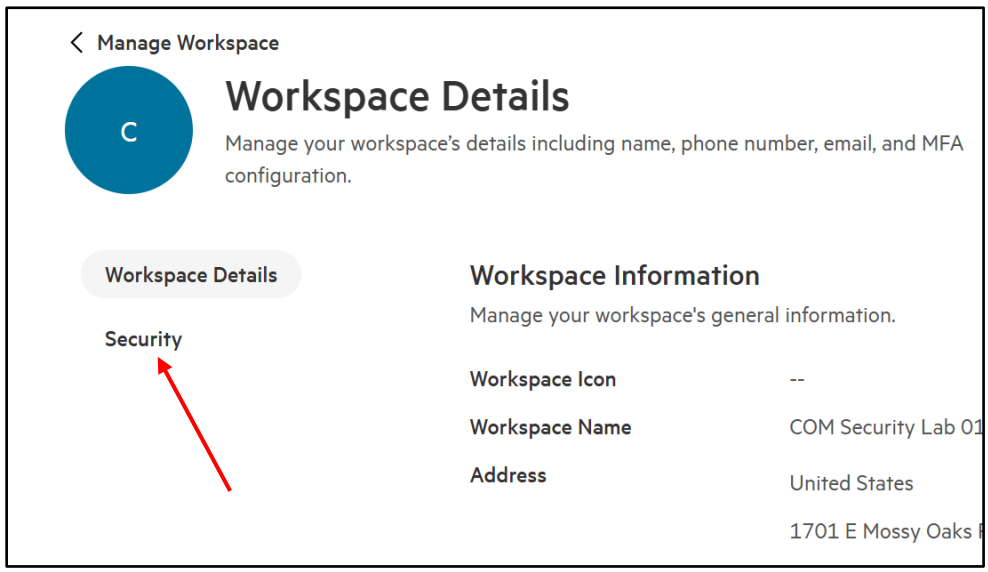
4. Now navigate back to **Manage Workspace** by clicking the left arrow.



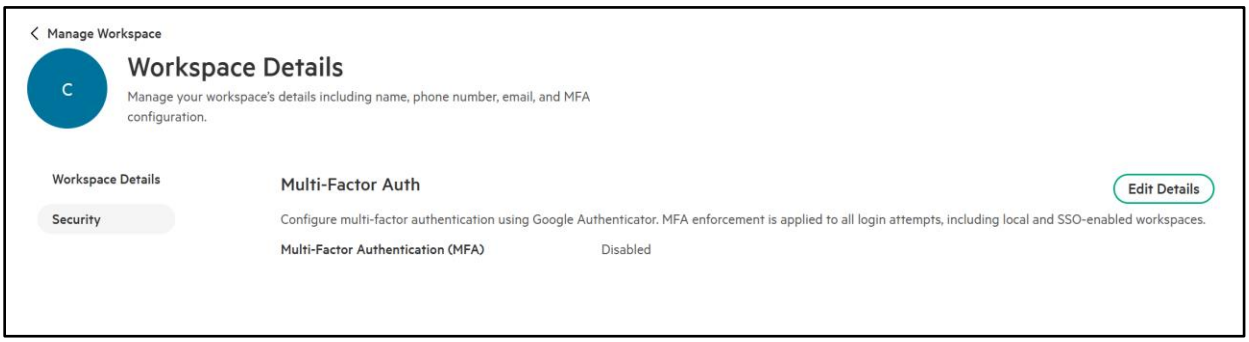
5. Select the **Workspace Details** tile**.**

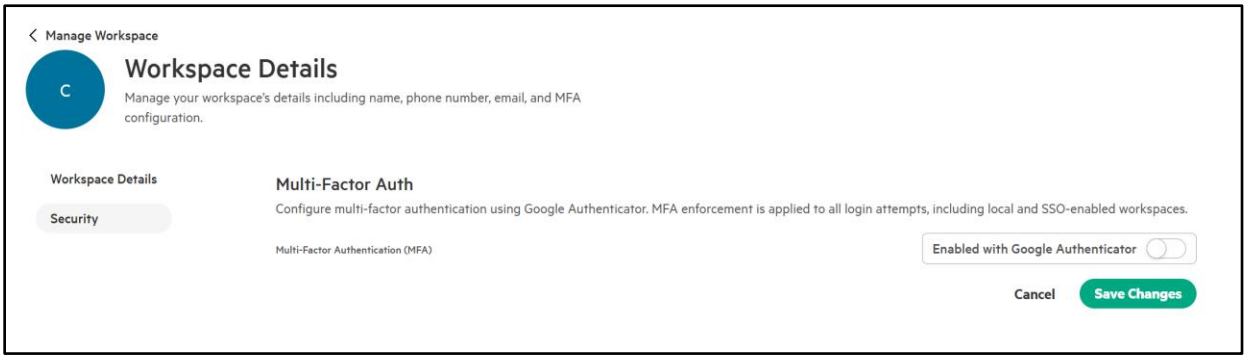


6. Navigate to the **Security** tab.



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.

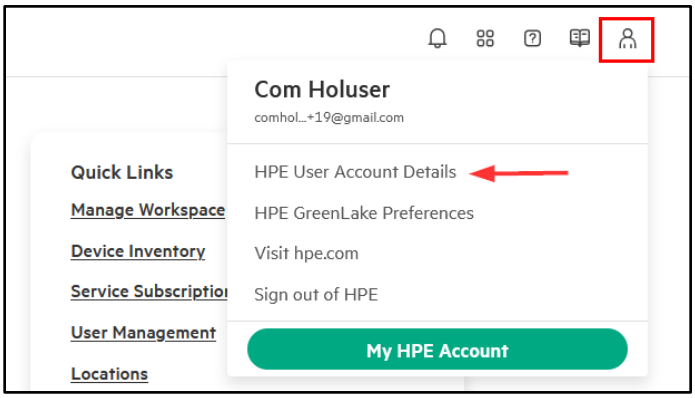




Note: For the purpose of this lab, we will NOT be configuring MFA on these Workspaces.

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.



This concludes this section of the lab.

Establishing a connection from HPE iLO to HPE GreenLake

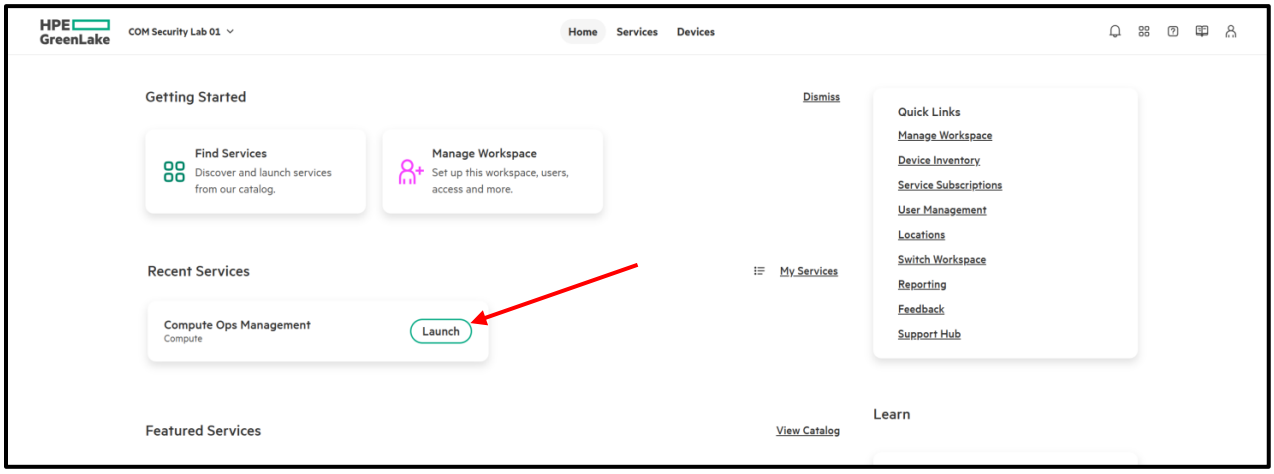
For our lab purposes, the HPE GreenLake Workspace company in this environment is called *COM Security Lab XX*.

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.

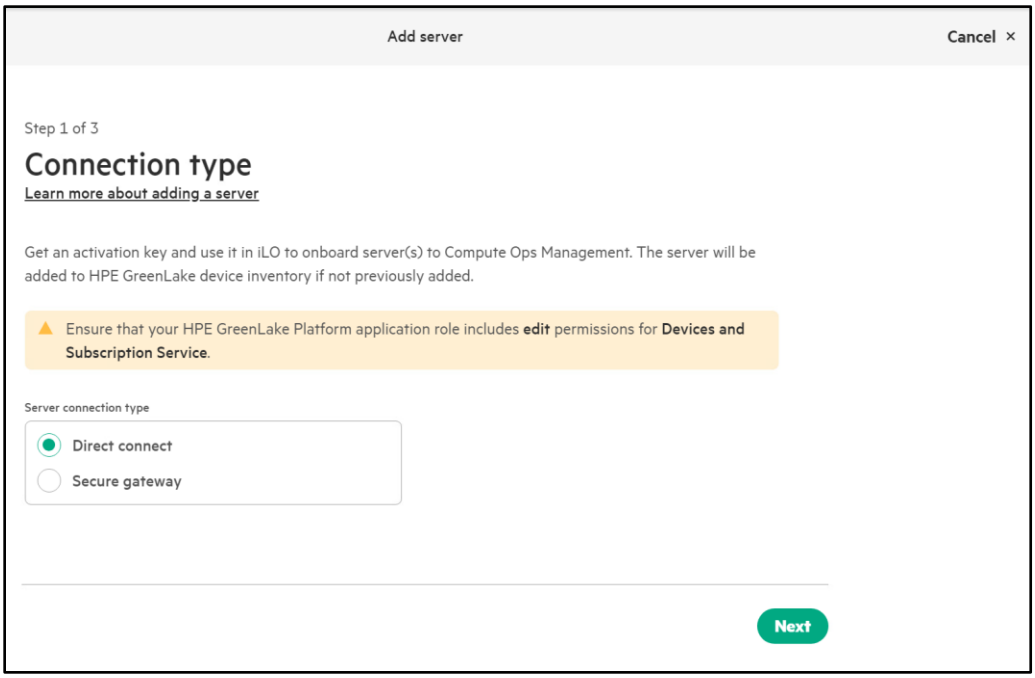
1. From the HPE GreenLake Recent Services section, choose the **Compute Ops Management Launch** button to connect to HPE Compute Ops Management main menu.



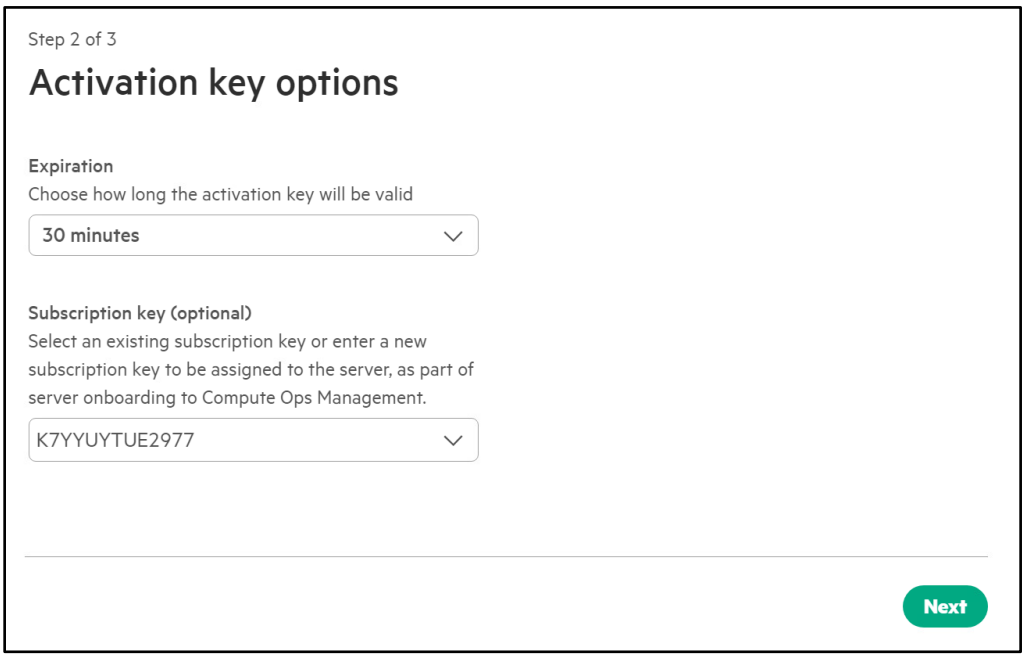
2. Navigate to the **Servers** tab across the top of the page.

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

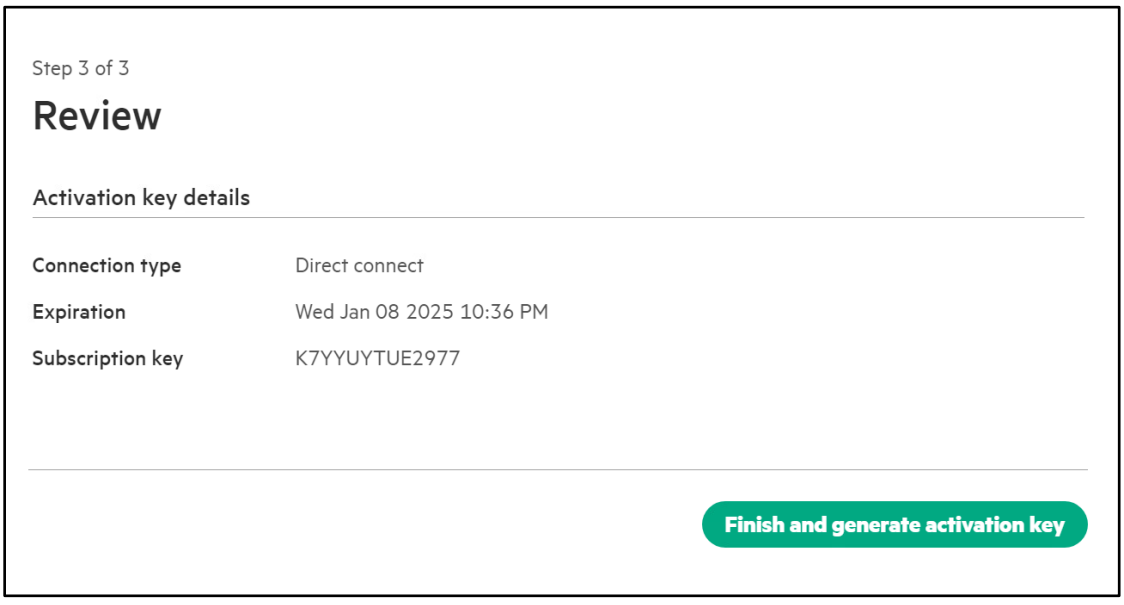
4. At this time, we will select **Direct connect** as our Server Connection type**.** Click **Next**.



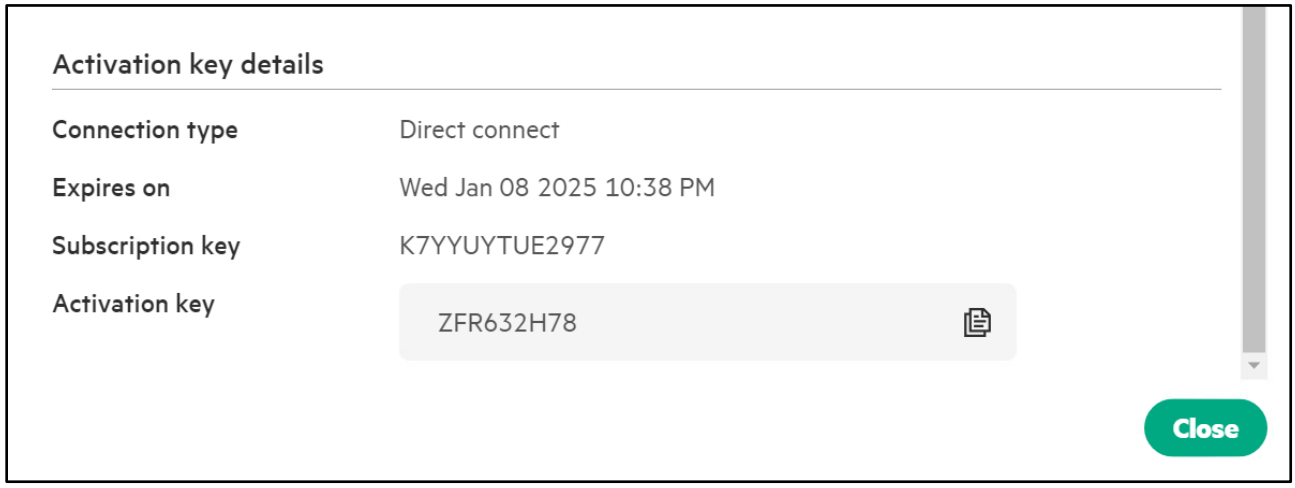
5. Here we can select how long our Activation Key will be valid for and which Subscription Key we will apply. For this lab, let's choose **30 minutes** and **any available subscription key** and click **Next**.



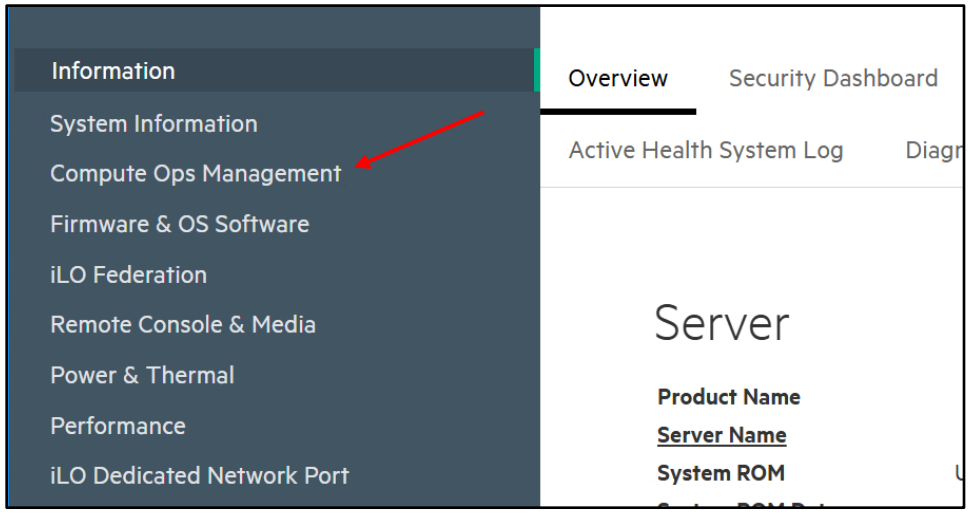
6. Once you have reviewed the details, click **Finish and generate activation key.**



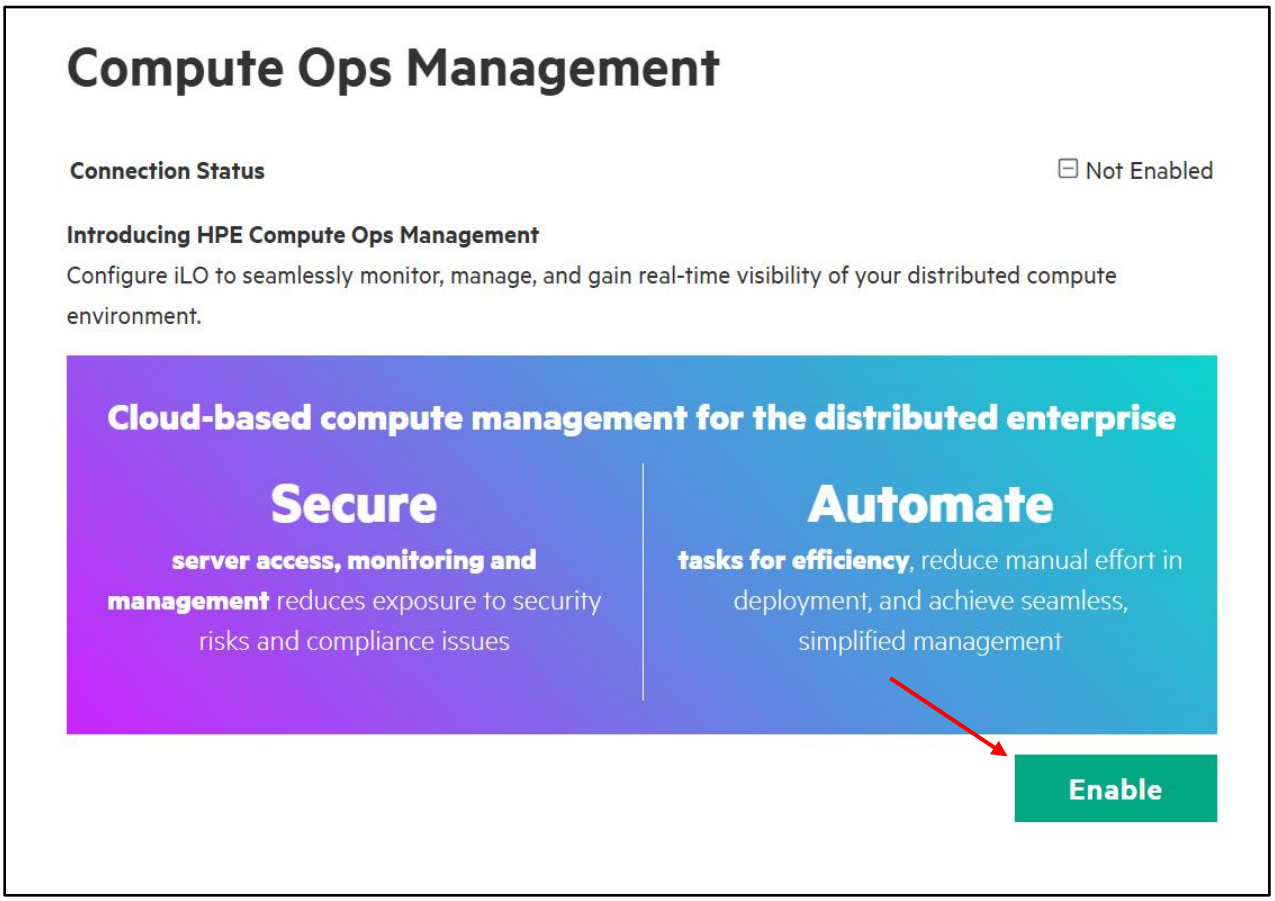
7. We will now take note of our Activation Key, so we can use it in our HPE iLO to connect to Compute Ops Management. Click the **copy icon** and then close this pop up.



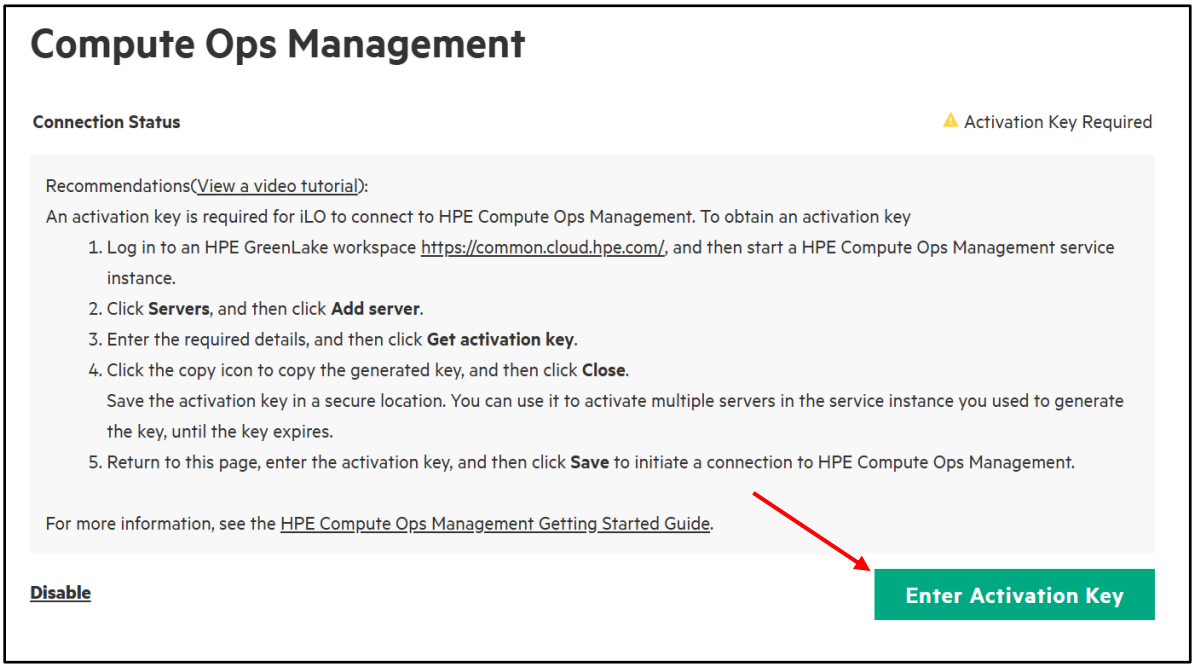
8. Return to the Web Browser Tab, which is connected to your assigned Server's iLO, then navigate to **Compute Ops Management** on the left-hand side of your screen.



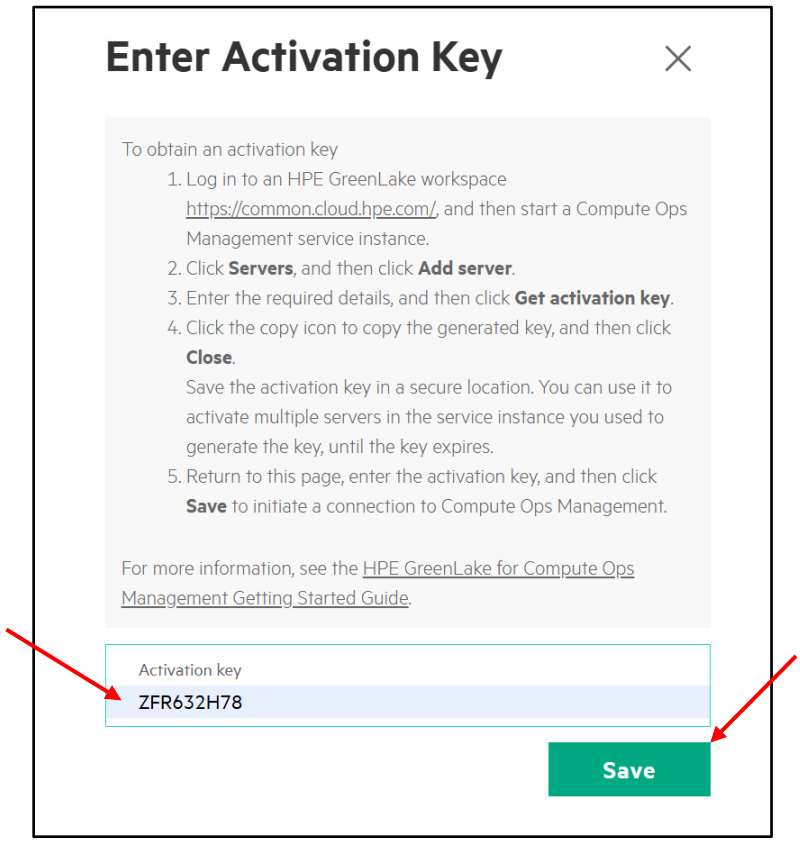
9. Click **Enable** to enable the Compute Ops Management connection.



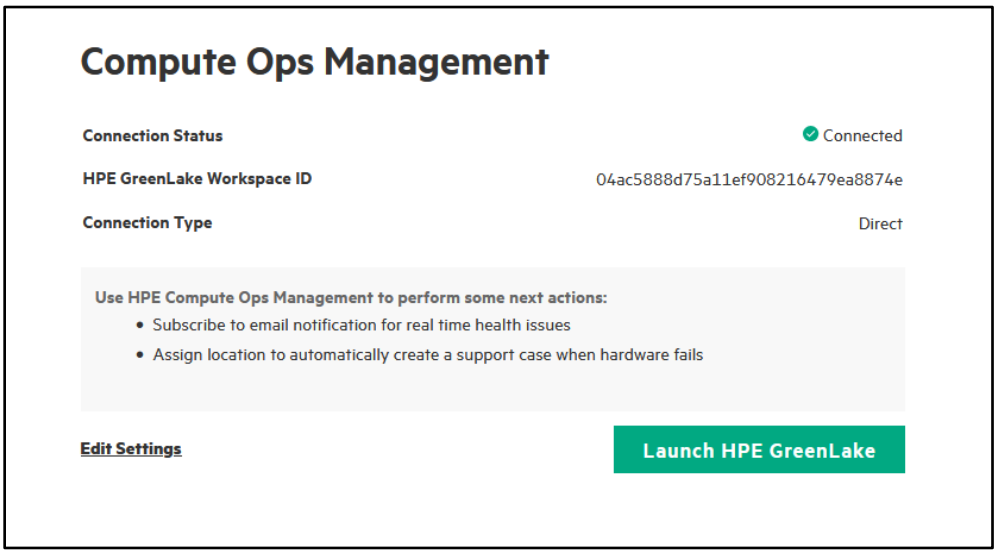
10. Then click on **Enter Activation Key.**



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.**



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

This concludes this section of the lab.

Securing your Server Fleet with HPE Compute Ops Management

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

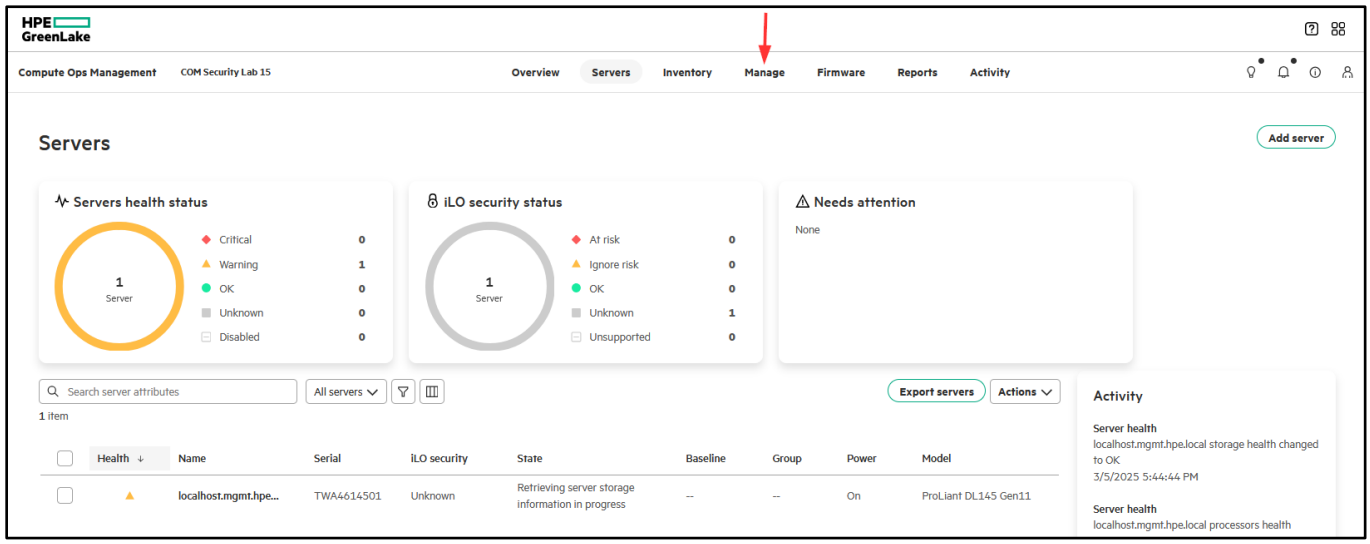
This equips organizations with a unified compute management experience that streamlines compute operations through one cloud-based console providing instant availability to new services and features as they become available.

Configuring Server Groups and Applying Server Settings

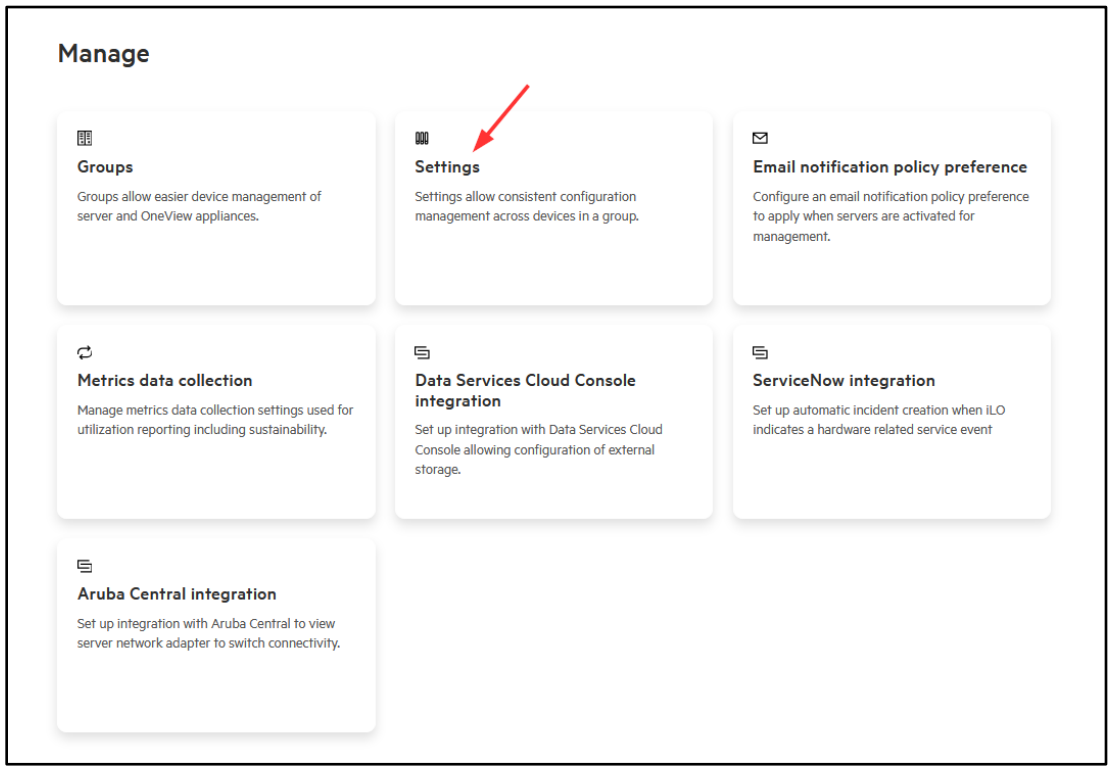
In this portion of the lab, we will focus on the security configuration and lifecycle management aspect of your assigned server. We will create settings for the systems and place those settings into Groups. This ensures consistency across all servers assigned to those groups.

Return to your HOL Horizon Browser session.

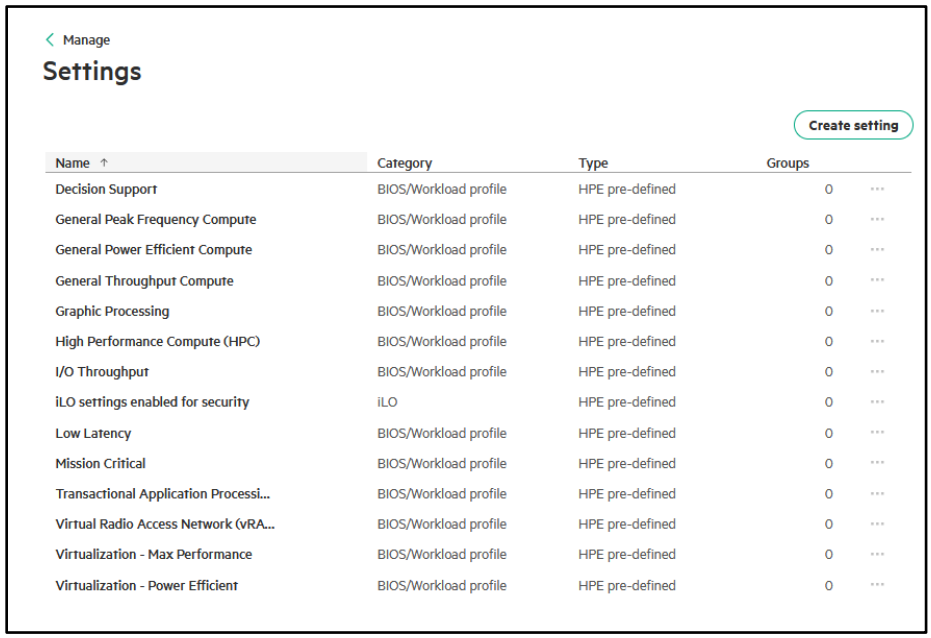
1. From the HPE Compute Ops Management main menu. Select the **Manage** option.



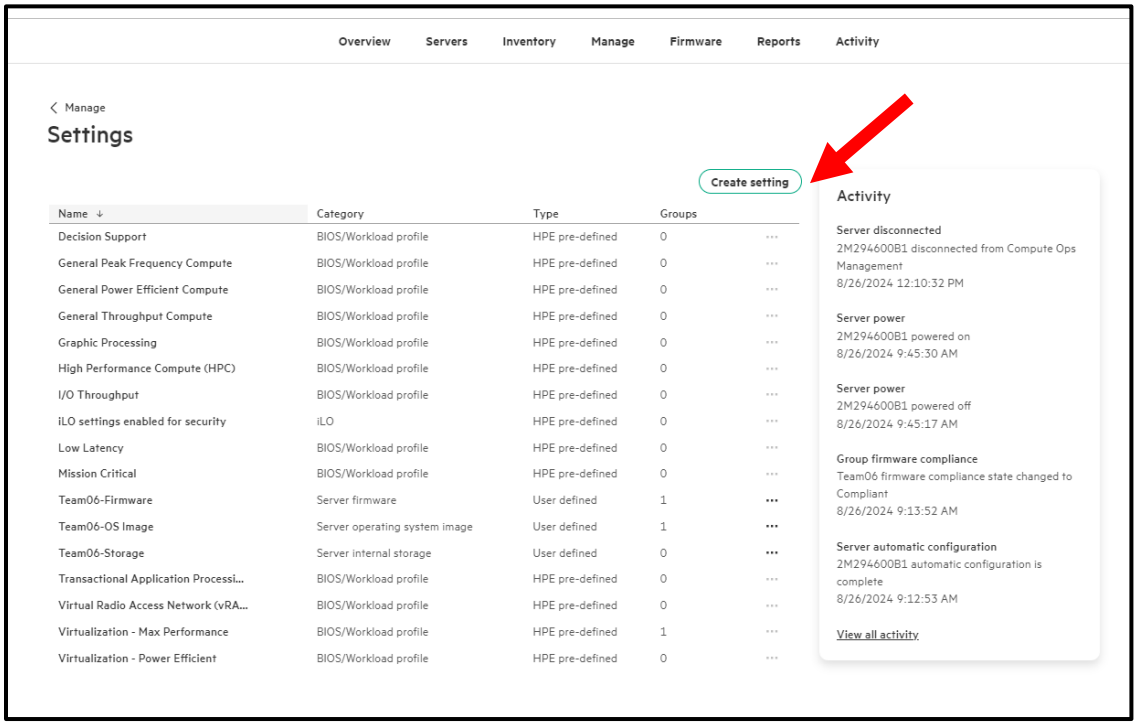
2. Now pick the tile for **Settings**.



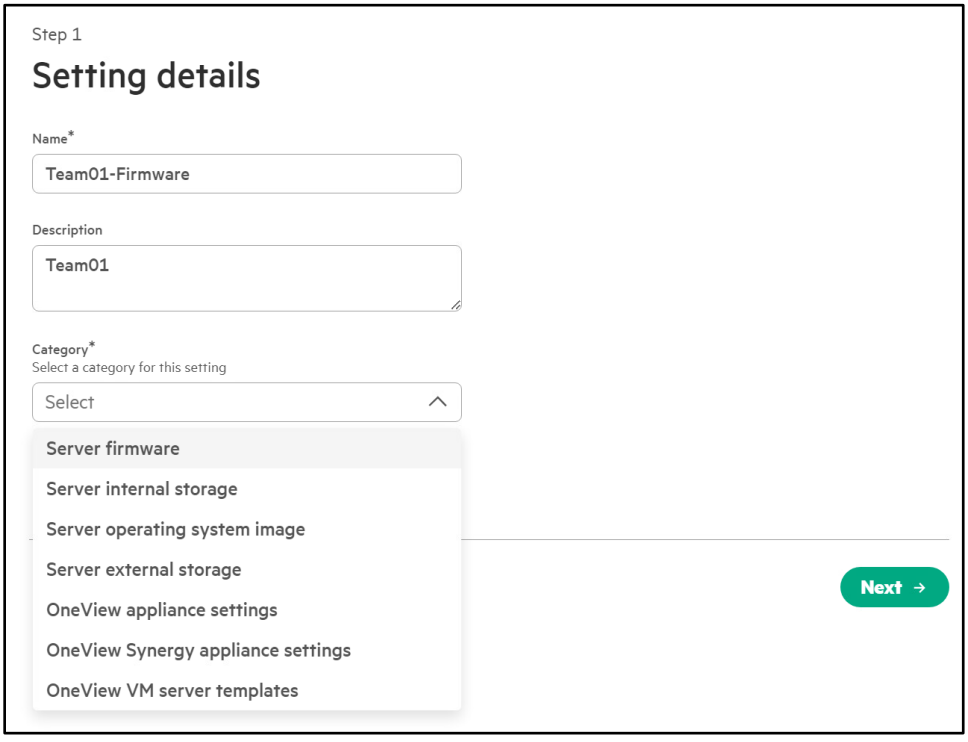
3. Take notice of some of the settings in the Name column and also the Type column associated with each setting. HPE provides some pre-defined settings based on HPE ProLiant UEFI Workload Profiles. These settings are popular with administrators using HPE best practices for workloads like virtualization.



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

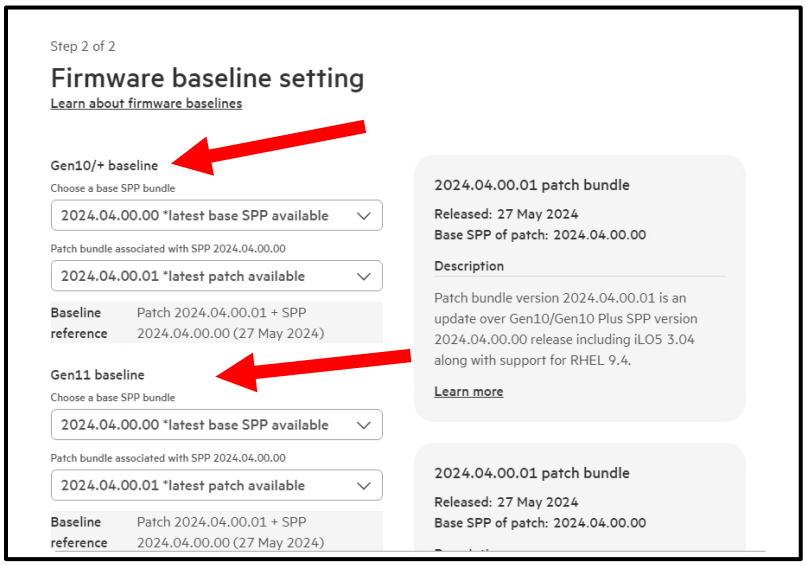


5. On the Server setting details page, **enter your Team name with -Firmware** appended to it. Also **enter your team's name in as a Description**. Finally pick the **Category of Firmware** from the pull-down box.

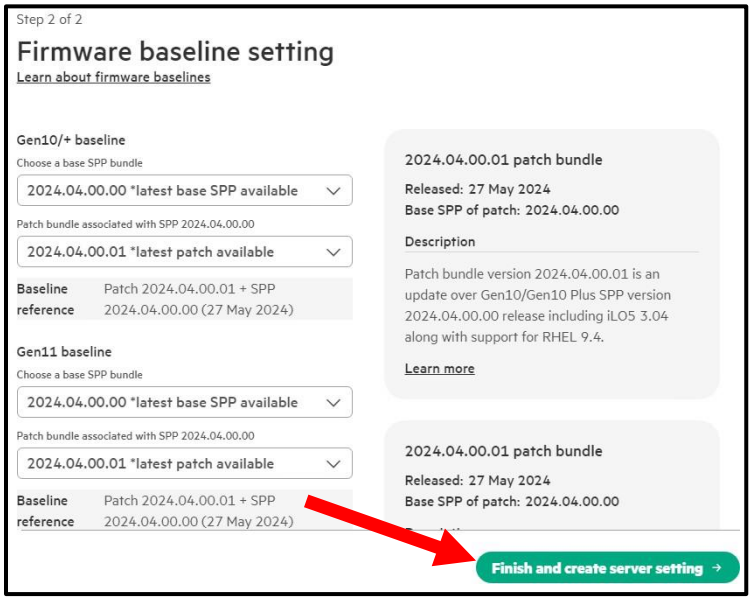


6. Click **Next** to continue.

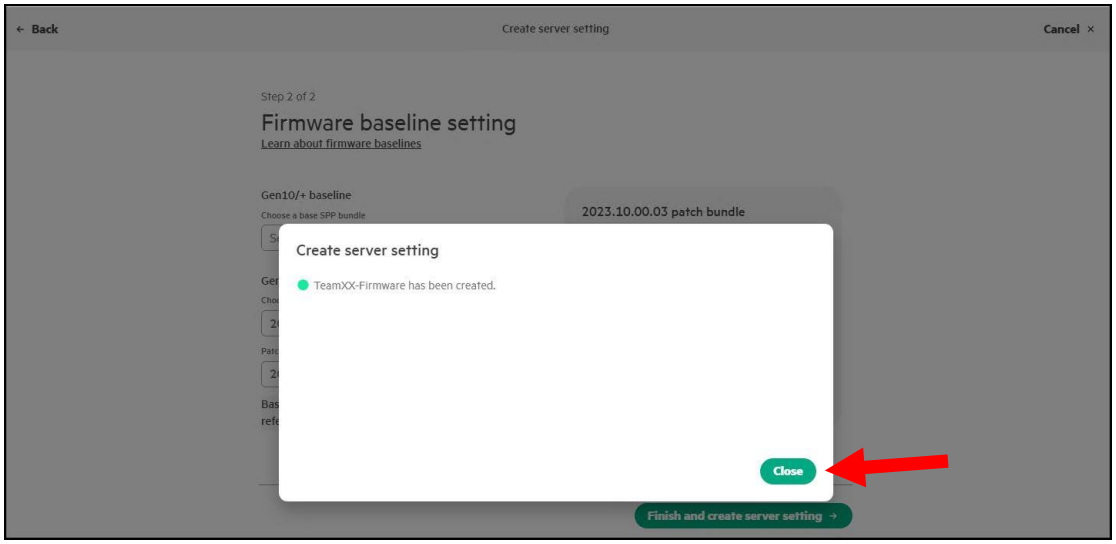
7. Now in step two of the process, **use the pull-down menu in the Gen10/+ and Gen11 section** to select the latest versions of SPP and the latest patch bundles if available.



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



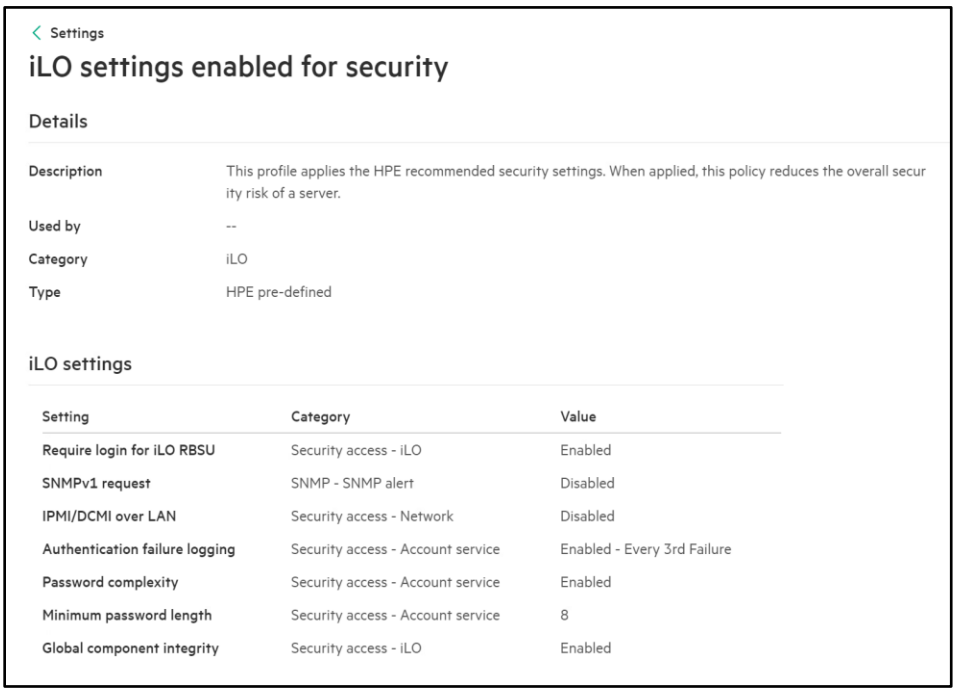
9. You should see the setting for firmware successfully created. Click on **Close** to finish the process.



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:

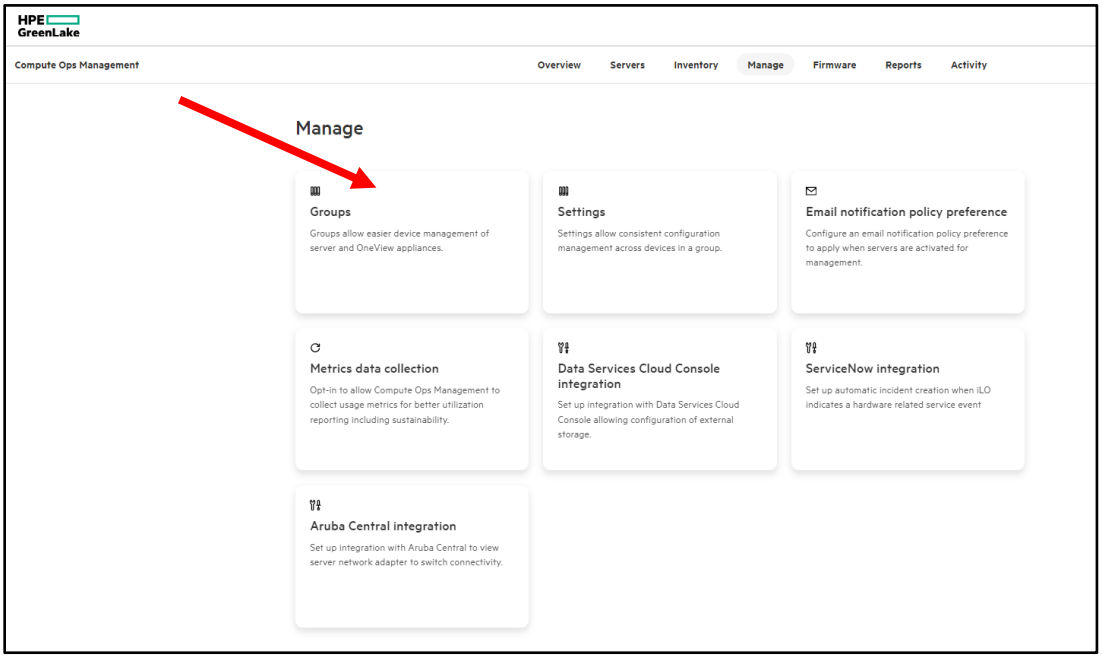


This concludes this section of the lab.

Creating server groups and associating server settings

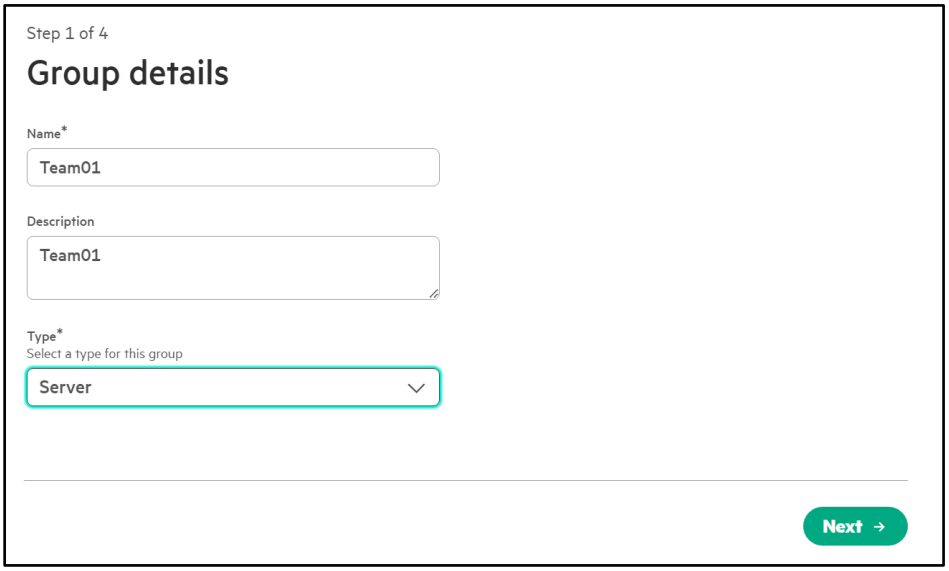
Server groups allow you to organize servers based on specific criteria (e.g., location, function, or role). When you create or edit a server group, you can apply server settings and server group policies. Servers directly managed by HPE Compute Ops Management can be added to server groups where these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

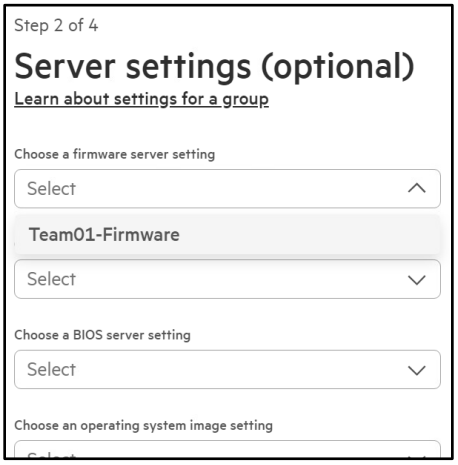


2. At the **Groups** page, click on **Create a group.**

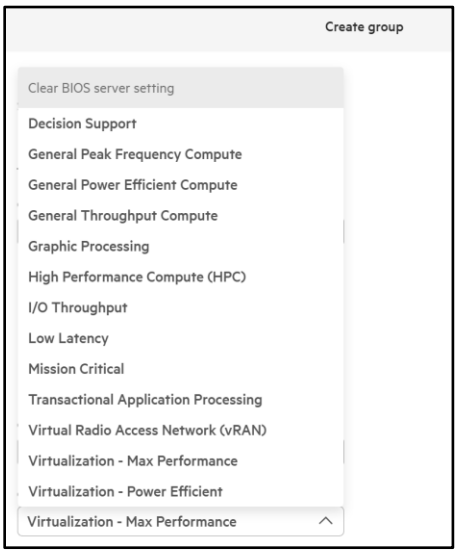
3. In the Group details section, **enter your Team name** in the Name field and **then again for the Description** field. Select **Server** as the type, then click on **Next** to continue in the wizard.



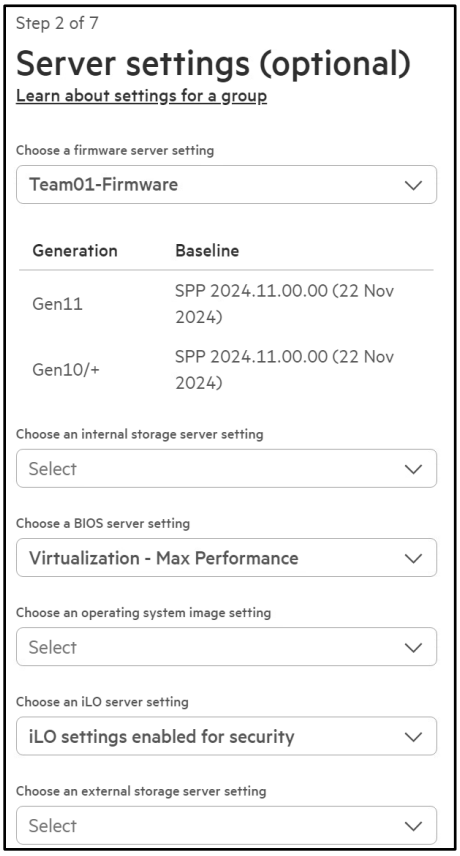
4. In the next screen of the wizard, **use the pulldown menu** to **choose** your previously created **Firmware setting**.



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

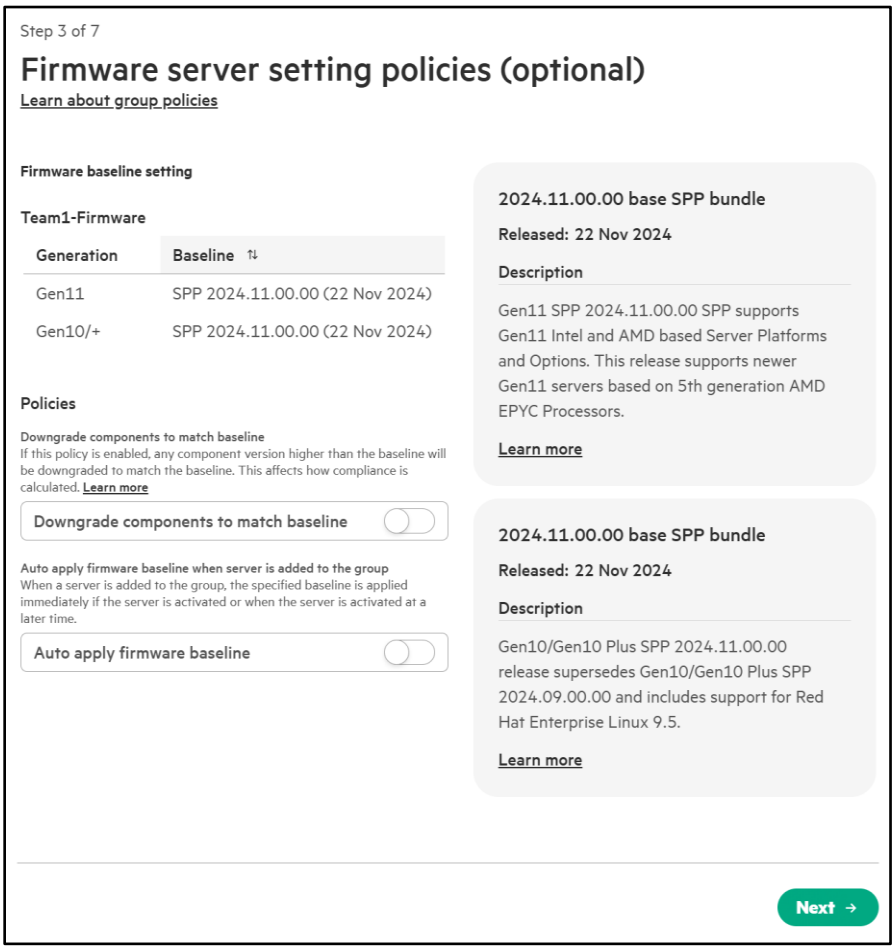


6. In the section **Choose an iLO server setting** box select **iLO settings enabled for security.**



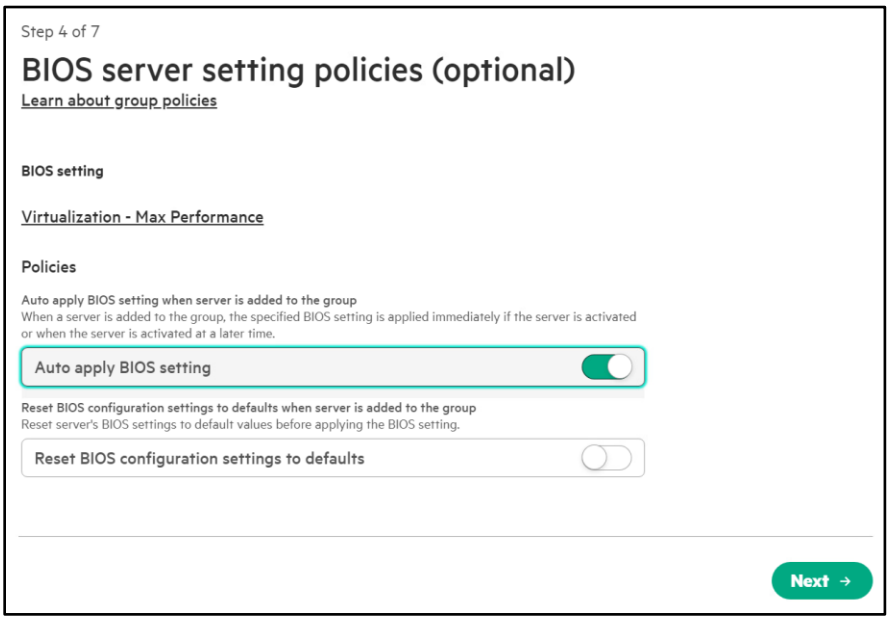
7. Leave the rest of the options in this initial section at their default values, and then select **Next** to advance in the wizard.

8. Normally we would enable the Auto apply, but for the purpose of this Lab we will leave it **disabled**.

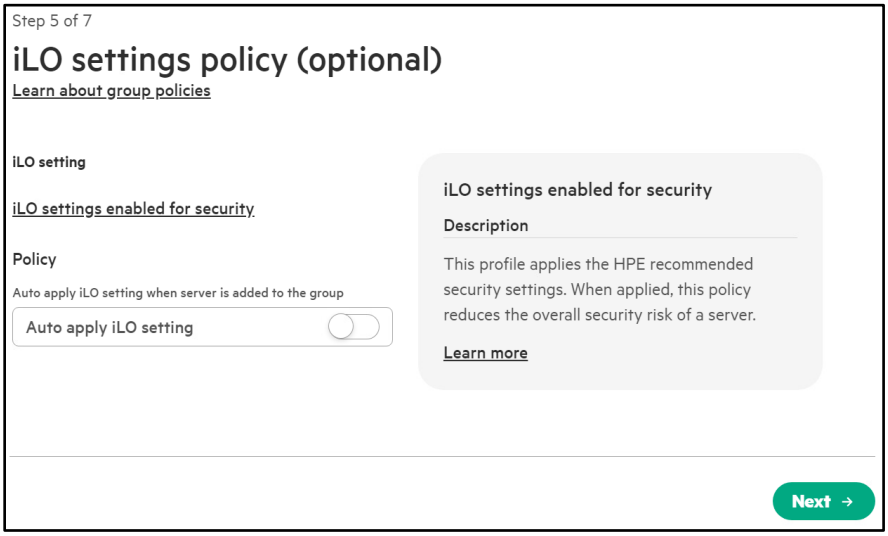


9. Click **Next** to continue.

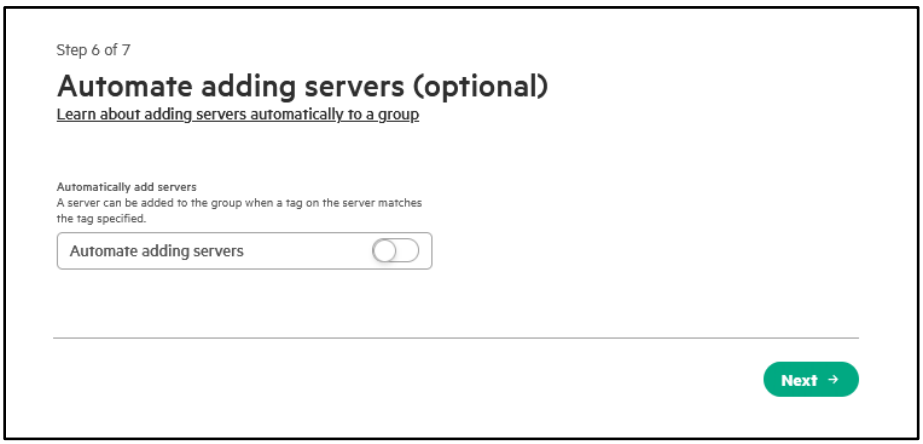
10. **Enable** the Auto apply BIOS settings policy and then select **Next**.



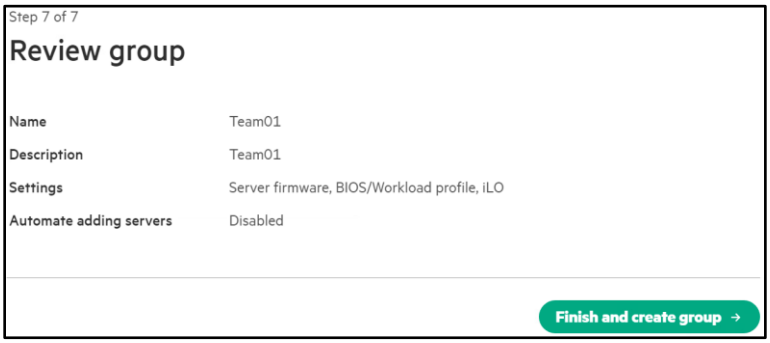
11. For **auto applying the iLO Setting**, leave this **disabled** for now so we can **manually apply this later** in the Lab, click **Next** to continue.



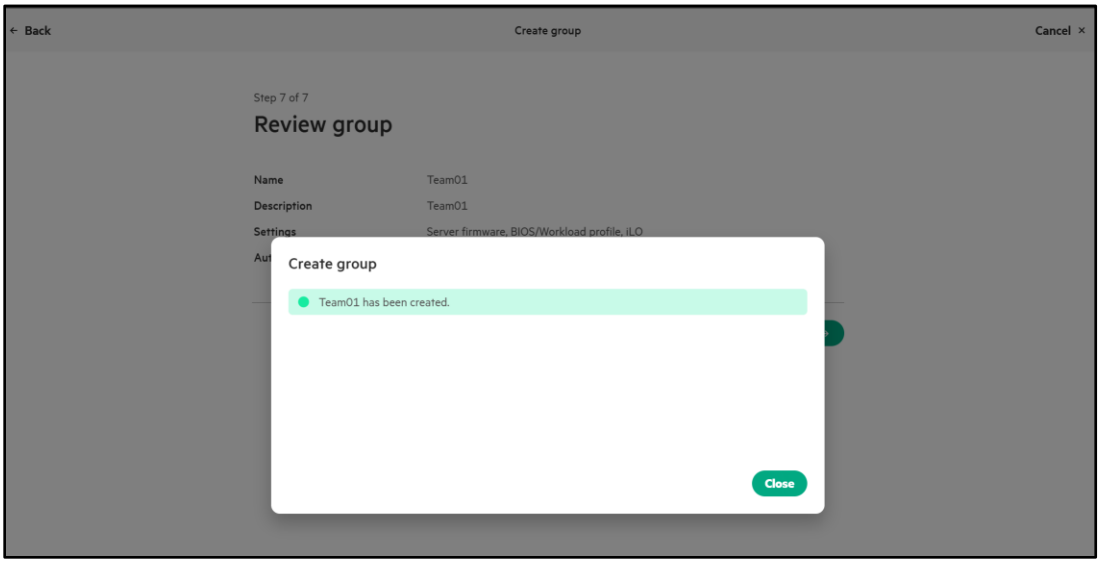
12. For the question of how we are adding our servers to the group, we are going to setup the group for manual addition of servers to the group. Select **Next** to move to the finish.



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



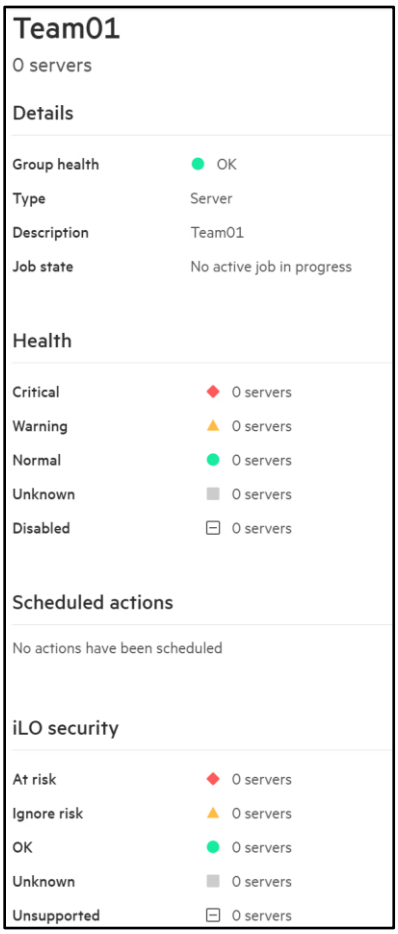
14. The group should be created, and you can click on **Close** to finish the process.



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

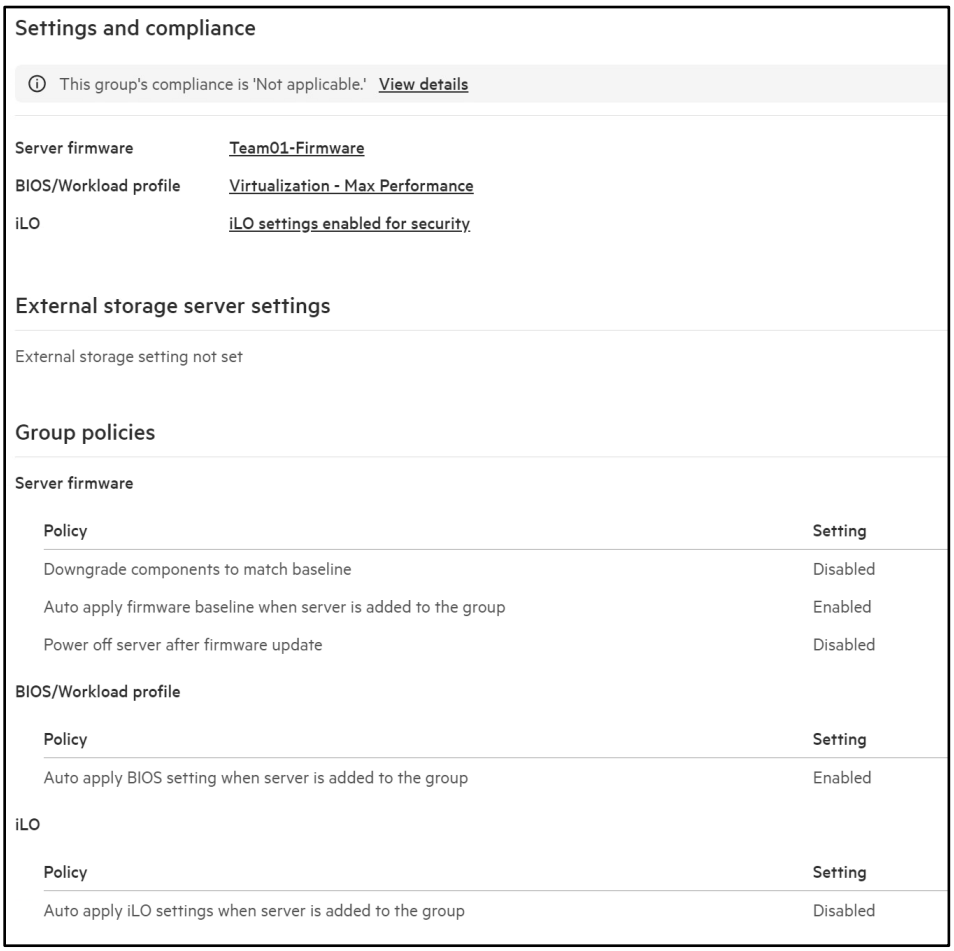
Scheduled actions

No actions have been scheduled

iLO security

At risk	0 servers
Ignore risk	0 servers
OK	0 servers
Unknown	0 servers
Unsupported	0 servers

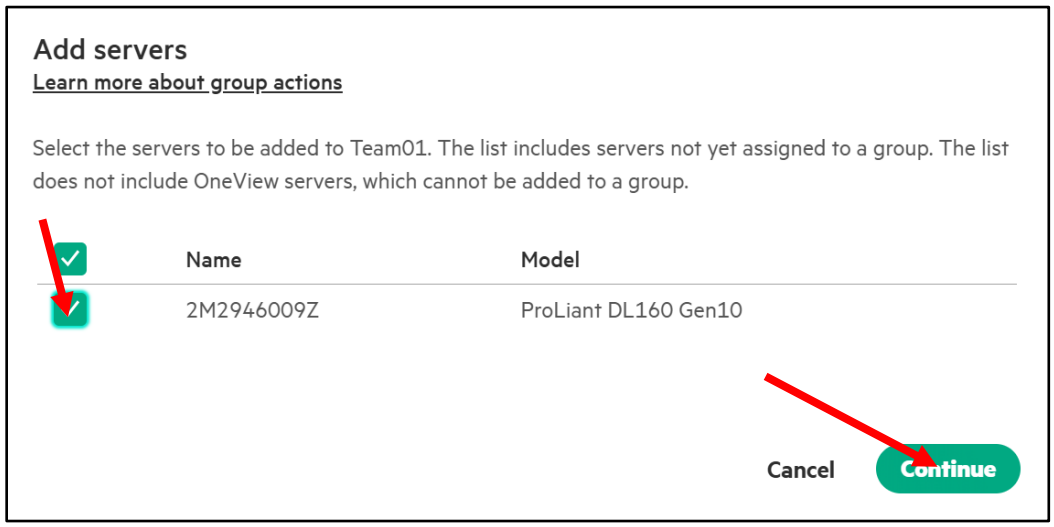
17. Scroll down to **Settings and compliance**. These are the details of what you just defined at the group level.



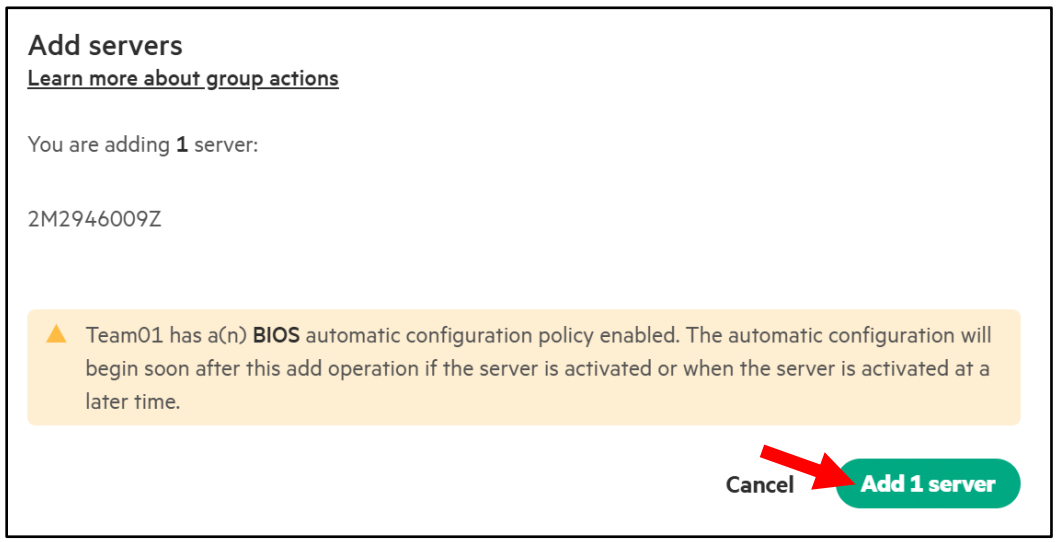
18. Scroll back up to the top of the page and click on the **Actions** button (to the right of the frame) to reveal how functions are performed on the entire group.

19. Click **Add servers**.

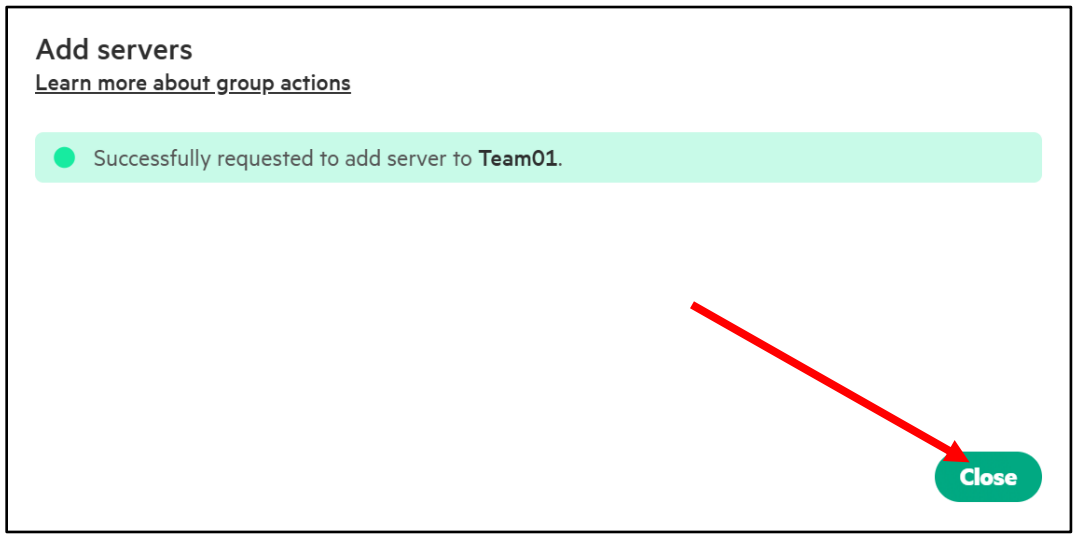
20. **Select your server** by clicking the **checkbox** next to its name then click **Continue** to proceed to the summary.



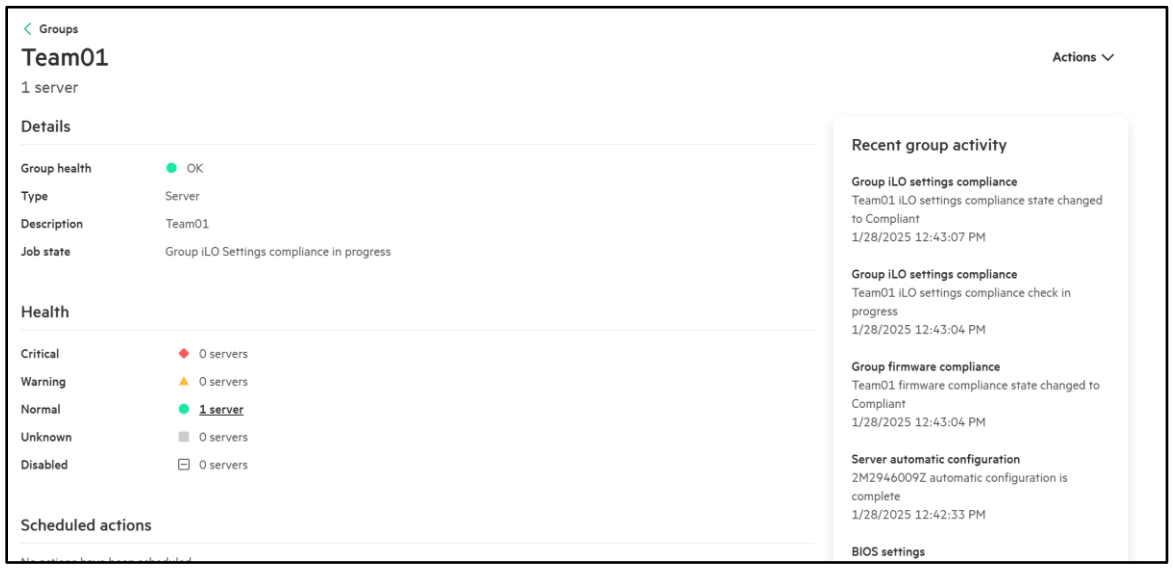
21. Review the actions that will take place on your server before clicking **Add 1 server.**



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.



This concludes this section of the lab.

Advanced Security settings for iLO

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

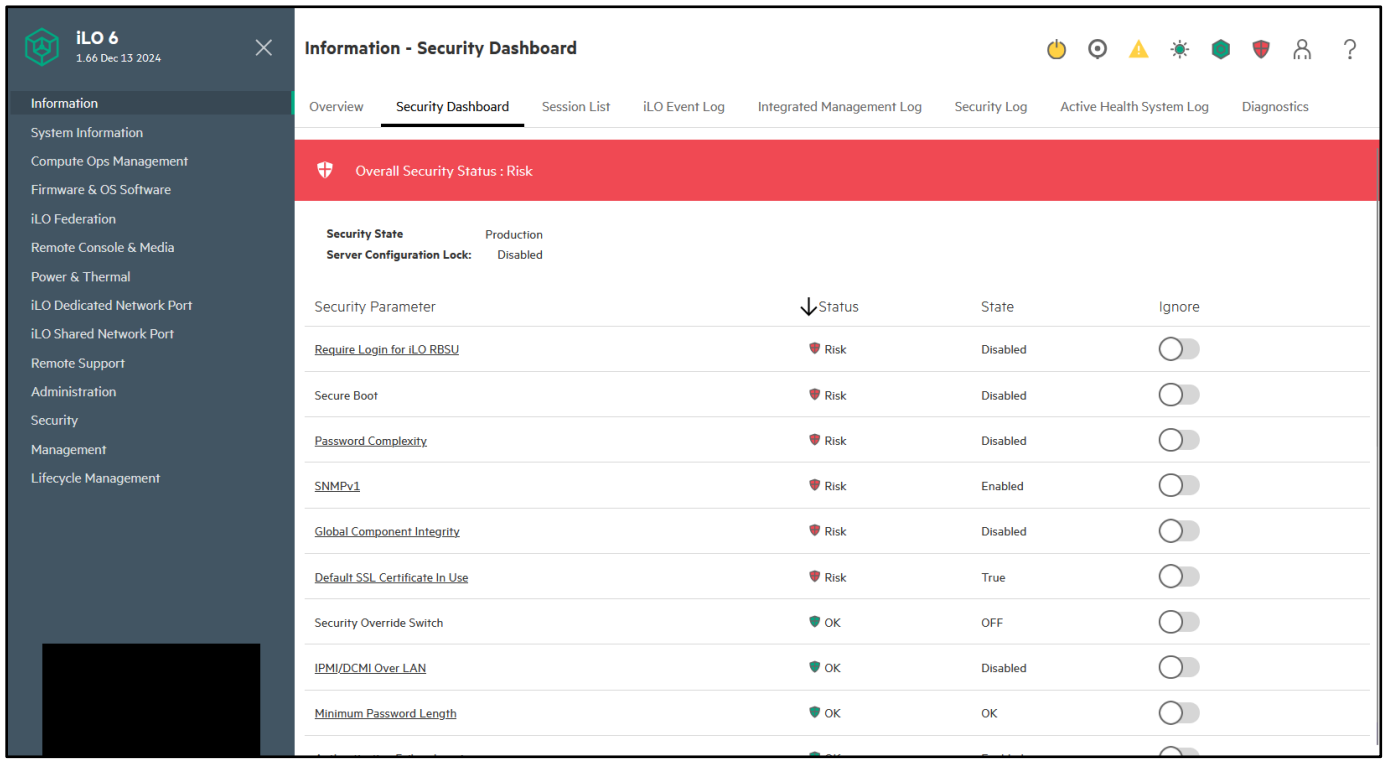
In this lab we will look at security parameters like in Network Settings where we can enable/disable various services (e.g., SSH, SNMP, Virtual Media.) We will configure anonymous data and IPMI/DCMI over LAN. Idle Connection Timeout values can be set.

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

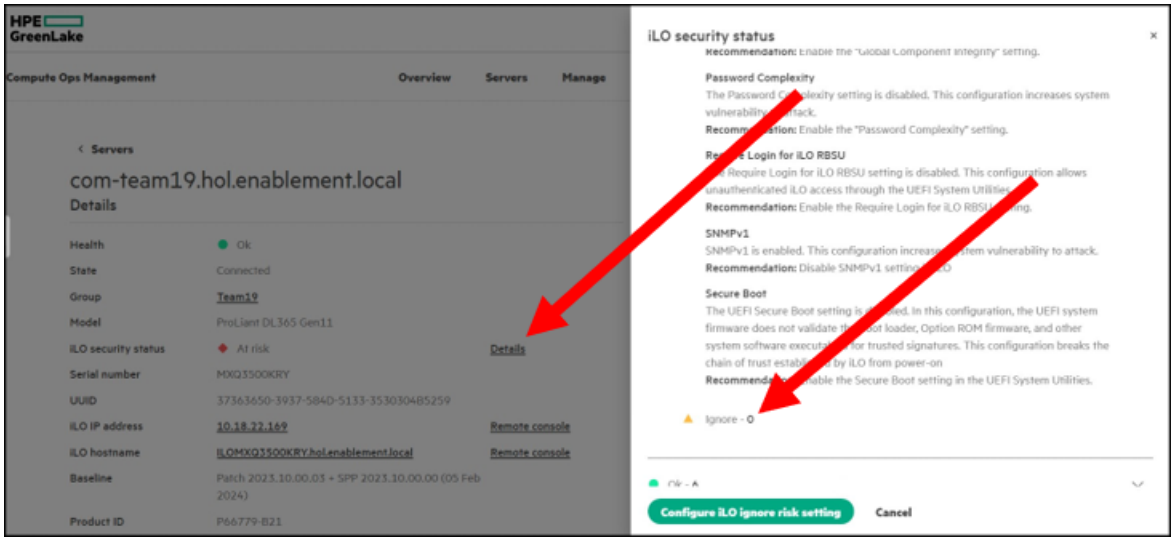
Finally, the iLO Security Dashboard provides real-time insights to monitor and manage security settings proactively.

1. Navigate back to your **assigned Servers iLO.**

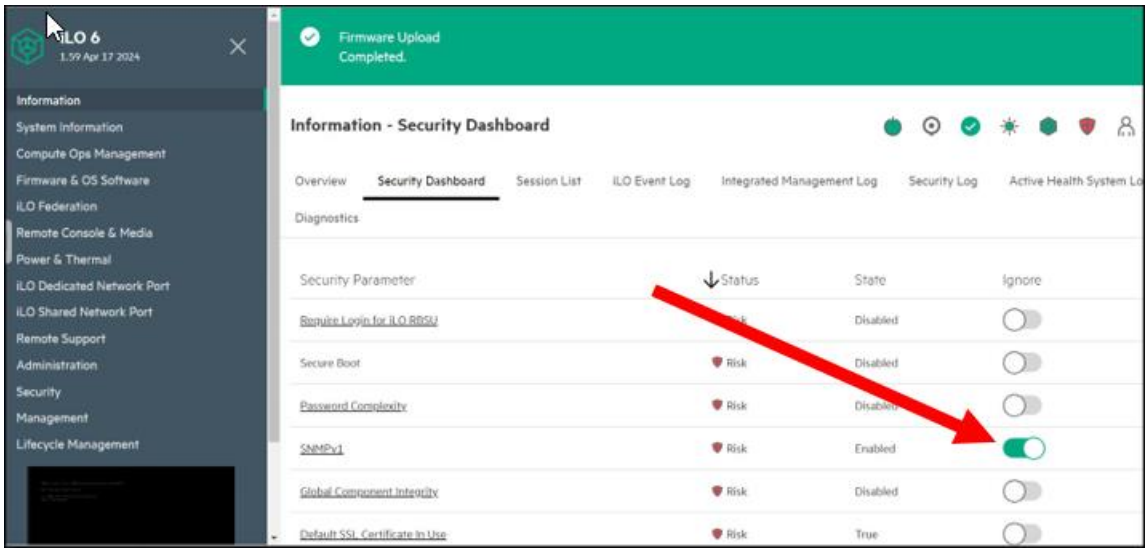
2. From the iLO Information page, click on the **Security Dashboard** tab across the top of the page.



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.

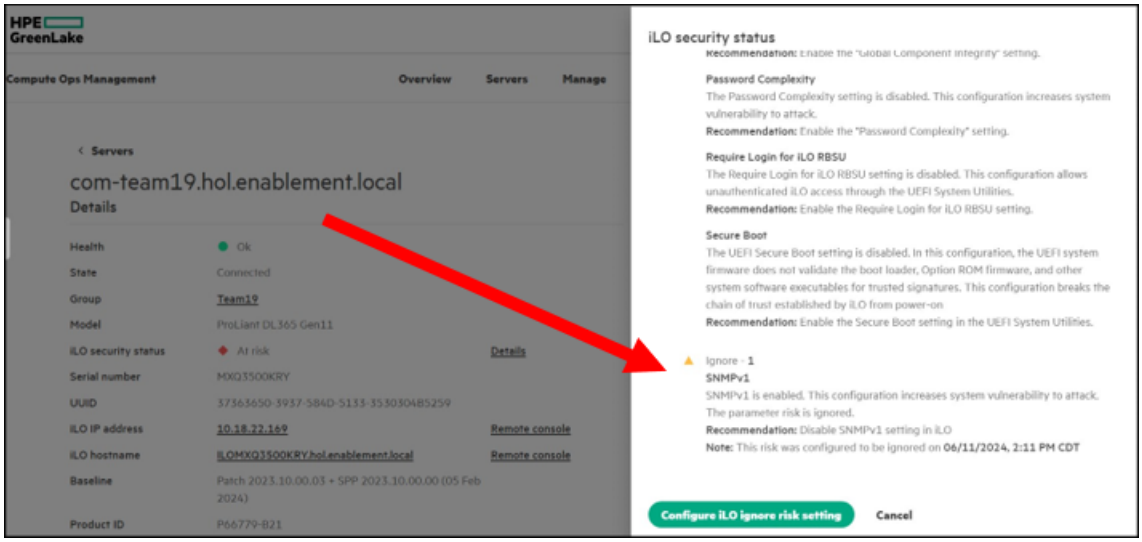


4. Return to the iLO6 **Security dashboard** screen**.** Select the option for **SNMPv1** and toggle on the ability to **ignore the error**. This is not a best practice for the “real world”, but we are demonstrating the connection between your iLO6 and COM.

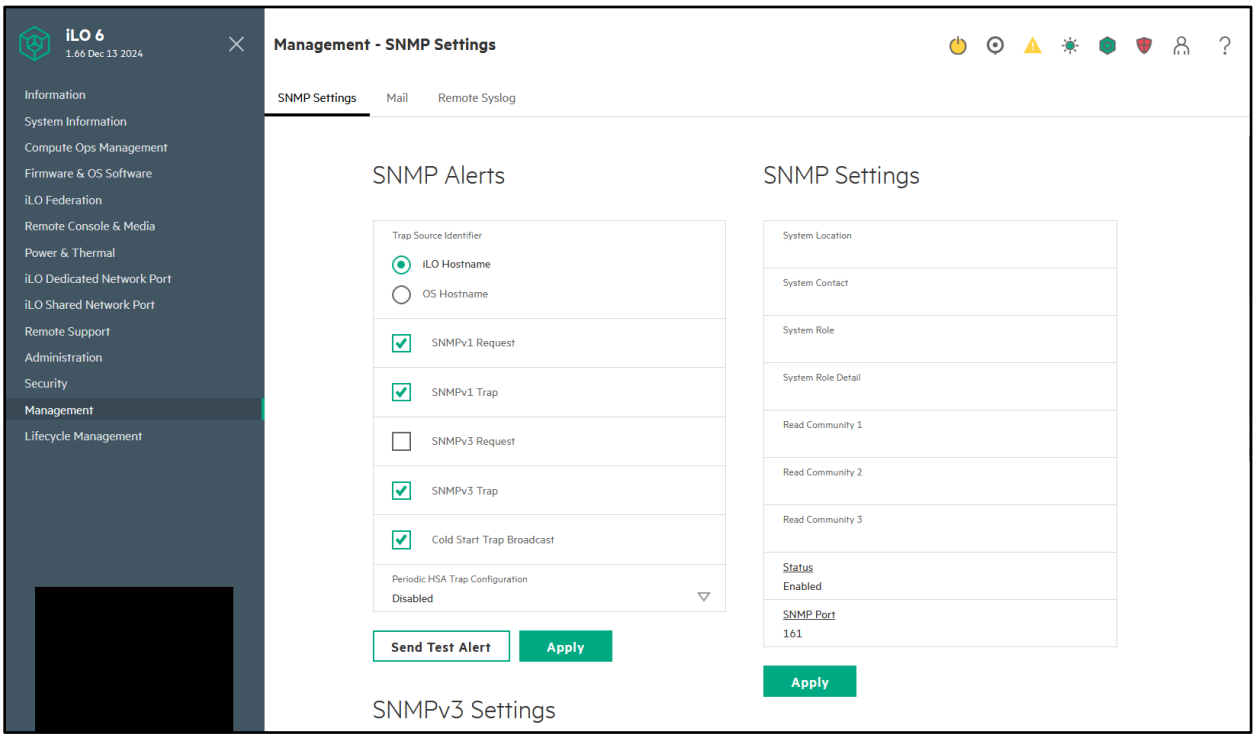


Note: This task can be easily automated using the **Enable-HPECOMIloIgnoreRiskSetting** cmdlet from the **HPECOMCmdlets** PowerShell module.

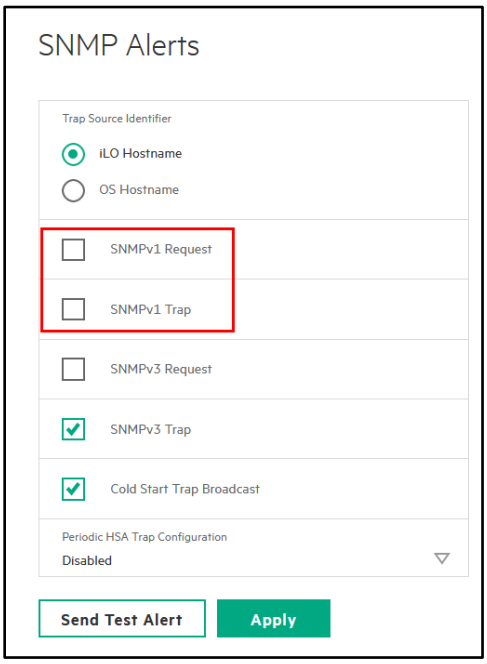
5. Back at the COM screens, you see that now we do have an error that is ignored.



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**.

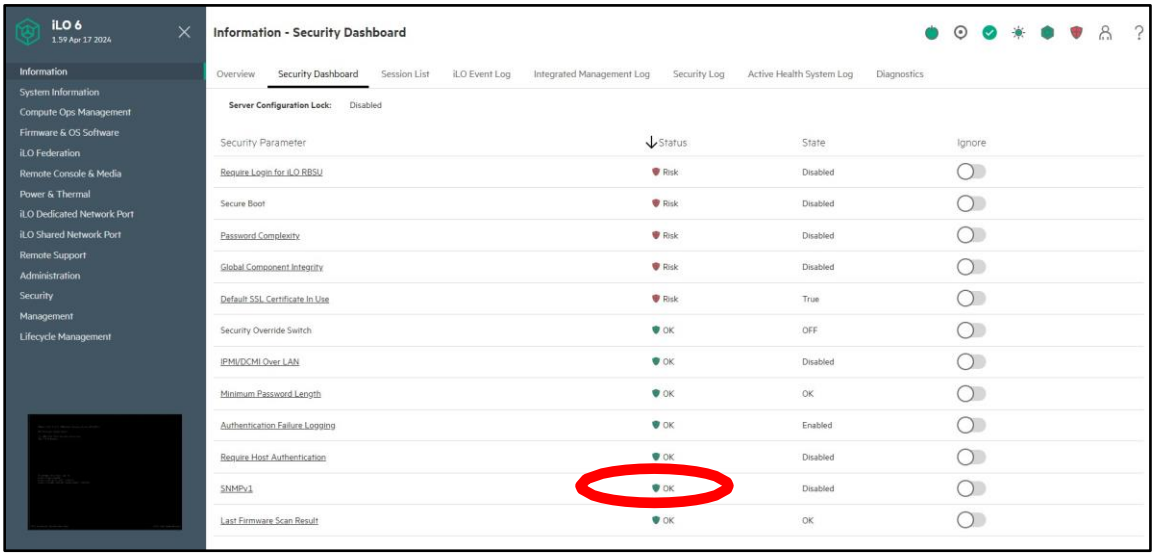


7. In the SNMP Alerts section, uncheck **SNMPv1 Request** and **SNMPv1 Trap**.

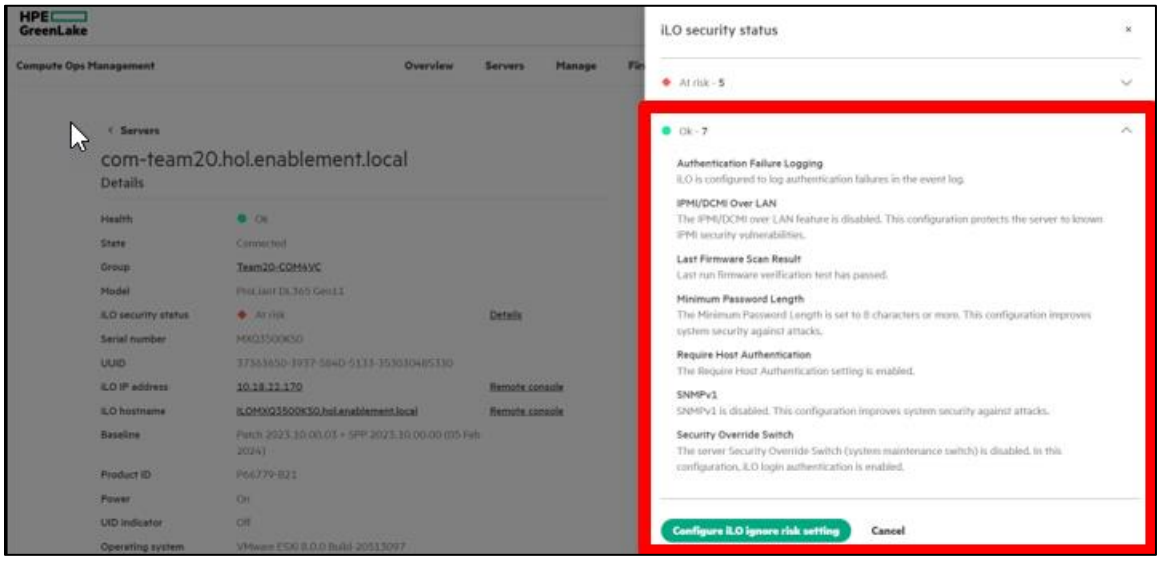


8. Click the **Apply** button.

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

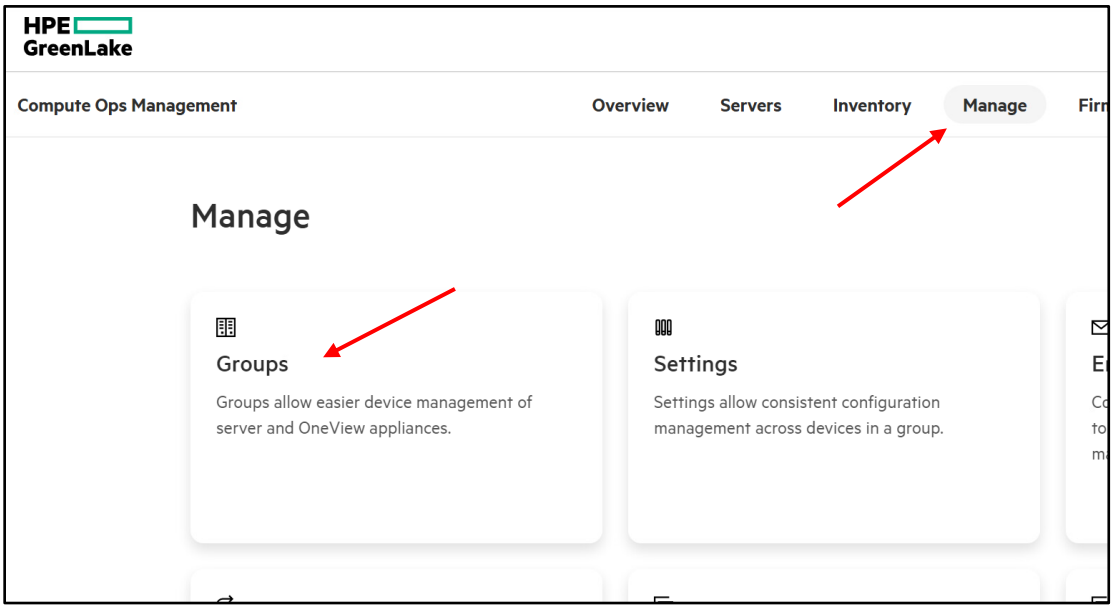


10. Return to the Details page that you have loaded in Compute Ops Management. Note that SNMPv1 is no longer a risk.



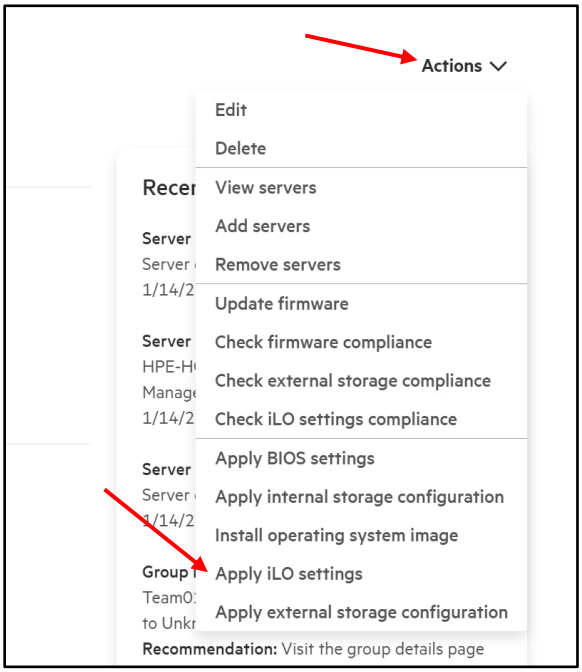
There are other items that need particular attention, such as Secure Boot and the use of self-signed certificates. These two are essential for iLO security. We will later cover how to generate a CA-signed certificate. For information on Secure Boot, you can refer to the UEFI System Utilities User Guide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

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.**

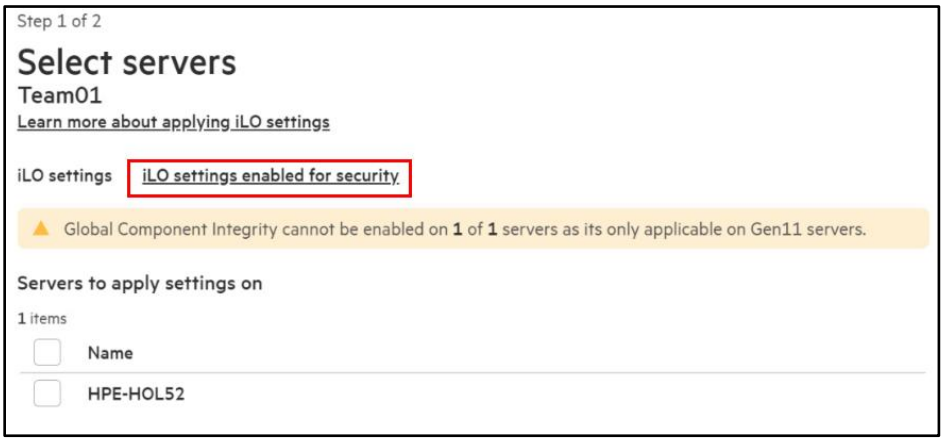


12. Click on the **hyperlinked Name** of your **Group/Team.**

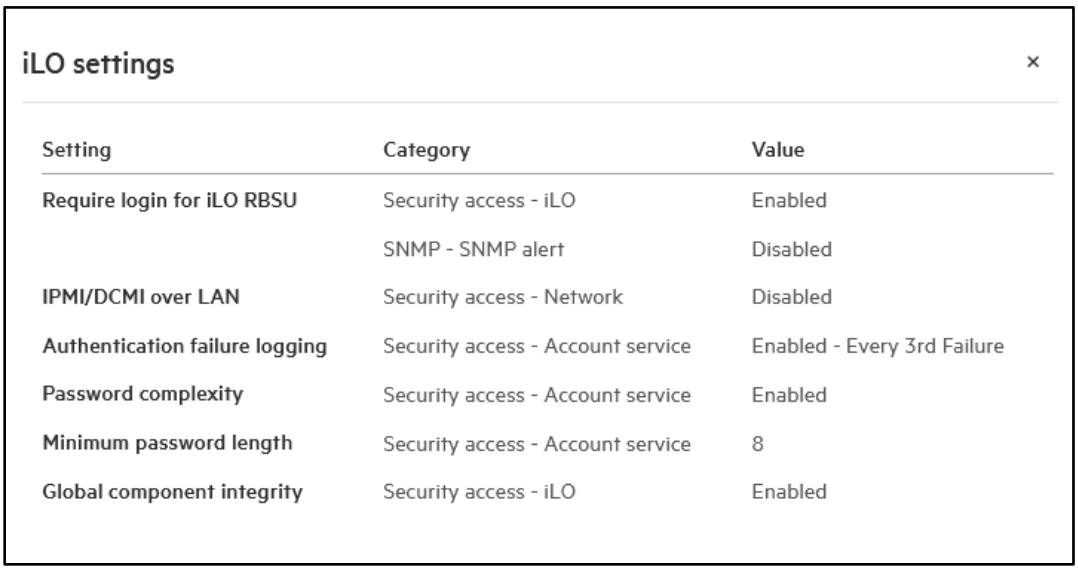
13. From the **Actions** drop down menu, select **Apply iLO Settings**.



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



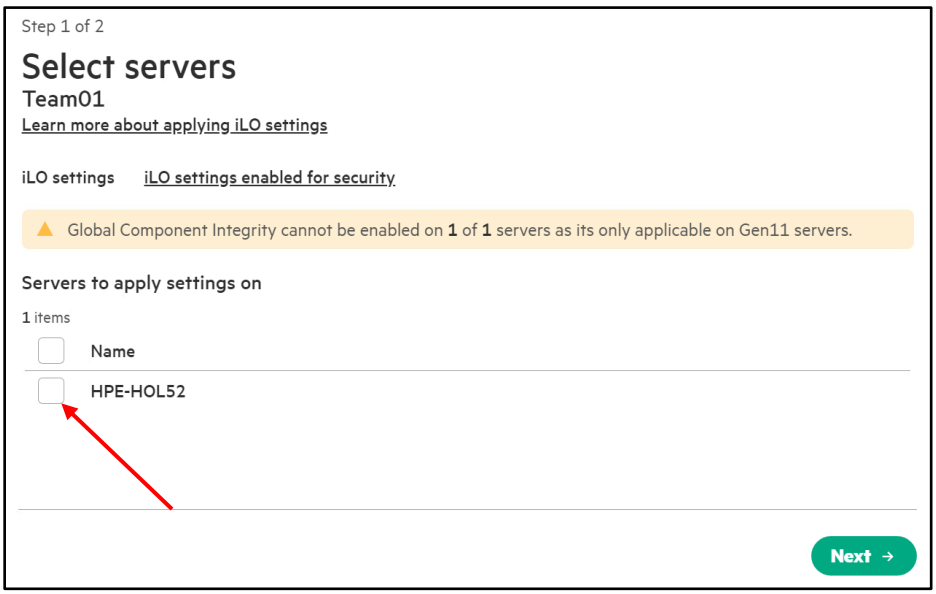
15. This list shows the **HPE recommended iLO settings** that will be pushed to our server to reduce the overall security risk:



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

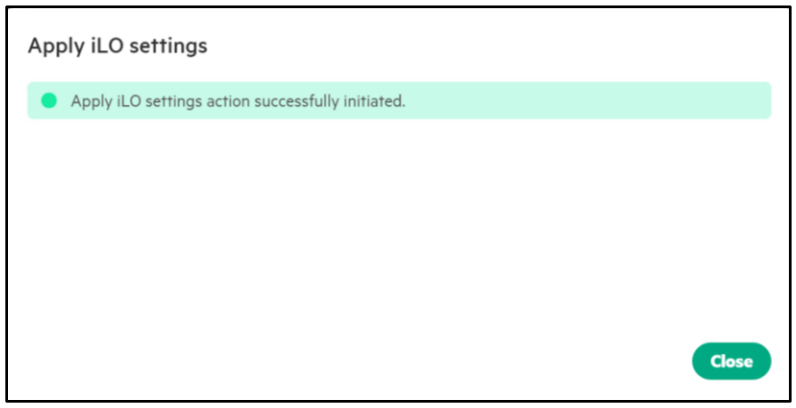
16. Click the **X** to close this popup.

17. Select your **assigned Server** from the list and hit **Next**.

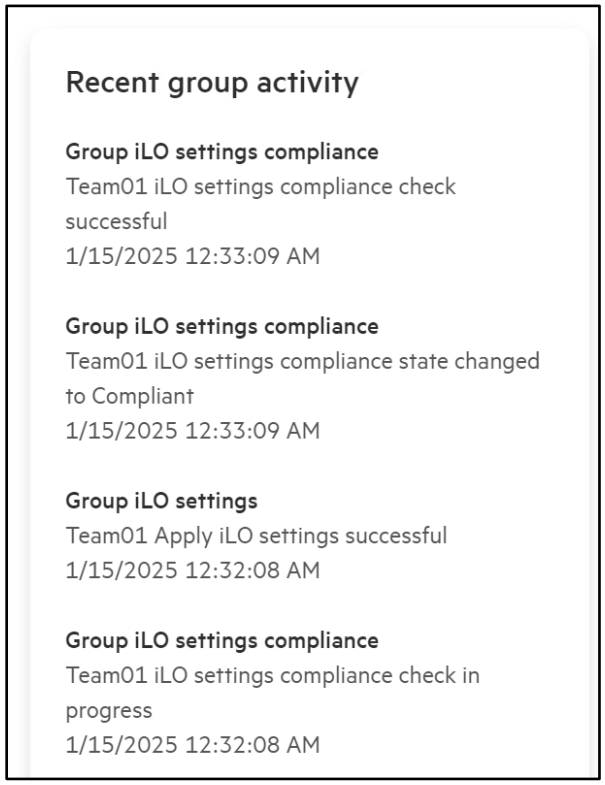


18. Review your changes, then hit **Apply iLO Settings.**

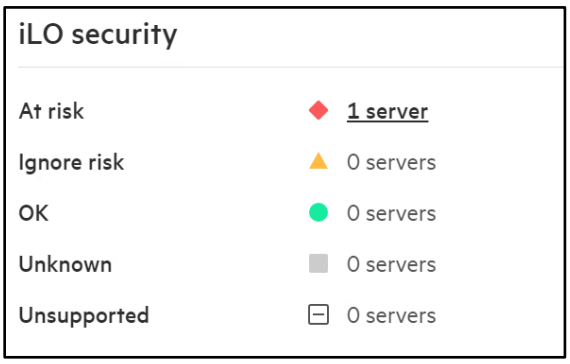
19. Hit **Close** on the pop up, to return to your Group details.



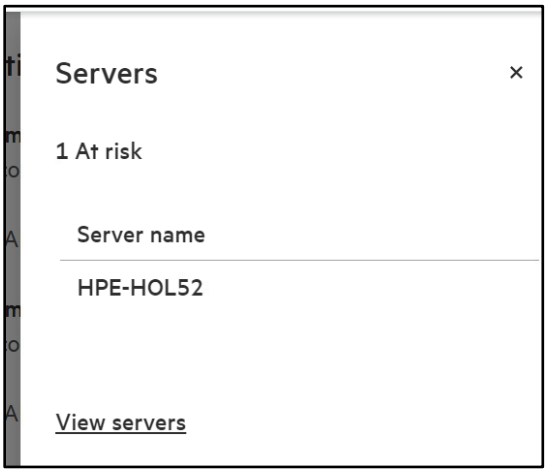
20. In the **Recent group Activity**, you should now see the **iLO settings being successfully applied** and the **settings compliance** changed to **Compliant**.



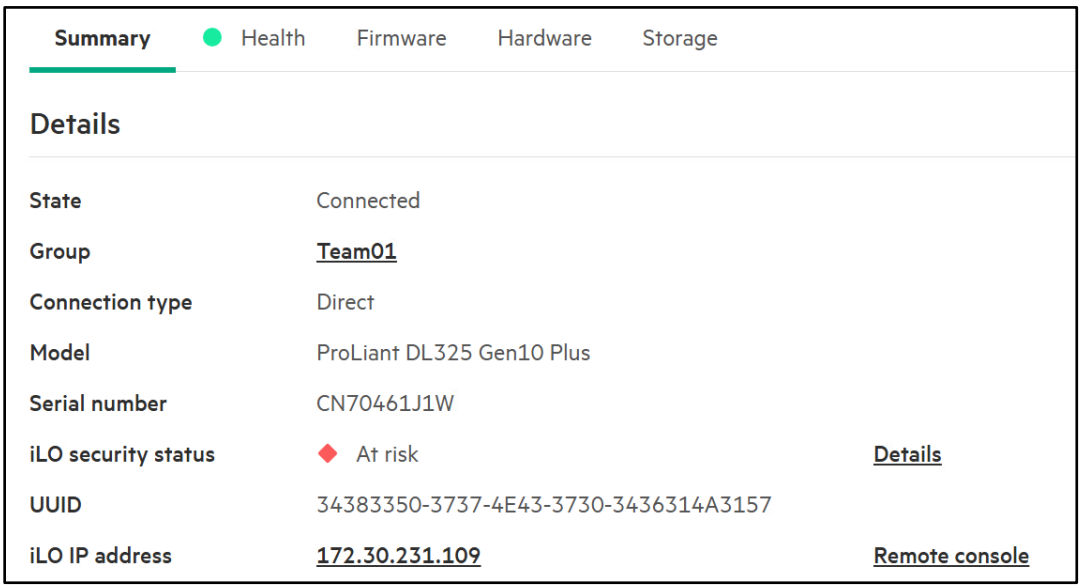
21. If we look to the **left of the screen**, we can see our **iLO Security** section still showing **At risk**. Let's click on the **hyperlink.**



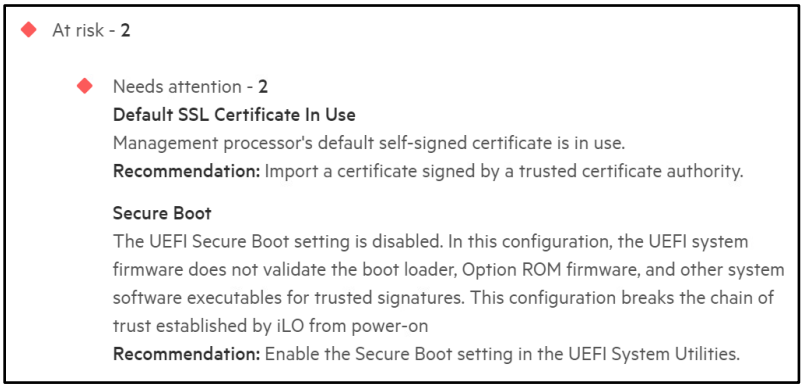
22. On the right, click again to select the **Server at Risk.**



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

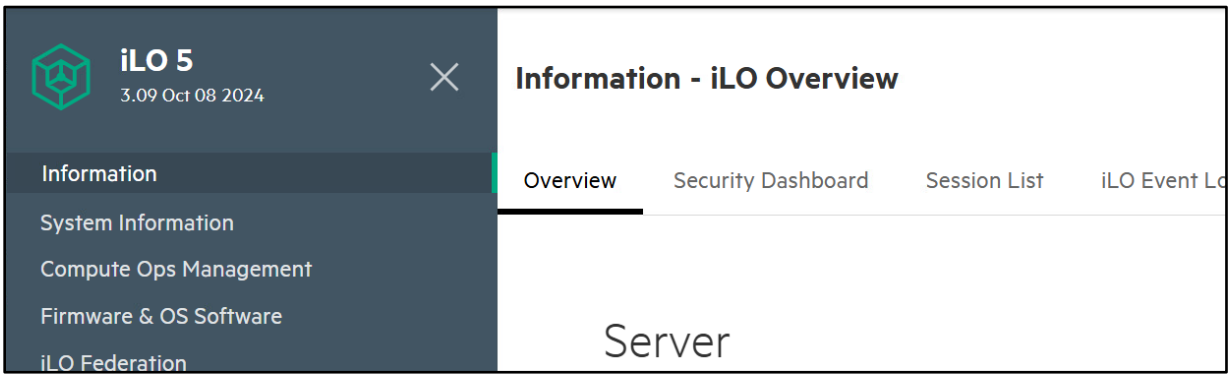


24. You should see **two items still at Risk**, both of these have **dependencies** outside of the COM deployed iLO settings which may require manual intervention to resolve.

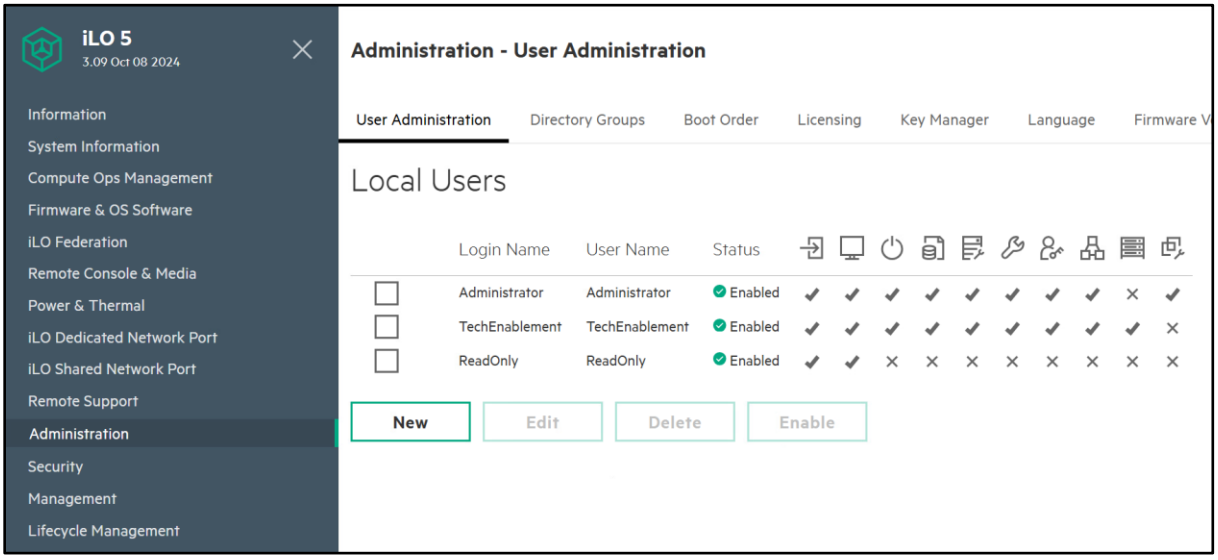


25. In the next section of this Hands On Lab, we will be following steps to **Request and Apply a Signed Certificate** from a **trusted Certificate Authority**.

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

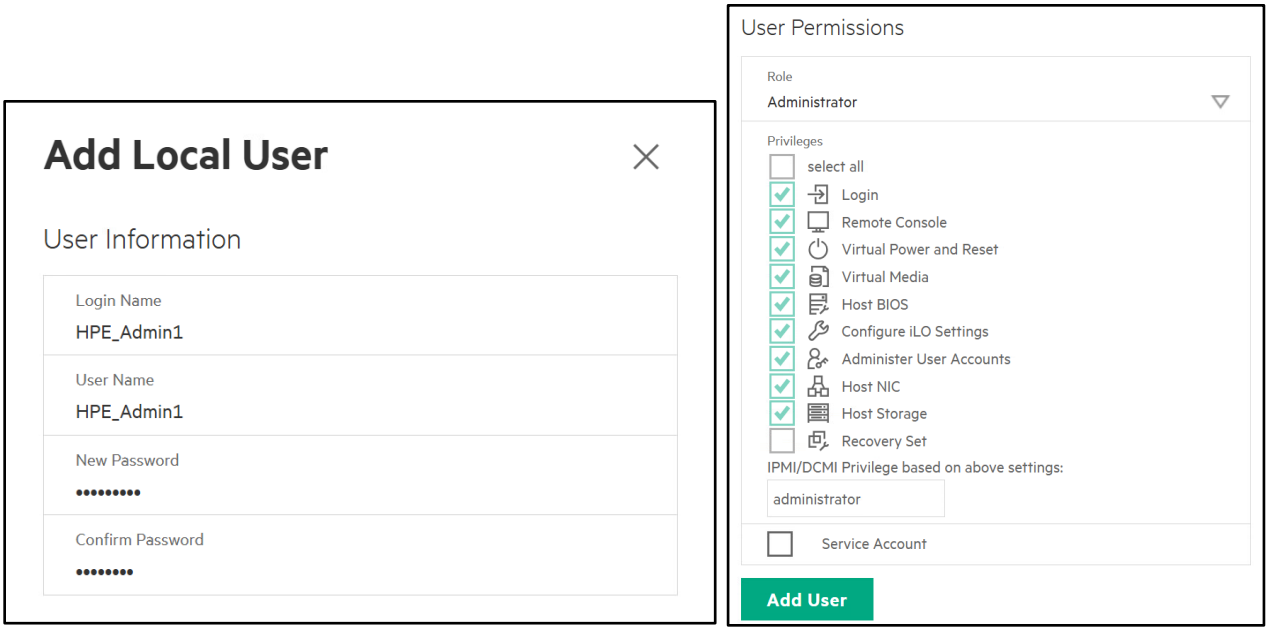


27. Earlier in the lab, we created a new Administrator privileged User with a simple password. Let's go back to **Administration** and look at creating another new user.

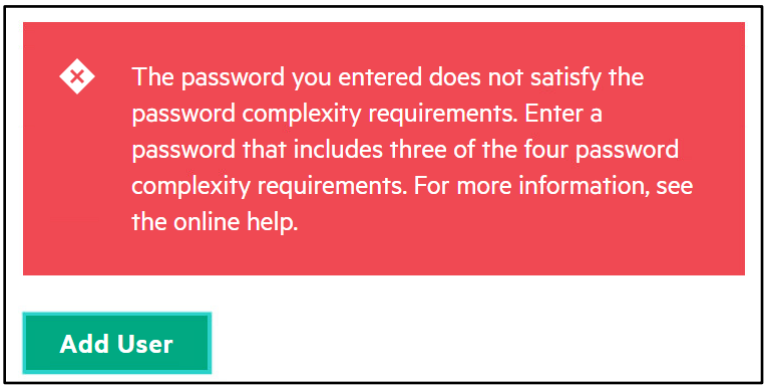


28. Click **New** in the Local Users frame and enter the following settings to create your new user account.

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



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.



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.

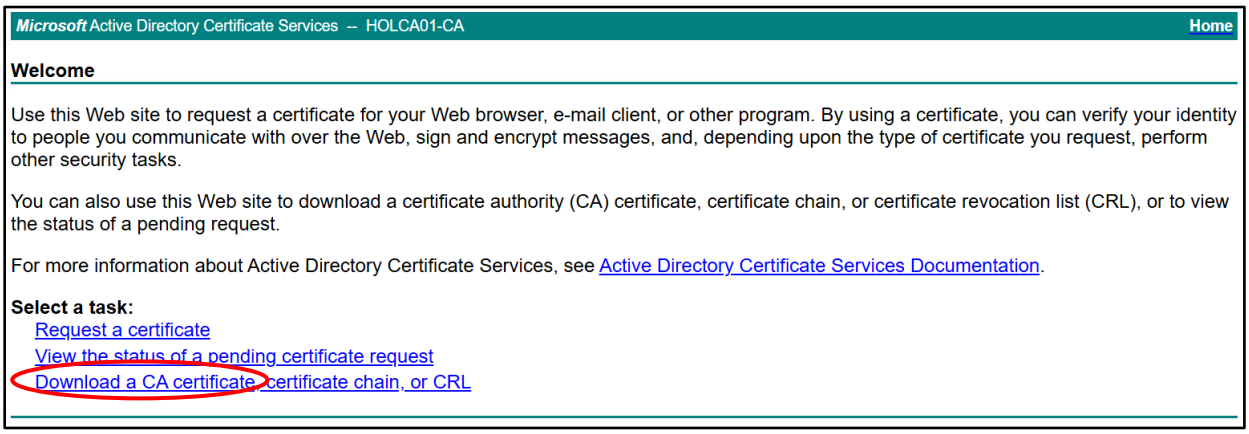
If you are looking for information about how to do it manually, see Generate CSR and Import an SSL Certificate.

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/**

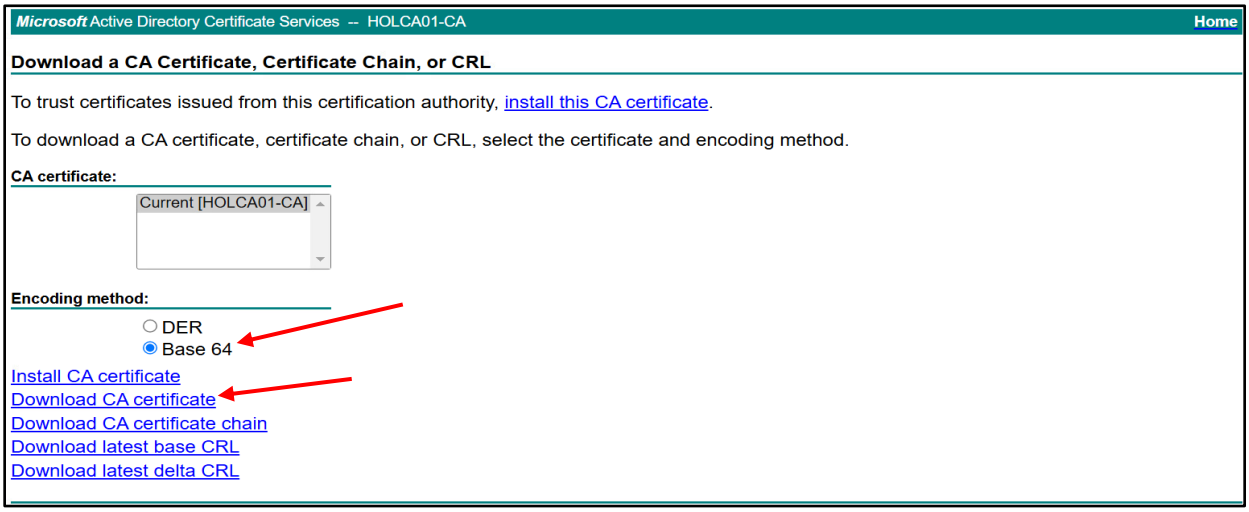
   This server is our internal lab Certificate Authority (CA) server, provided by Microsoft Active Directory Certificate Services.

2. Login with Username - **ENABLEMENT_ndes_svc** and Password - **Get-My-Cert!**

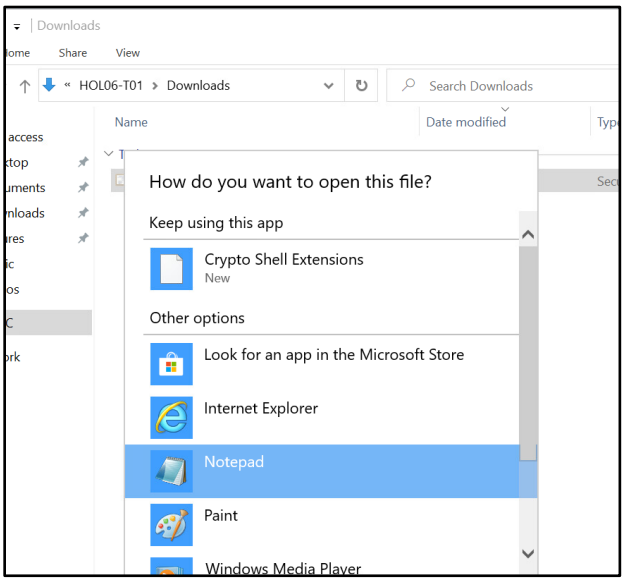
3. Click **Download a CA certificate.**



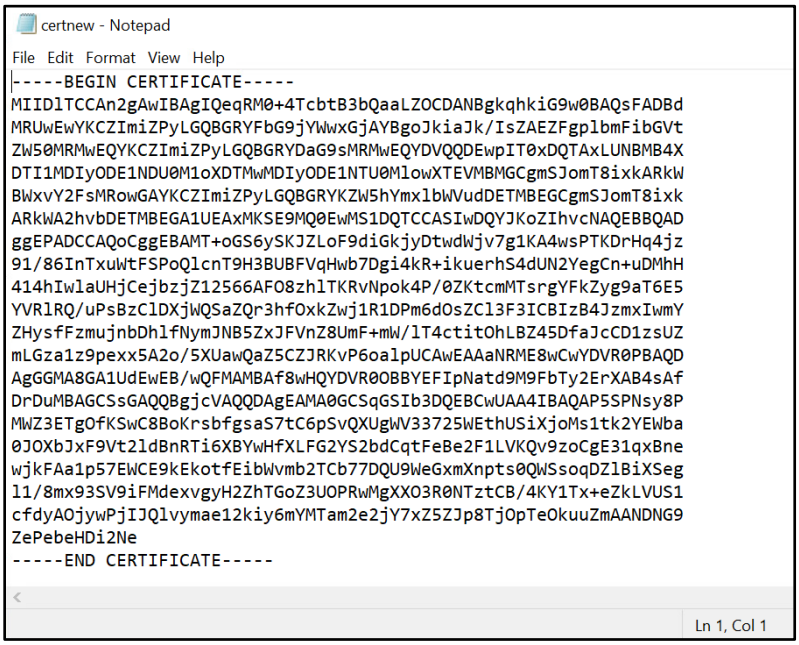
4. Ensure **Base 64** is selected as the Encoding method and then click **Download CA certificate**.



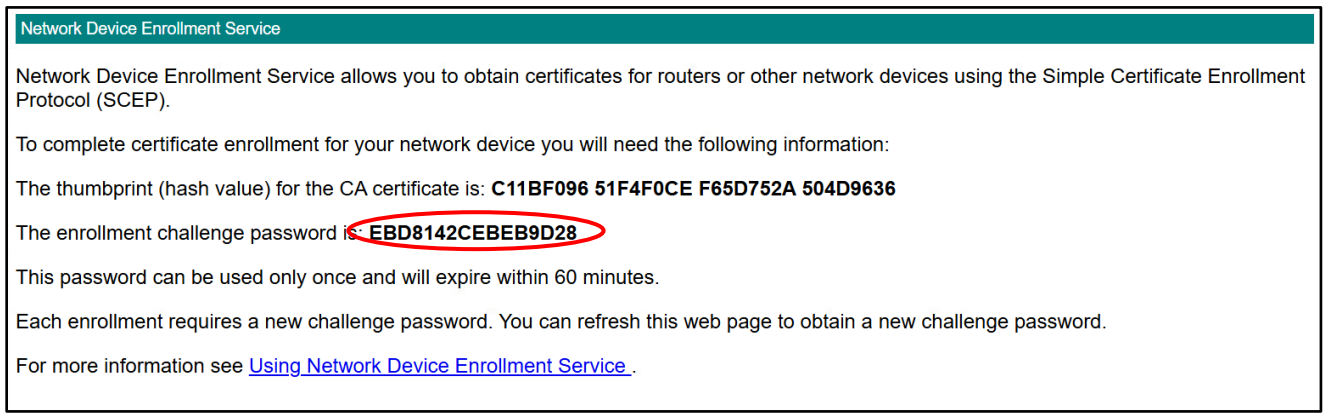
5. **Open the Folder** where it was just saved to and then **open the file in Notepad**.



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.



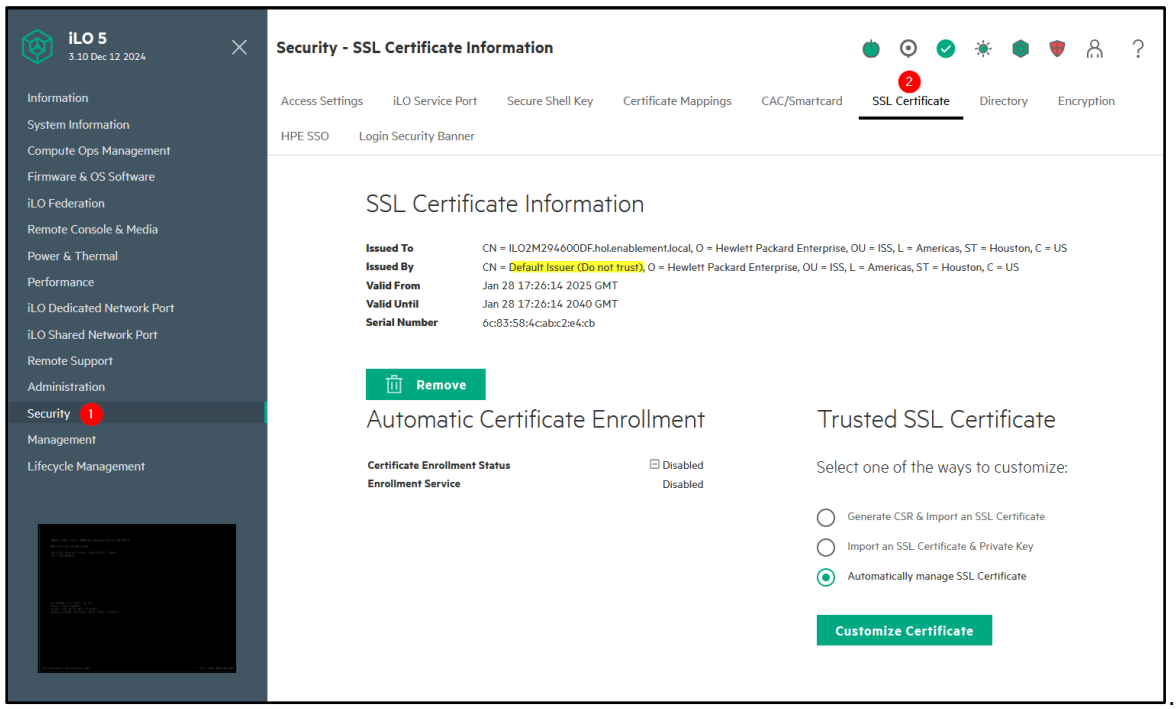
7. Next, you need to **retrieve** the **challenge password** from the certificate enrollment server – In a new tab navigate to **https://holca01.hol.enablement.local/certsrv/mscep_admin/**



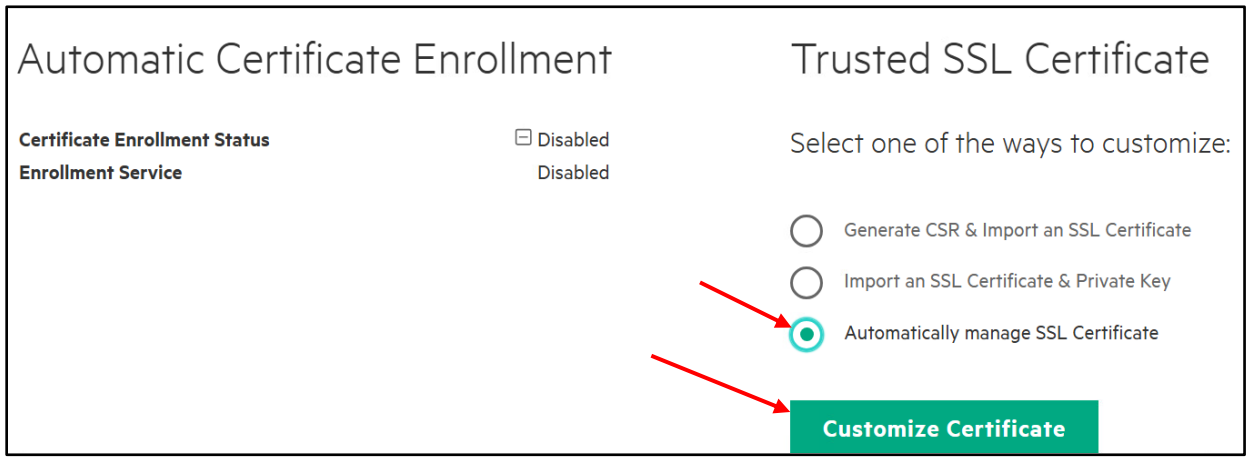
This URL is where you can obtain the challenge password that will be used later by the iLO to secure the connection with the NDES server during the certificate enrollment process. Note that the NDES server is the same as our internal lab CA server. Although this server plays both roles in our configuration, 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**.

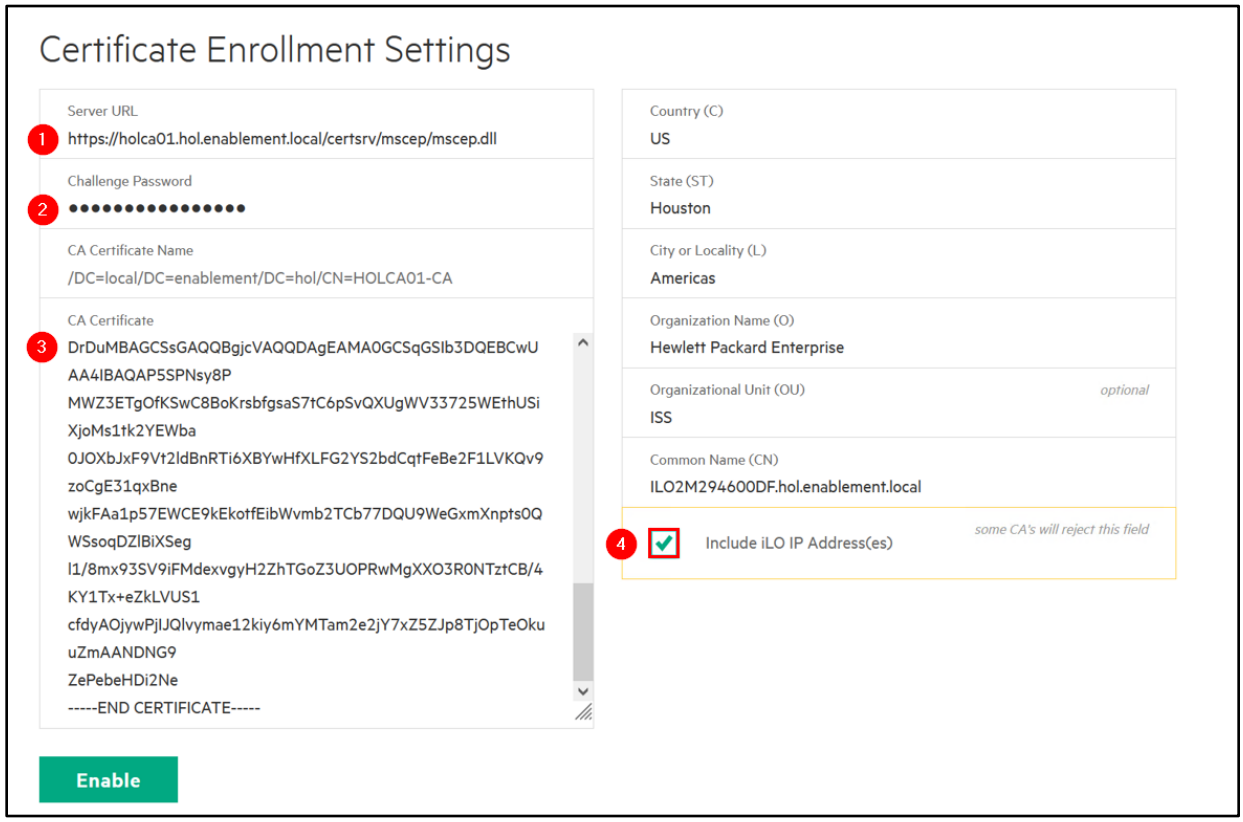
9. We will now navigate back to our **iLO Web UI**, click on the **Security** menu on the left, then **SSL Certificate**.



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**

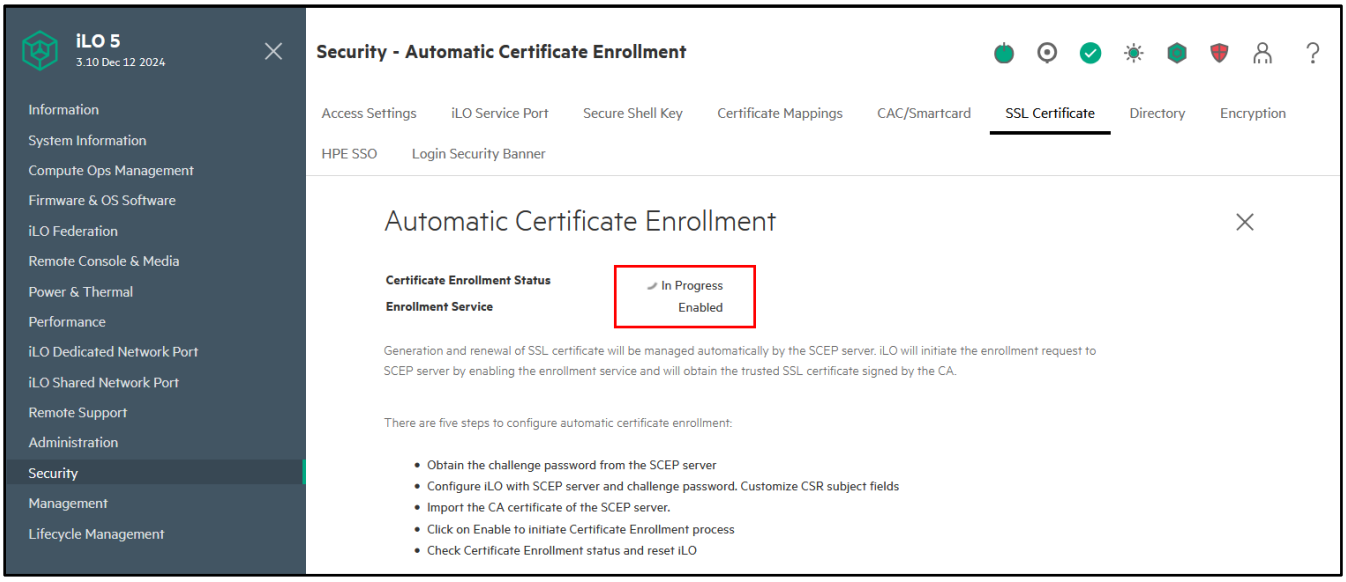


11. Then enter:
    1. Server URL: **https://holca01.hol.enablement.local/certsrv/mscep/mscep.dll**
    2. Challenge password: **type** the enrollment challenge password recorded earlier
    3. In the CA Certificate section, **paste** the content of the certificate you copied earlier from **Notepad**.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

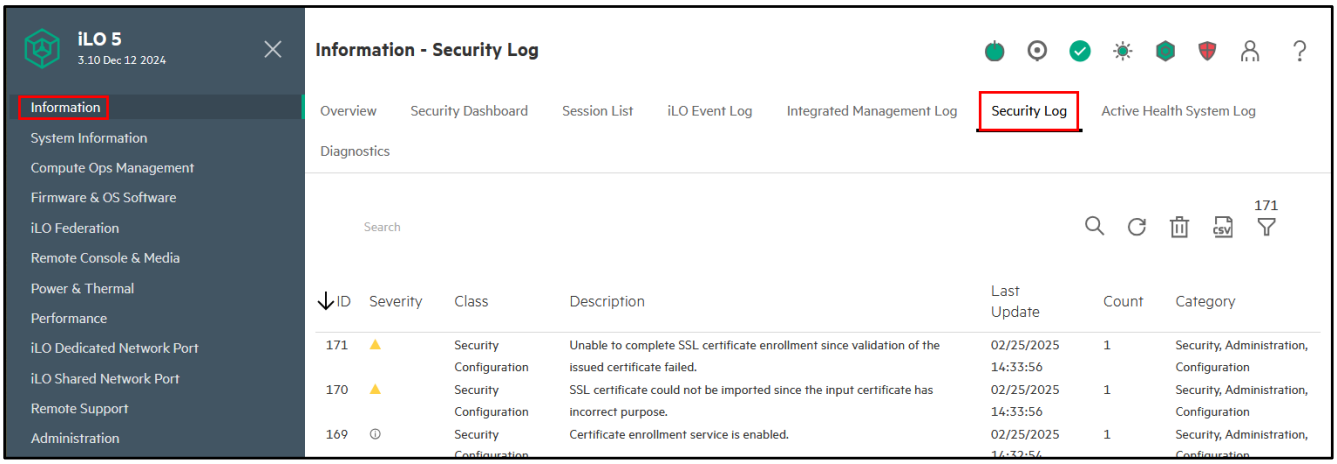


12. Then click **Enable**.

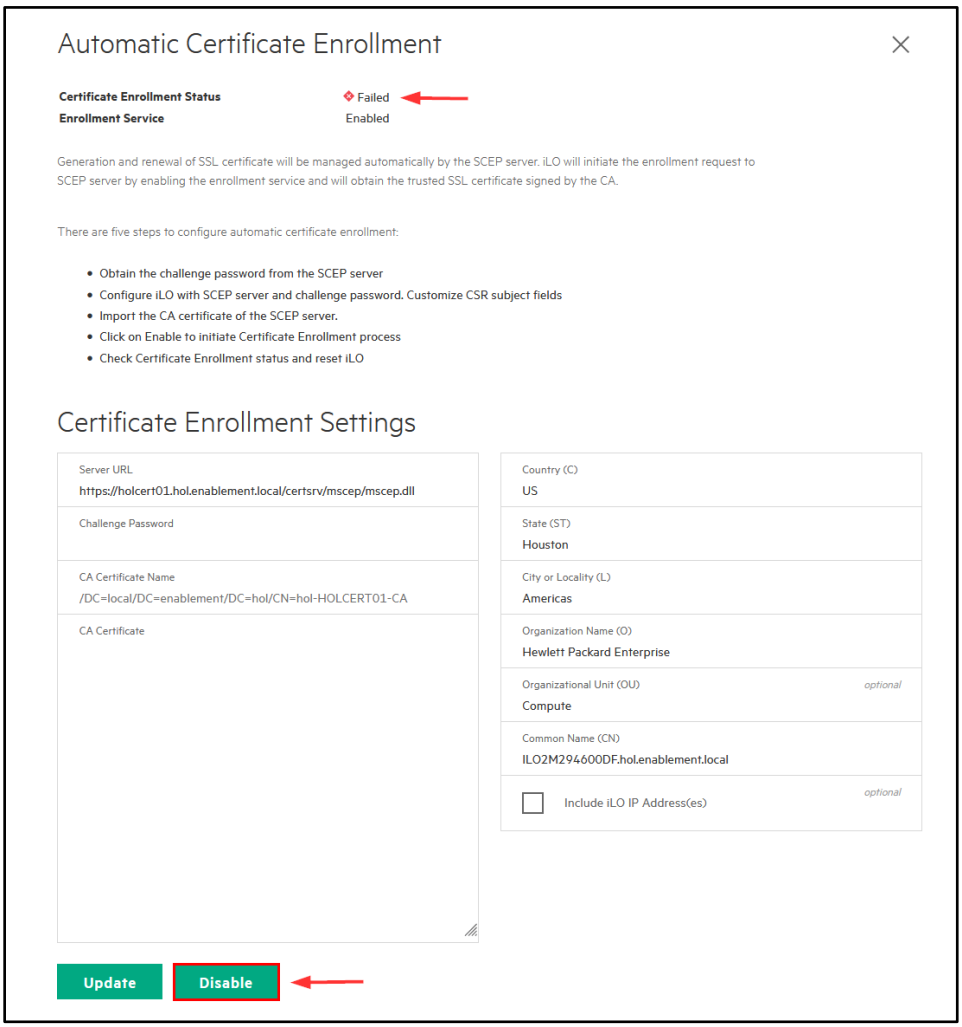
13. To see the progress of the certificate enrollment status, refresh the page by clicking on the **SSL certificate** tab**.**



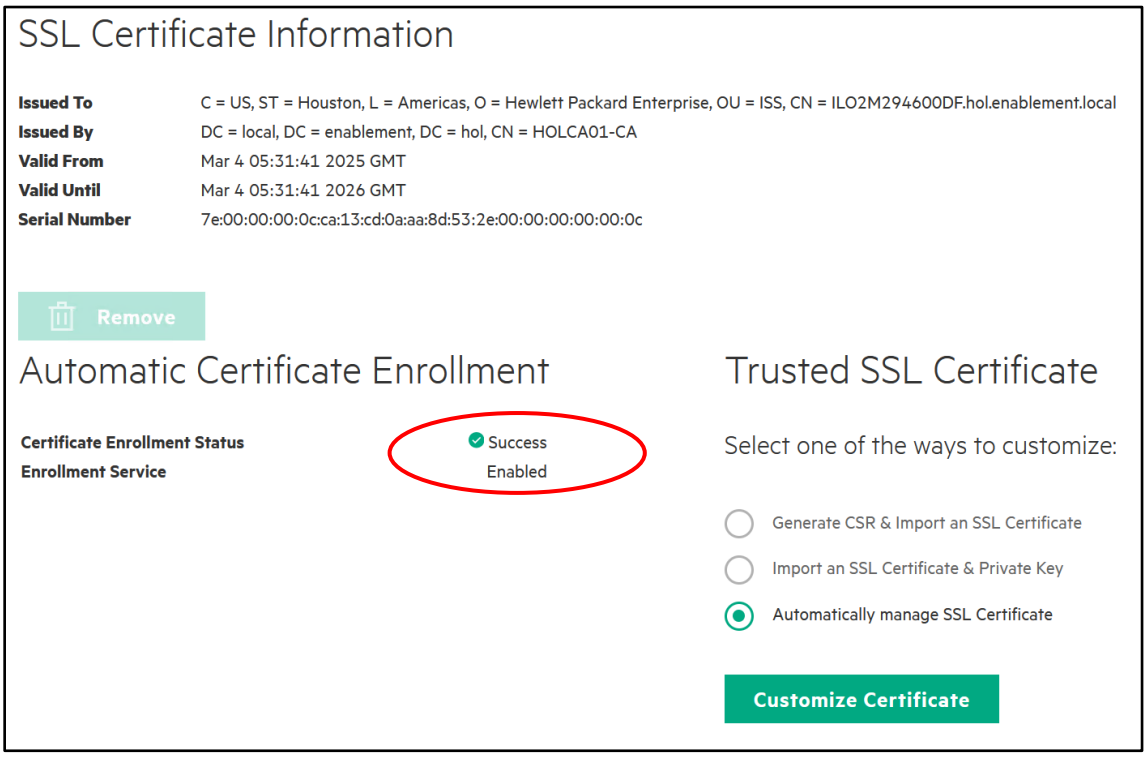
14. If you get a **Failed** status, you can check the iLO Security logs in **Information** / **Security Log**. This is where SCEP activity is generated.



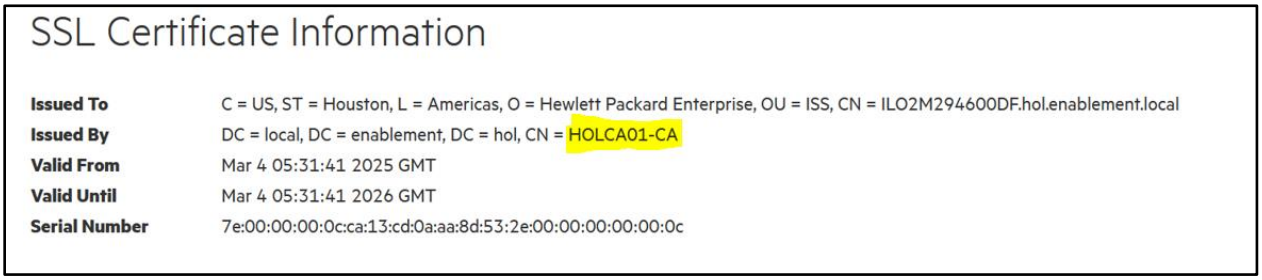
Note: If you face an enrollment failure, it is necessary to disable the certificate enrollment process by clicking on **Disable** before attempting a new enrollment.



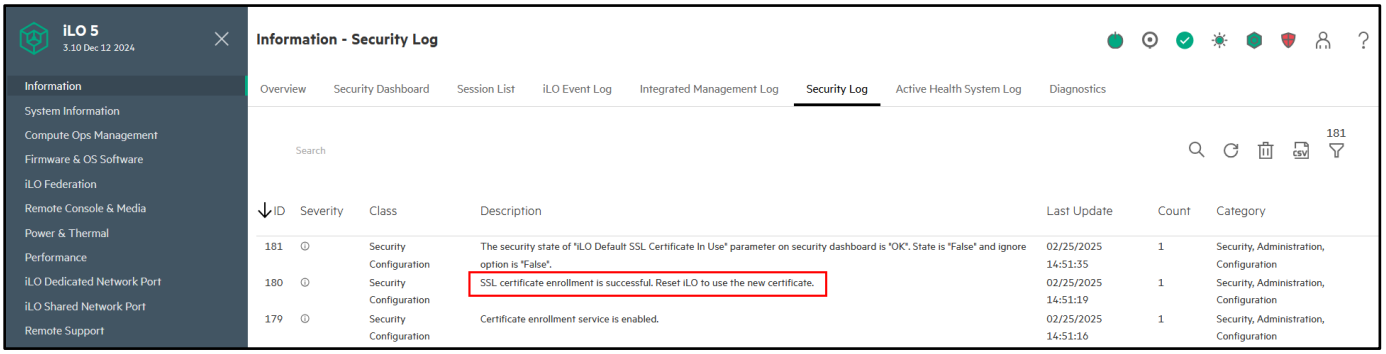
15. A successful Certificate Enrollment will show as:



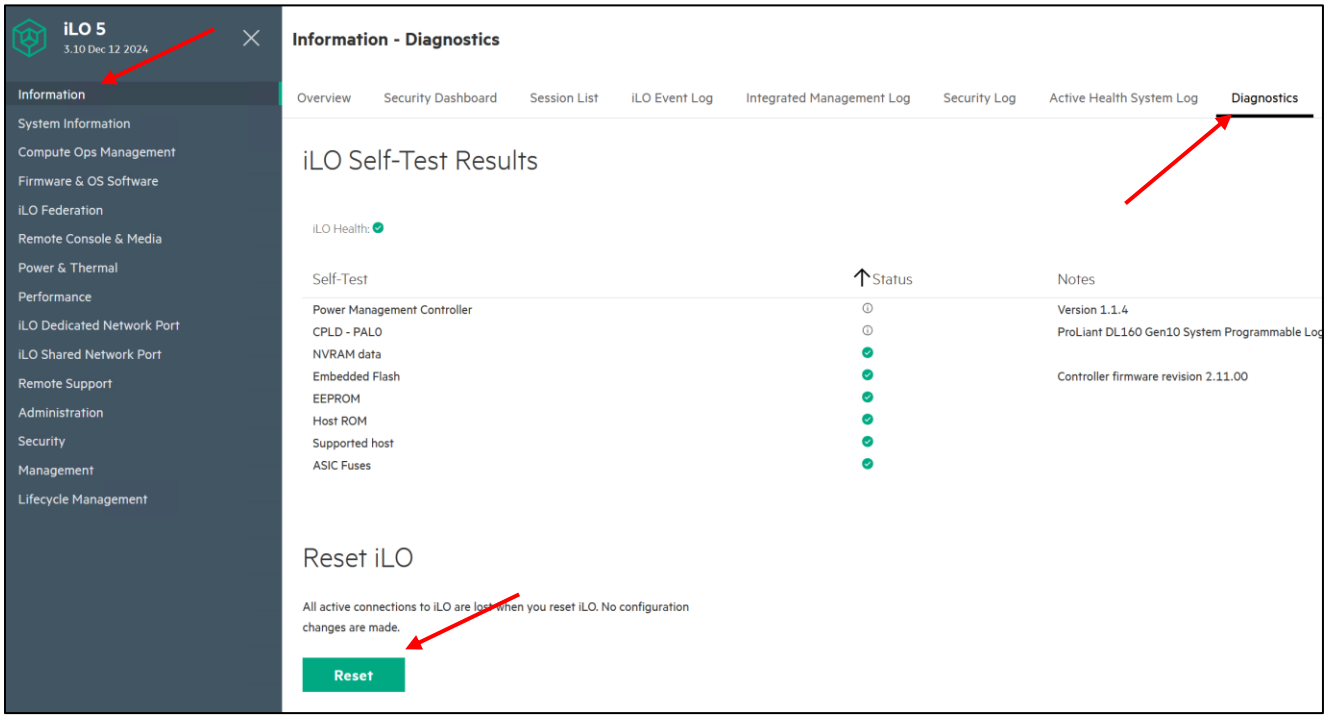
16. Note that now the **iLO** uses a **trusted SSL certificate signed** by our **certificate authority server**:



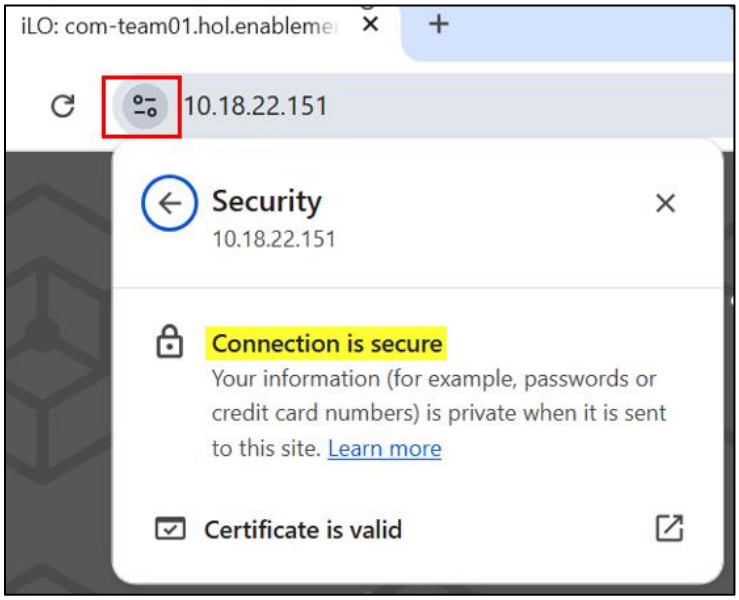
17. But as indicated in the **security logs**, the iLO must be **reset** in order to **activate the new certificate.**



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

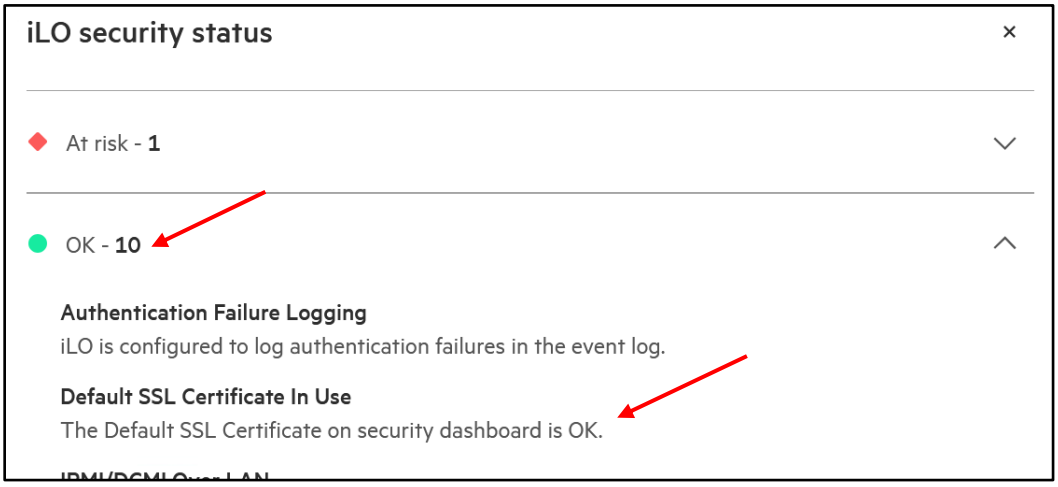


19. Give the iLO a **few minutes to reset**, then **open a new tab or browser** to login and confirm that the **connection** is now recognized as **secure** by the browser.



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.**



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.

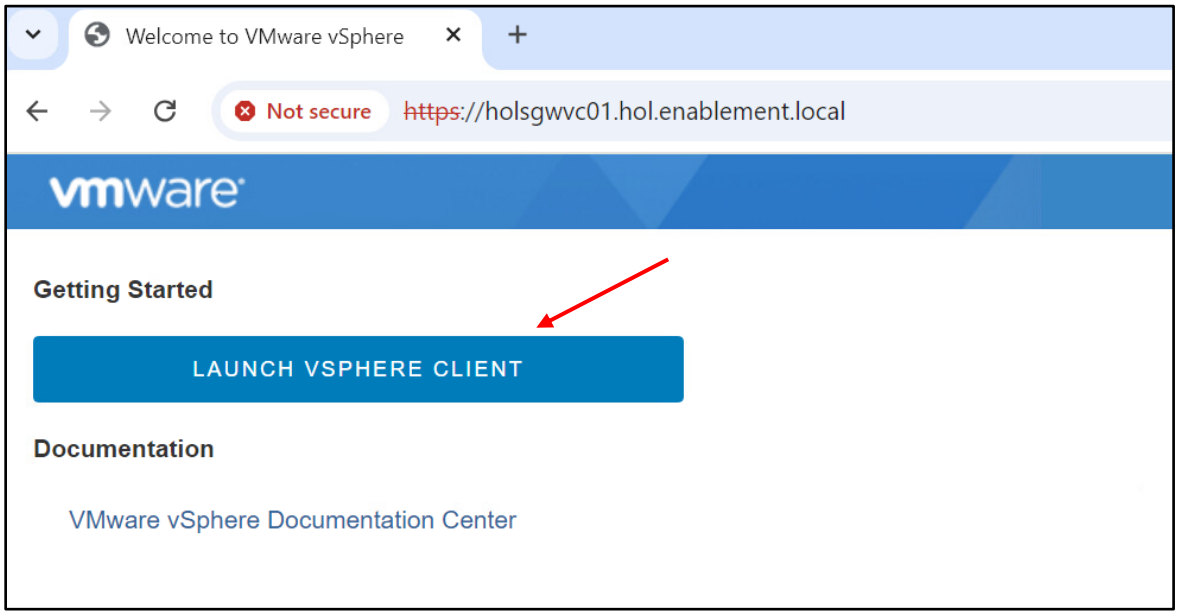
It can aggregate HPE iLO connections from the customer data center over an outbound connection to Compute Ops Management. The feature helps eliminate the need to have each HPE iLO individually connected over the internet to Compute Ops Management.

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.

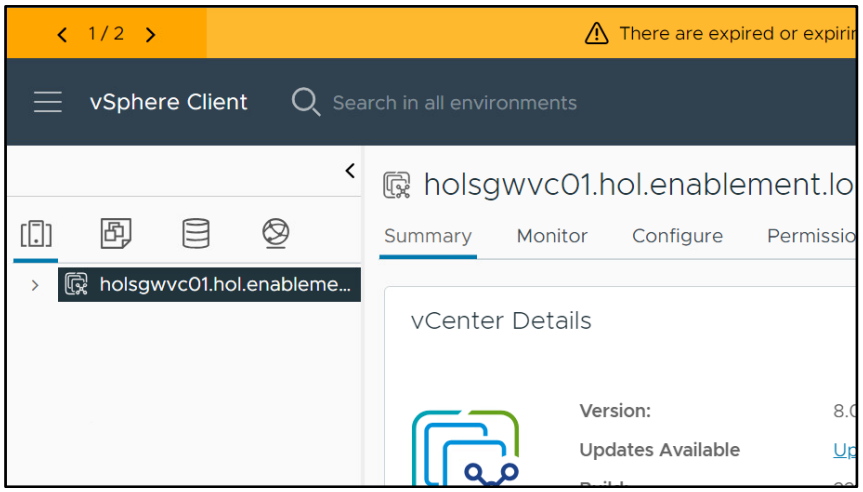
1. Open a fresh **Web Browser** or **Tab** and navigate to your VCenter Server at **holsgwvc01.hol.enablement.local**

2. **Confirm any Certificate Issues** to Proceed and then click **Launch vSphere Client**.

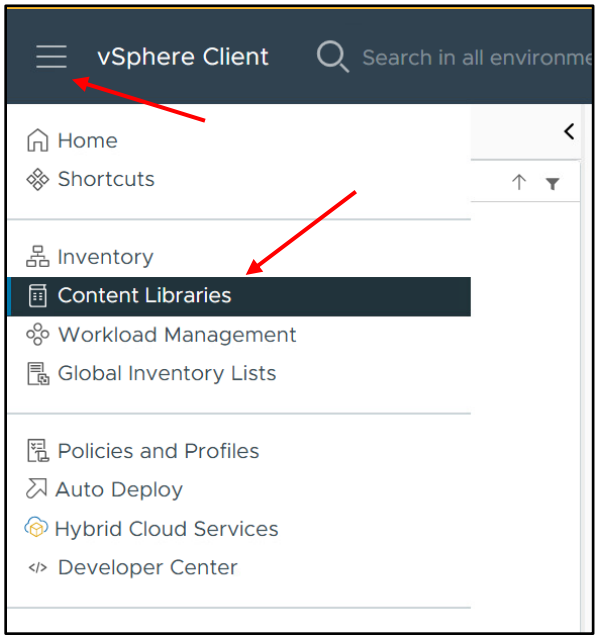


3. Use credentials **Administrator@vsphere.local** and **TechPr02025!** as the password.

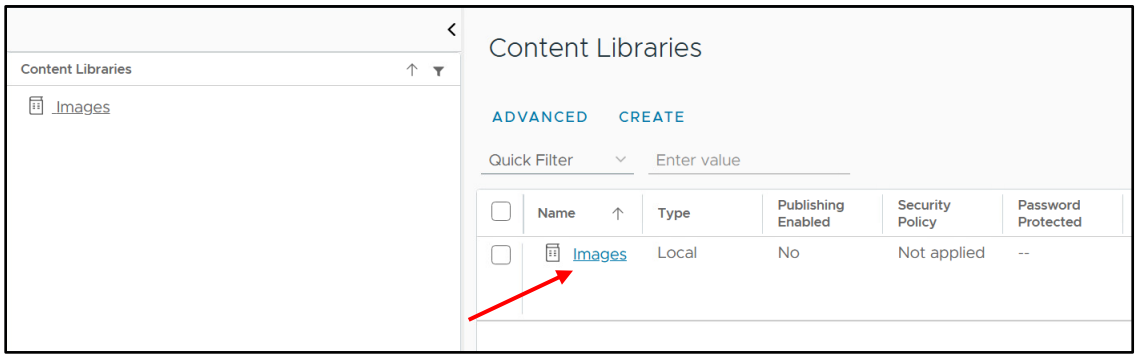
4. You should be now logged in to the vSphere Client



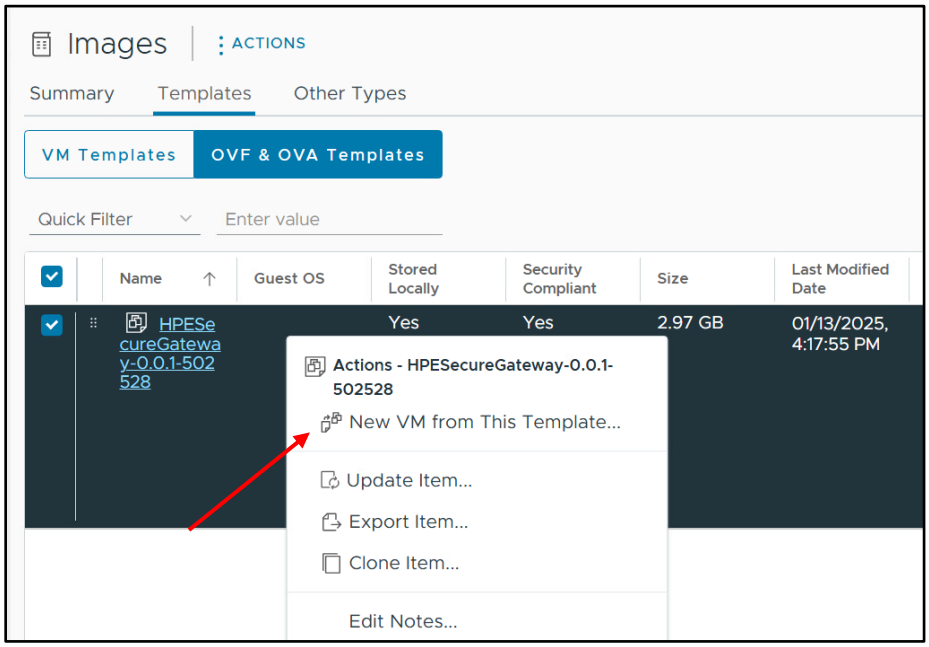
5. On the **left-hand side** of the screen, expand out the **vSphere Client menu**, and click on **Content Libraries.**



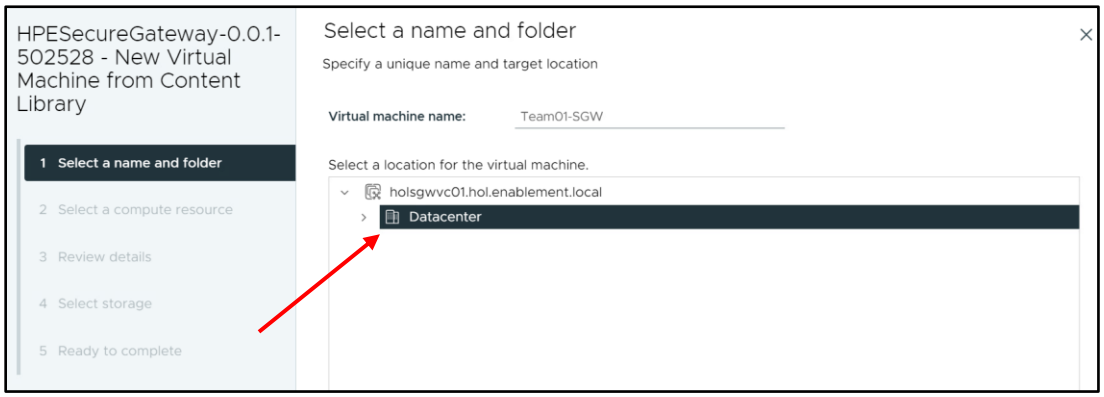
6. Click on **Images.**



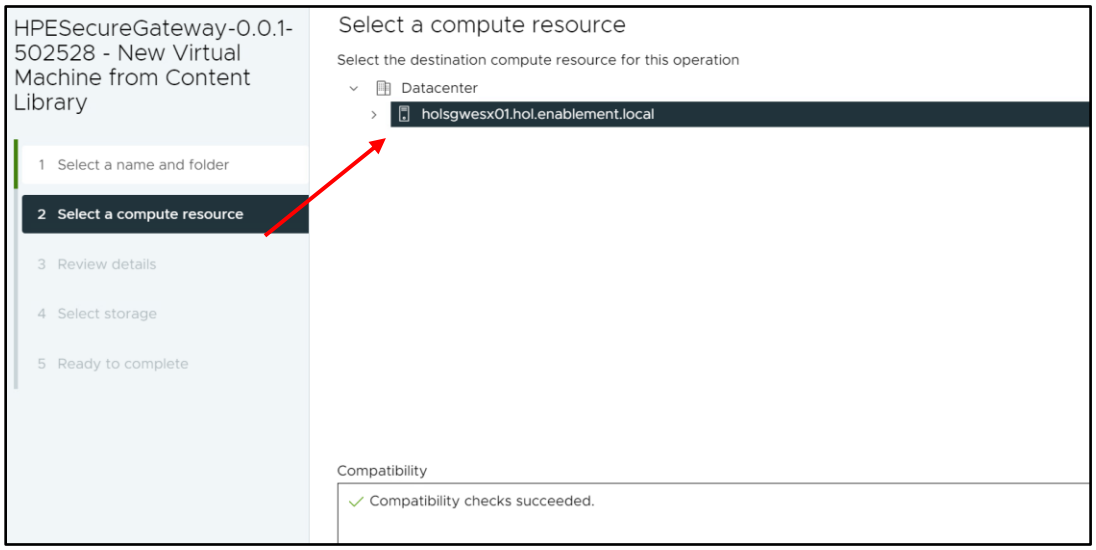
7. Right click on the **HPESecureGateway-X.X.X file** and select **New VM from This Template…**



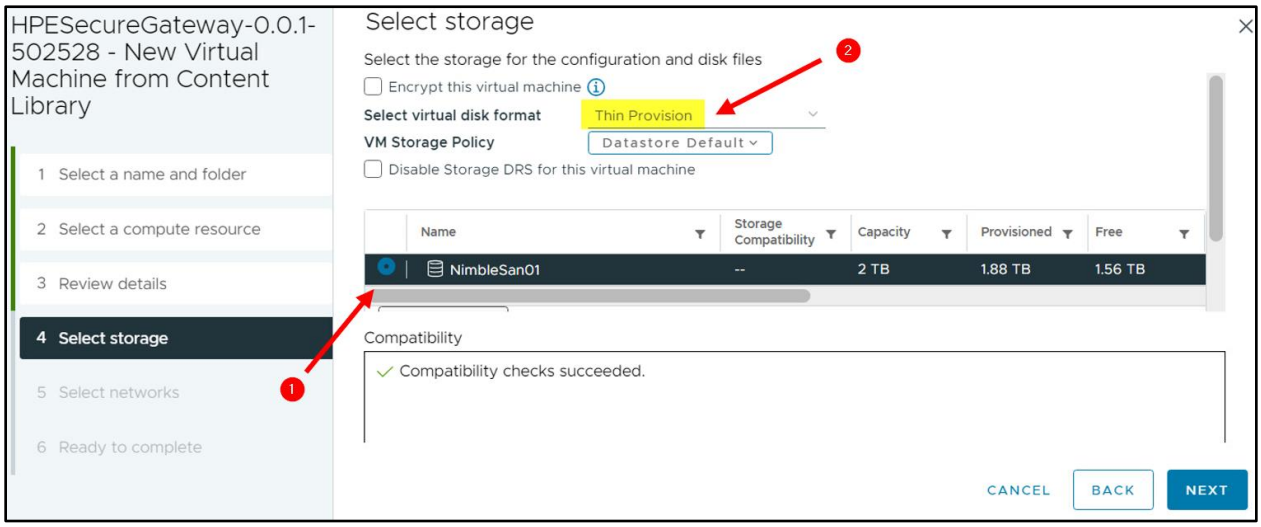
8. Set the Virtual Machine name as **TeamXX-SGW** where **XX** is your team number and select **Datacenter** as the location for the VM.



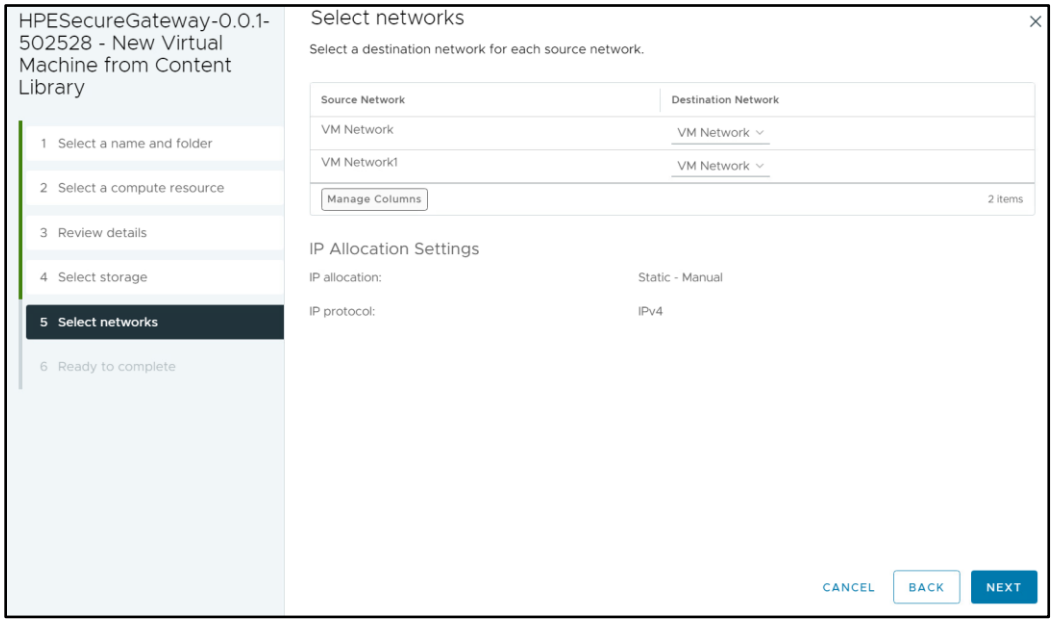
9. Click **holsgwesx01.hol.enablement.local** as the compute resource, then **Next** to proceed.



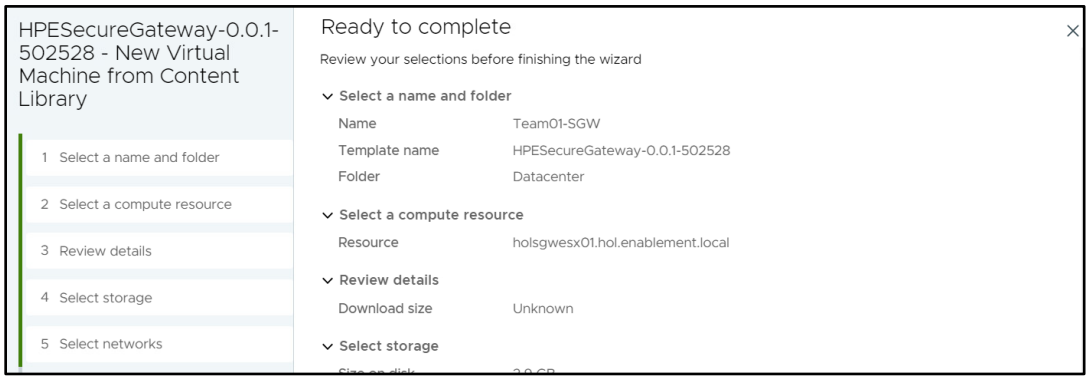
10. Click **Next** on **Review Details** and then for **Select Storage**, click **NimbleSan01**, change **Select virtual disk format** to **Thin Provision** and hit **Next.**

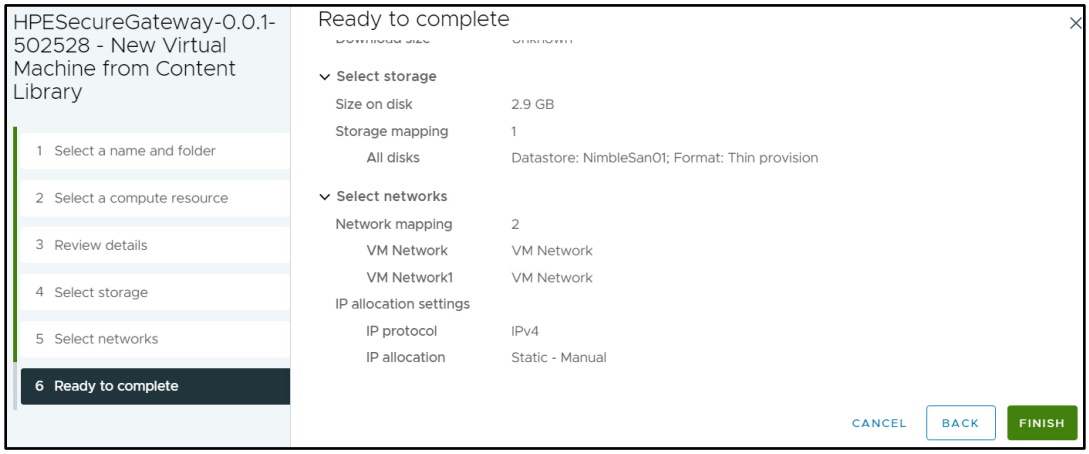


11. Leave the **defaults selected** for **Select Networks** and then **hit Next**.

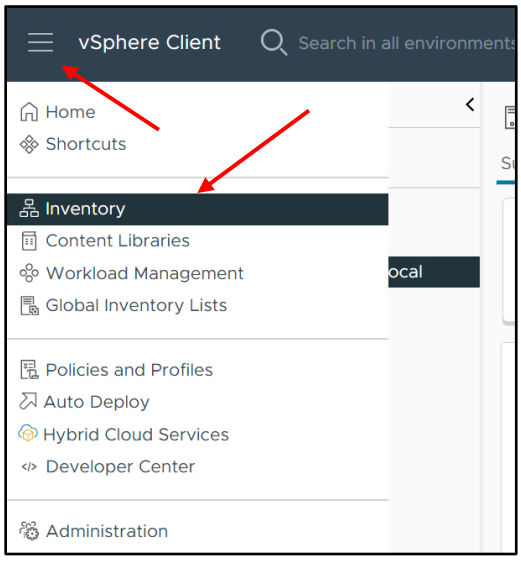


12. One last check and then hit **Finish** to complete the deployment.

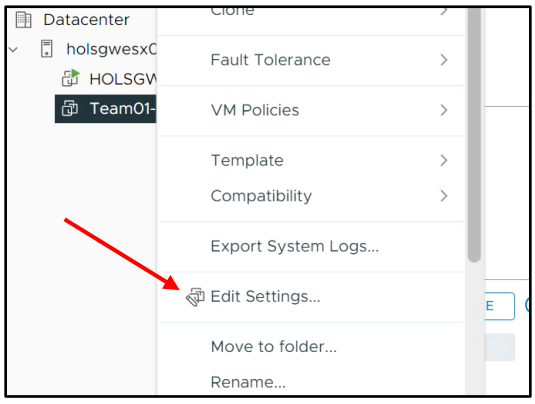




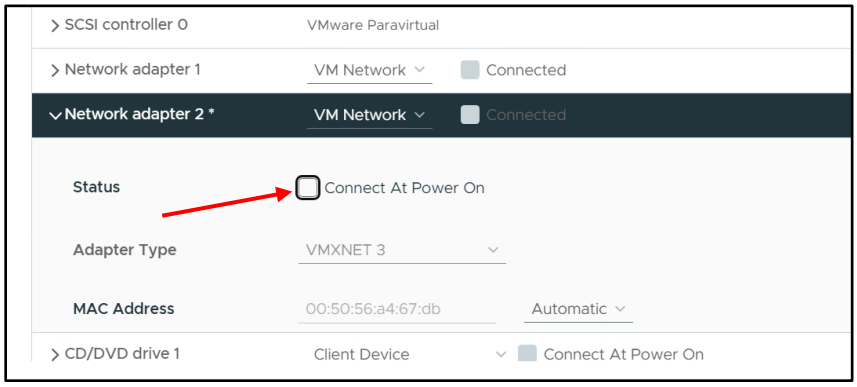
13. You can now navigate back to **Inventory Page** where you will see your **VM has been provisioned**.



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.

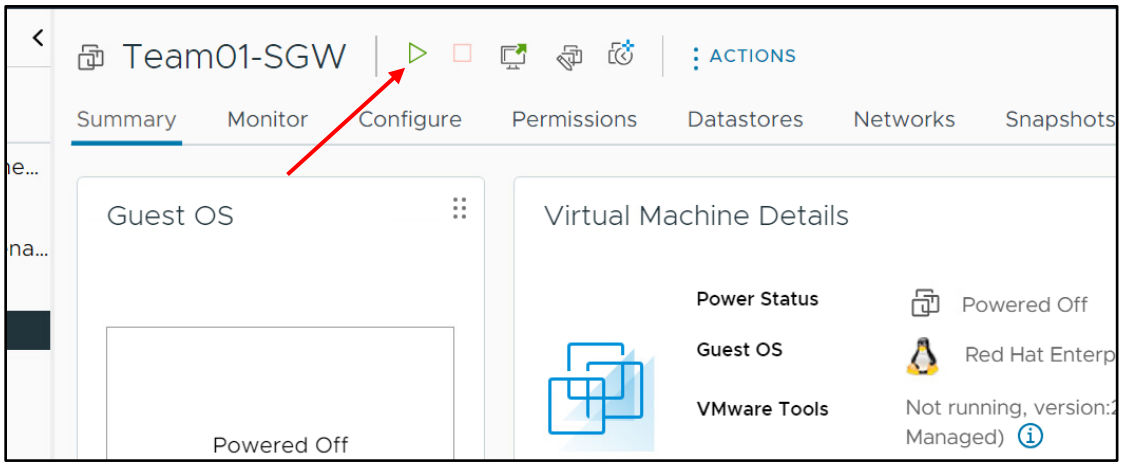


This concludes this section of the lab.

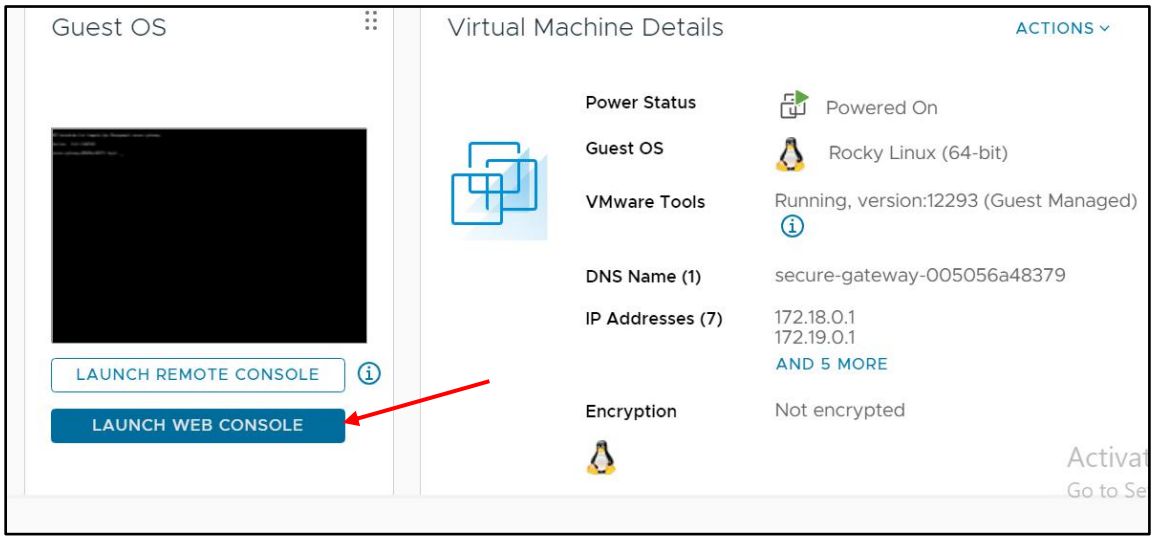
Configuring the Secure Gateway and connecting to COM

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.

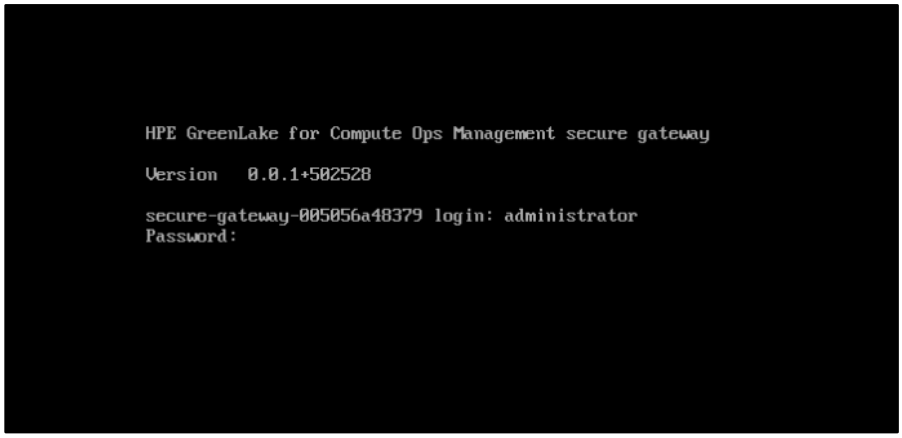
1. There are multiple ways to power on a VM, **click the Green Play button** or any alternative you prefer.



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**.



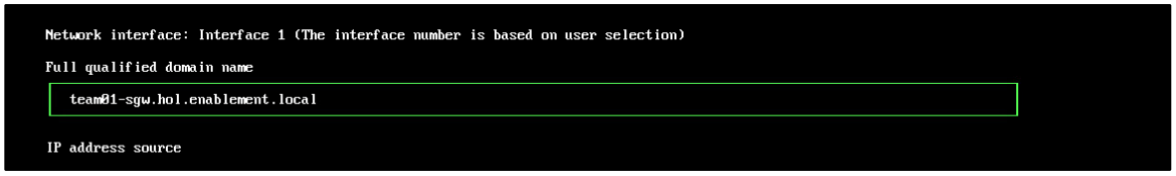
Note: For navigating through the TUI, you will need to use the **TAB** and **Enter** keys.

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.**

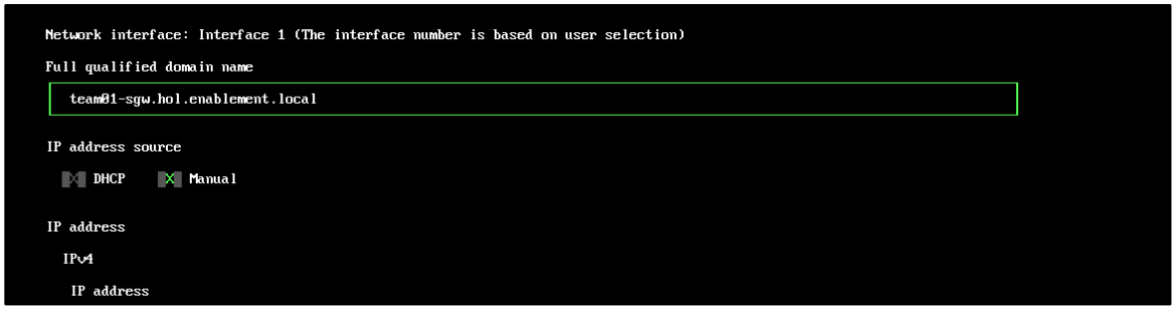
6. Hit **Next** on **Step 1 of 5**, as this is just **informational** regarding our **NIC MAC Address**.

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



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



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

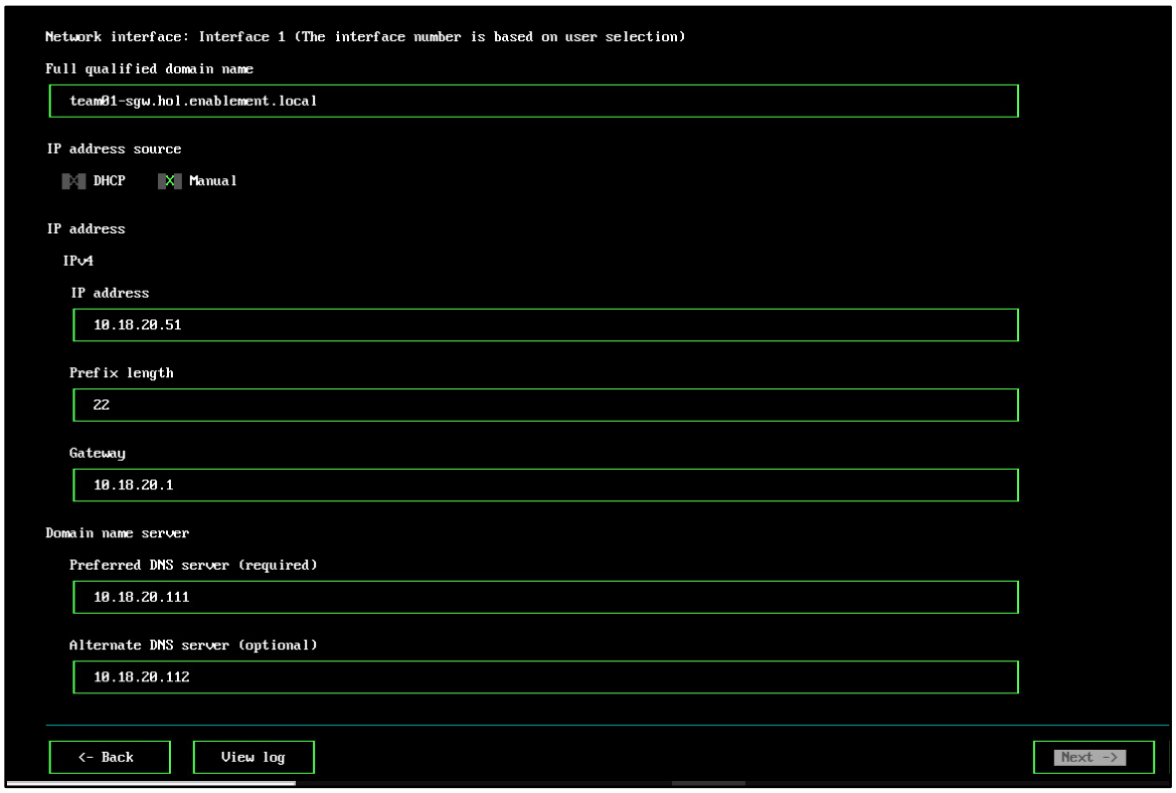
10. For the prefix length, it is **22**.

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**.

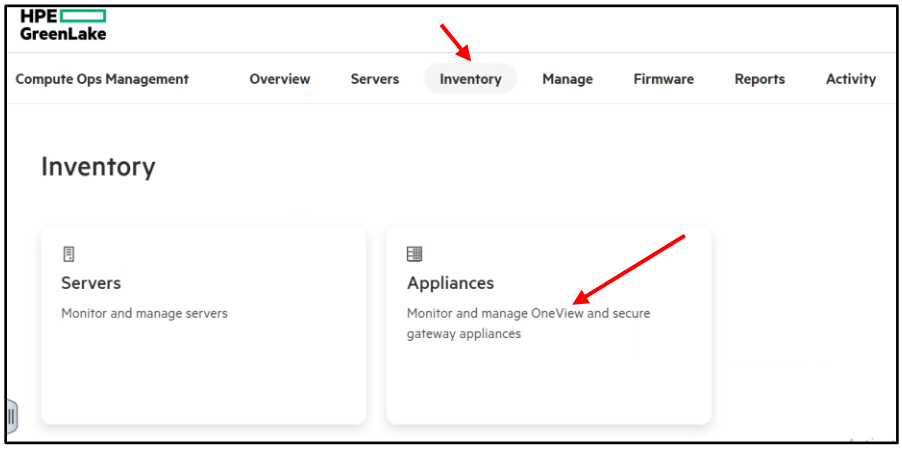
14. Once all entered correctly, select **Next** to proceed.



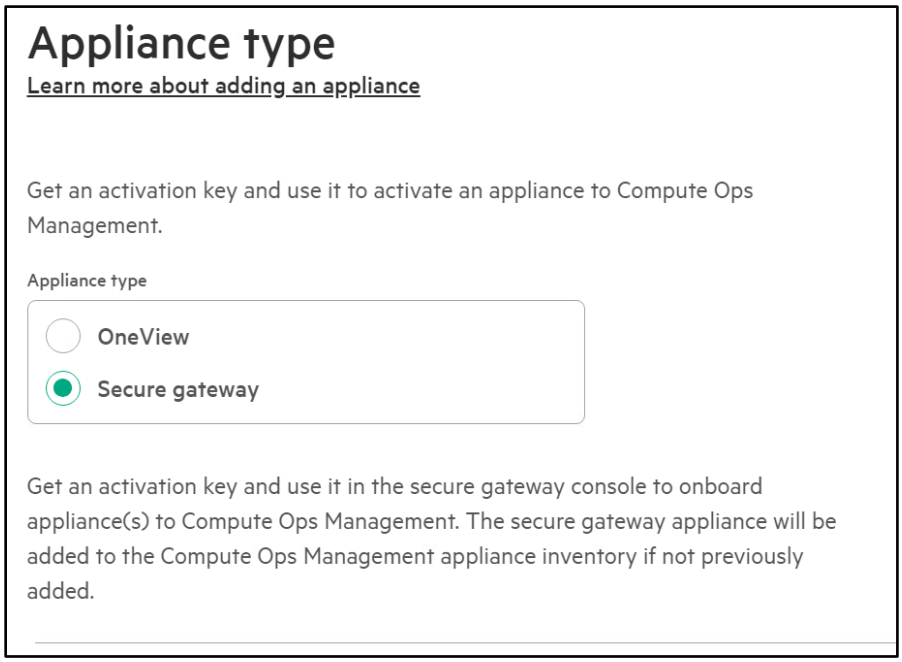
15. Leave the default options for **Time and Web Proxy** configuration.

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

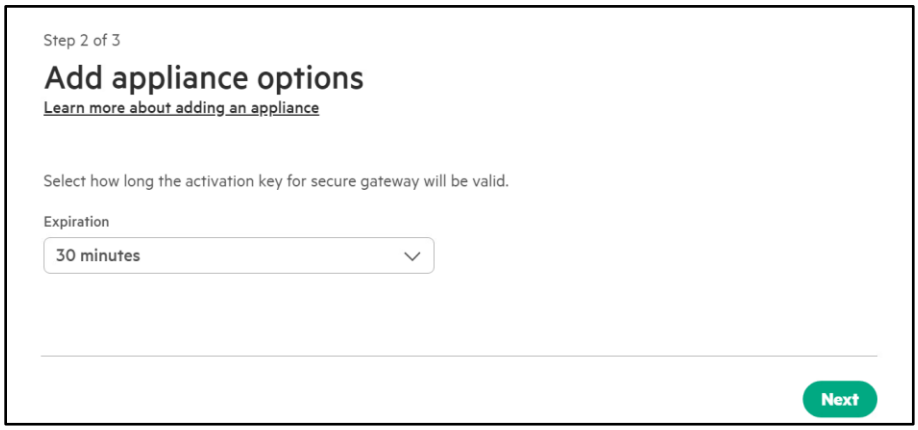
17. From the COM homepage, navigate to **Inventory**, then select **Appliances**.



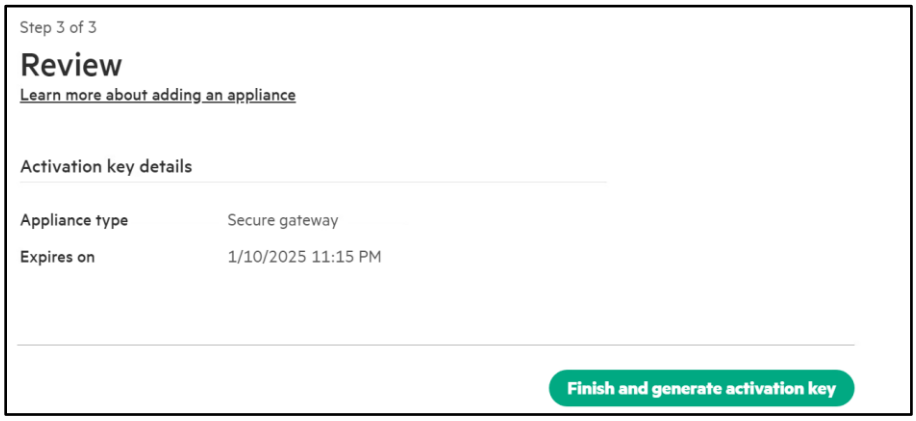
18. Click **Add Appliance**, ensure **Secure gateway** is selected.



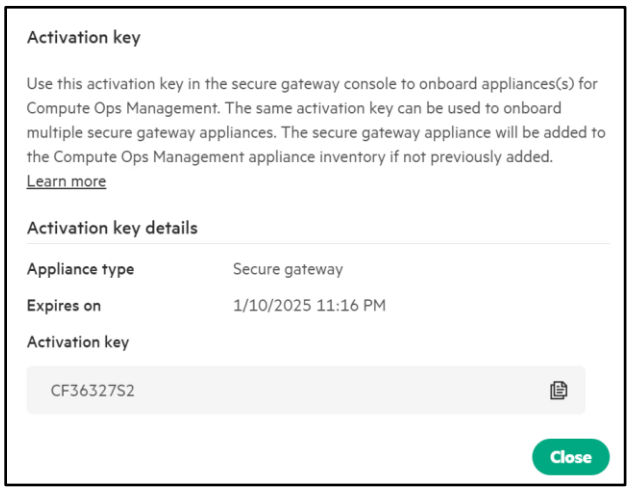
19. Set **30 minutes** for how long the activation key will be valid.



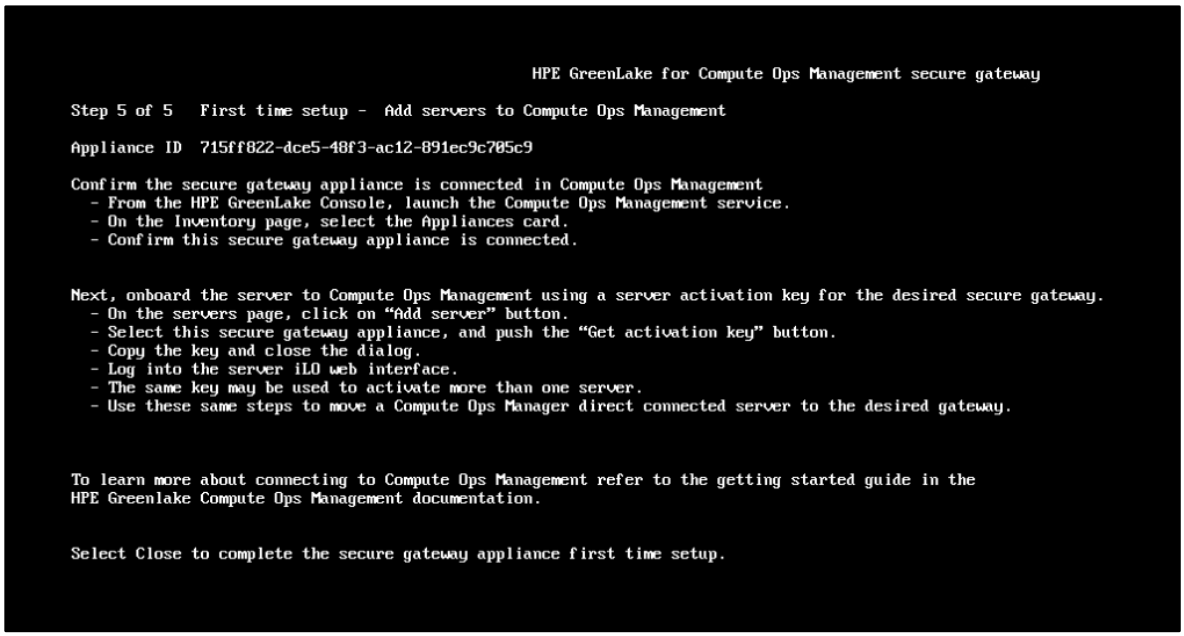
20. Then click **Finish and generate activation key**.



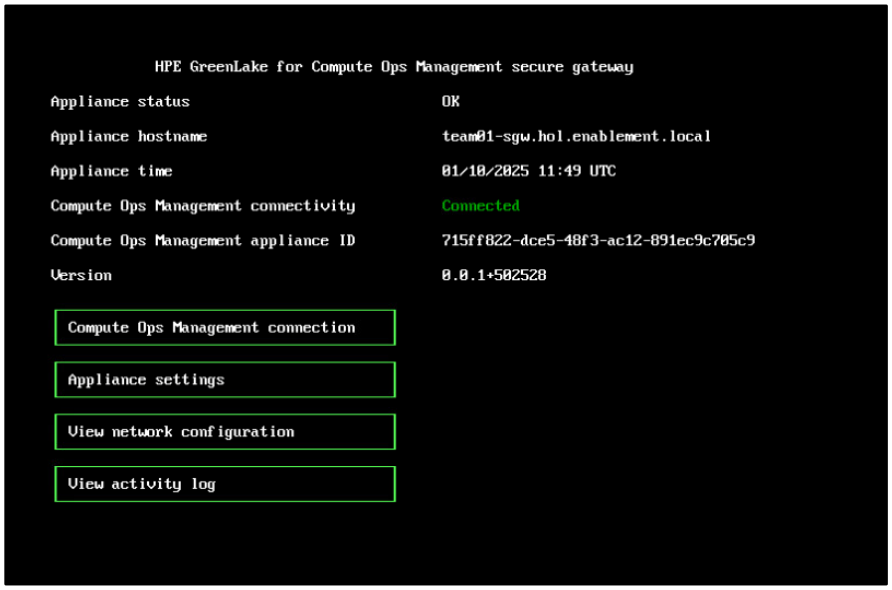
21. Take note of the **Activation Key** and then **type** this into the **TUI for the Secure Gateway Appliance**.

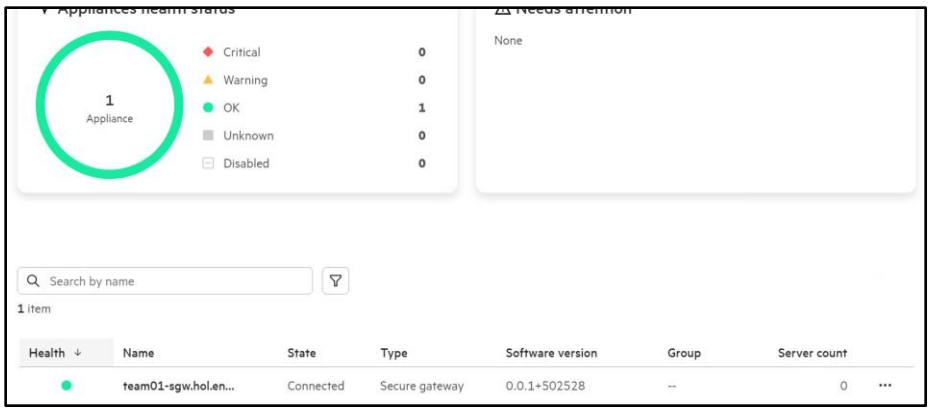


22. The Secure Gateway should now be **connected** and you can **Close** this last **informational** step.



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



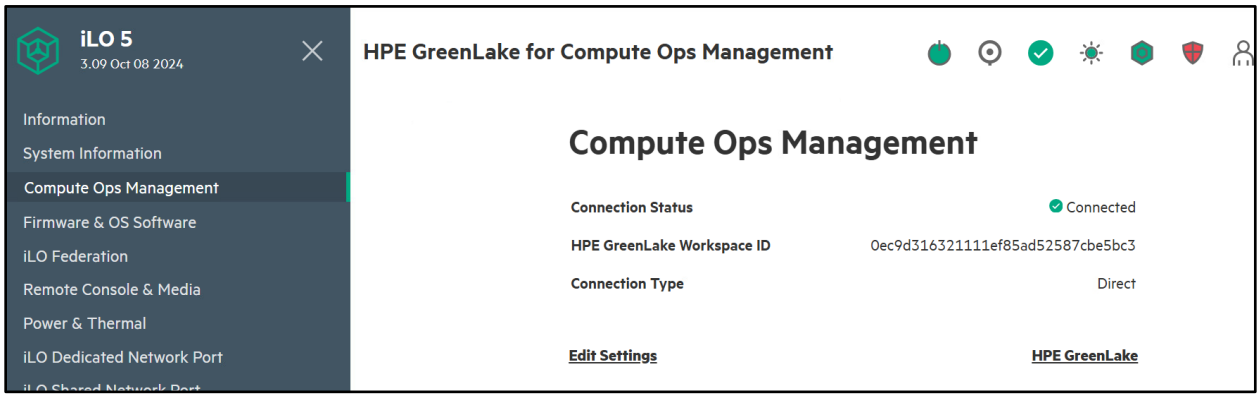


This concludes this section of the lab.

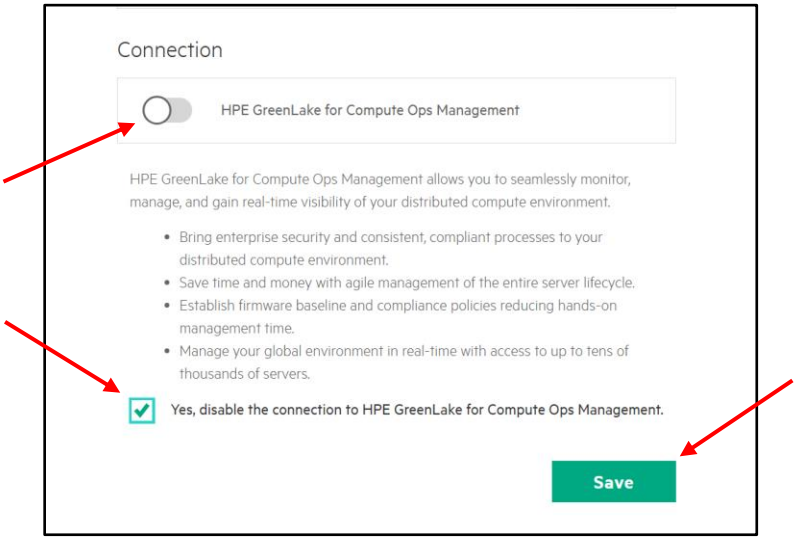
Connecting our HPE iLO to COM via the Secure Gateway

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

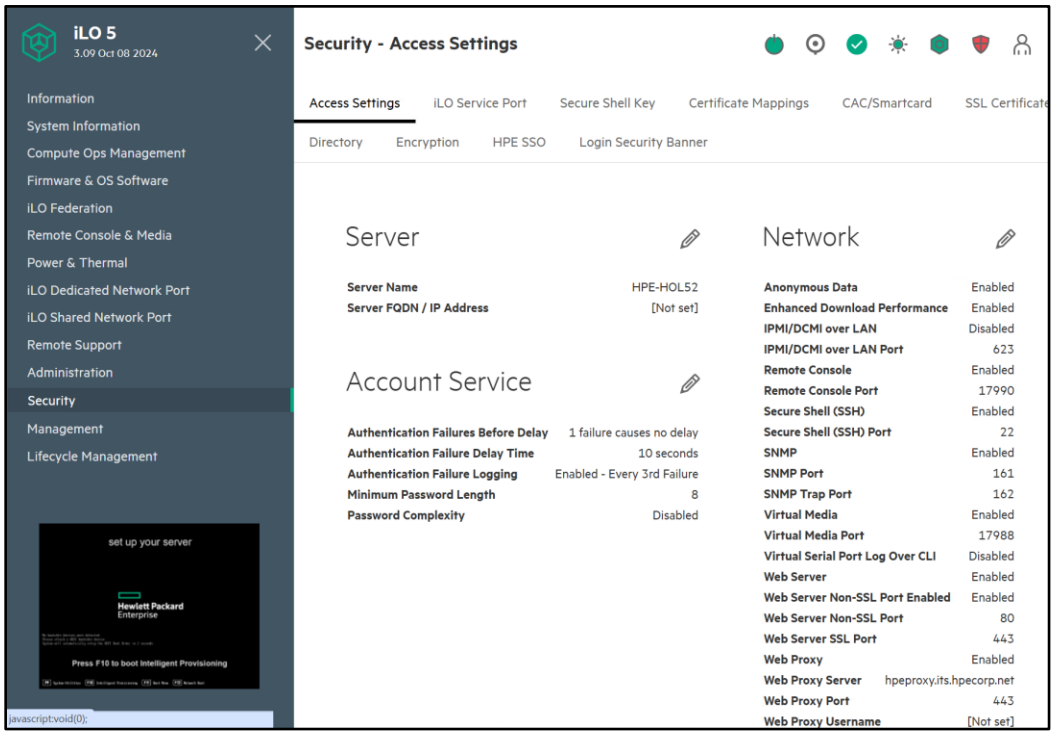
1. Return to the **Web Browser** that's connected to your **HPE iLO** and navigate to **Compute Ops Management** section on the left-hand side.



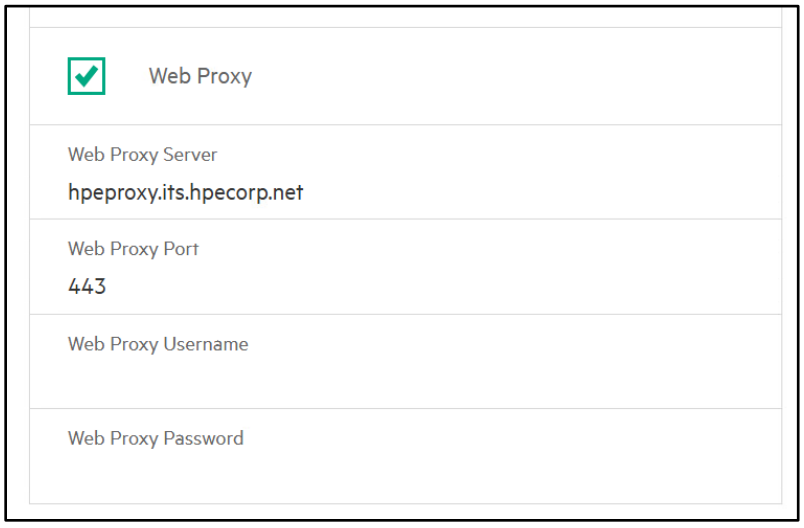
2. From here, click on **Edit Settings**, and **disable** the COM connection then click **Save**.



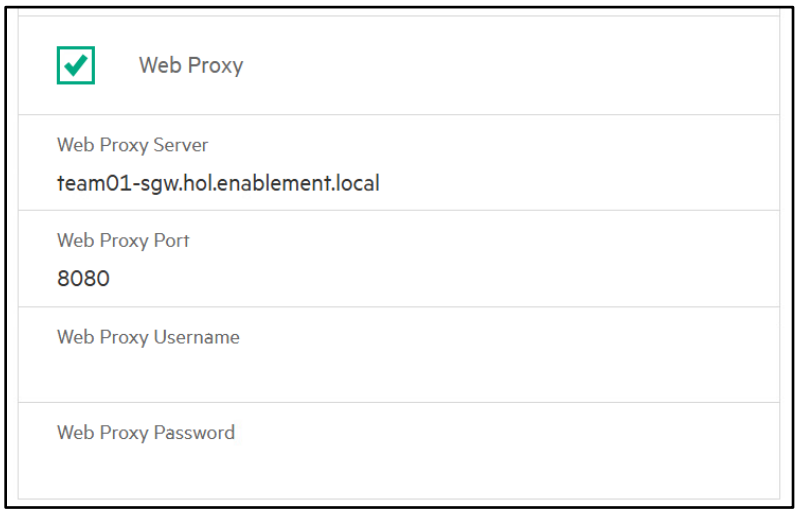
3. Then navigate to the **Security** section to update the **Web Proxy** details.



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



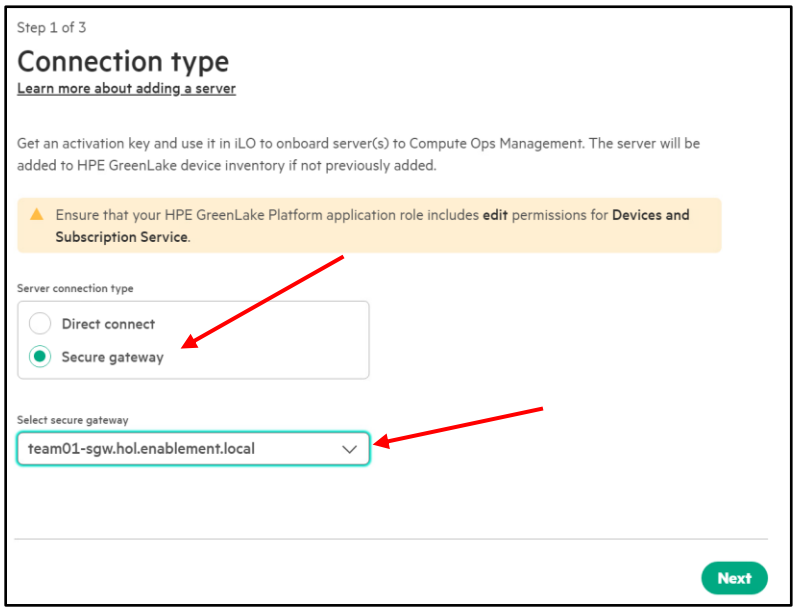
5. Update the **Web Proxy Server** to the FQDN of your newly created Secure Gateway Appliance. Refer back to your assigned FQDN to know what to enter here. For this example, we will use "Team01". Additionally, set the **Web Proxy Port** to **8080**.



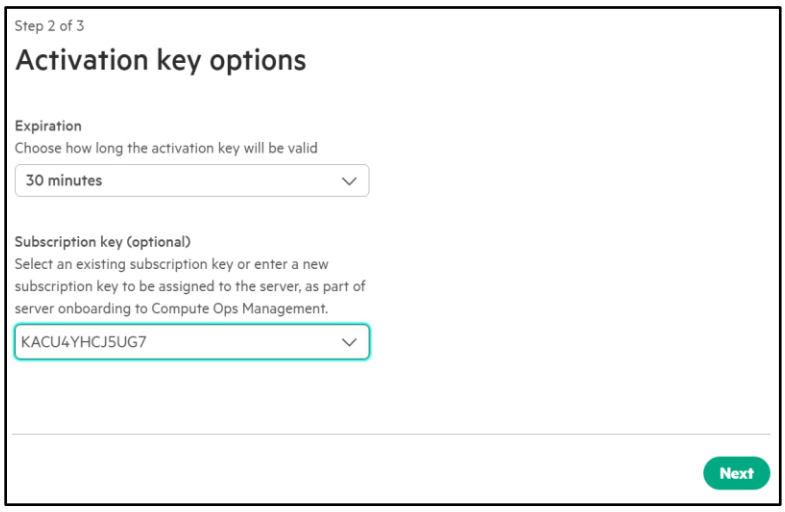
6. Find your **Web Browser** or **Tab** that's **connected to Compute Ops Management** and navigate to **Servers**. You will see your server showing it as **Reconnecting** or **Not Connected** depending on how fast you are.

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

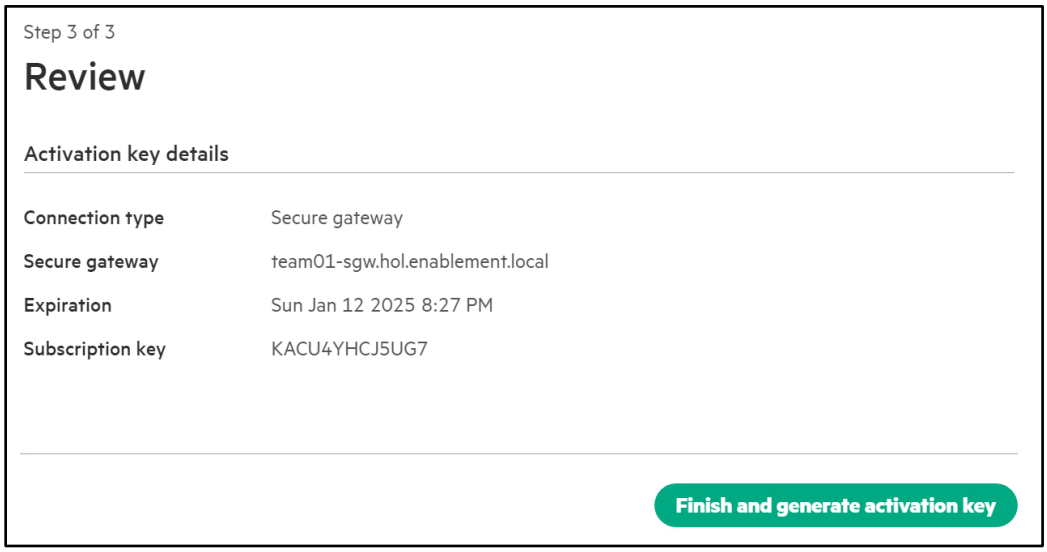
8. Change the **Server connection type** to **Secure gateway** and select your **assigned** secure gateway from the **drop-down menu**.



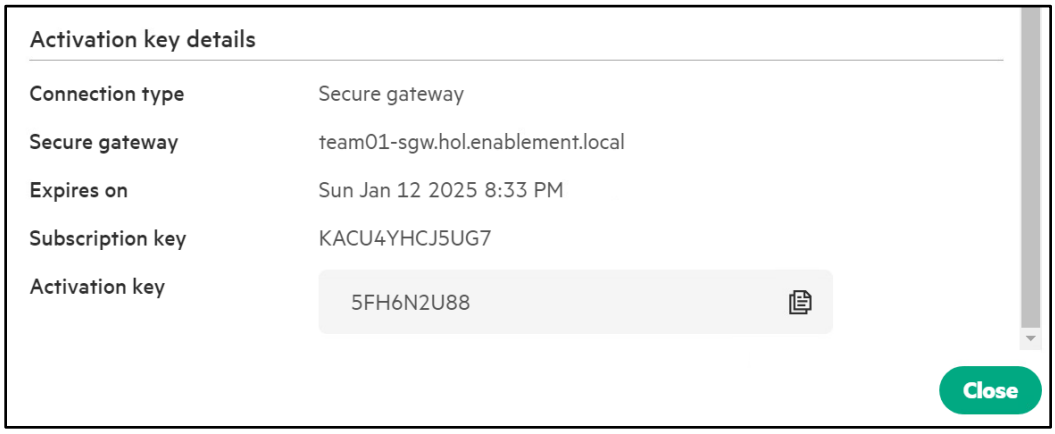
9. Change the Expiration to **30 minutes** and select an available **Subscription Key**.



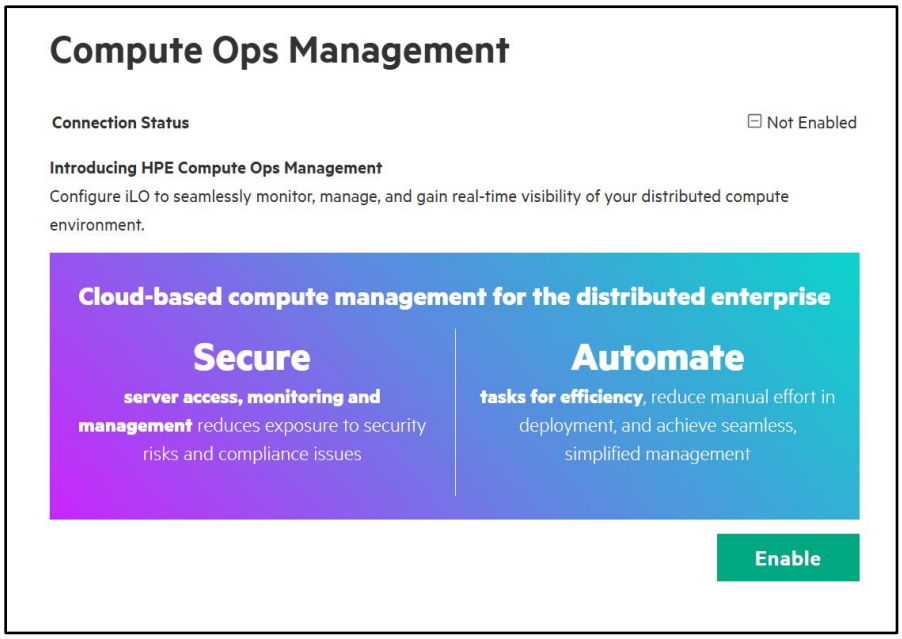
10. Review your Activation Key Details, then hit **Finish and generate activation key**.



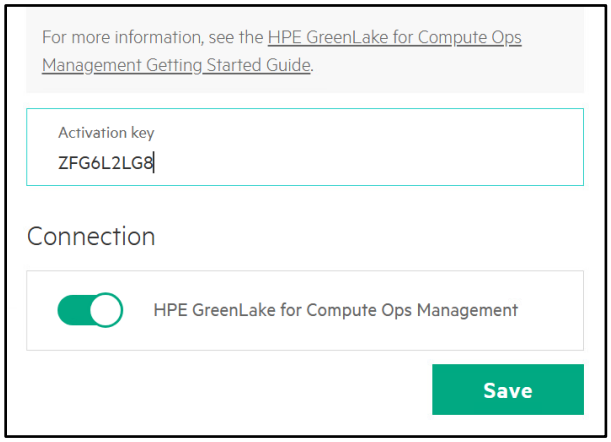
11. Take note of or **copy the Activation key**, then close the pop up.



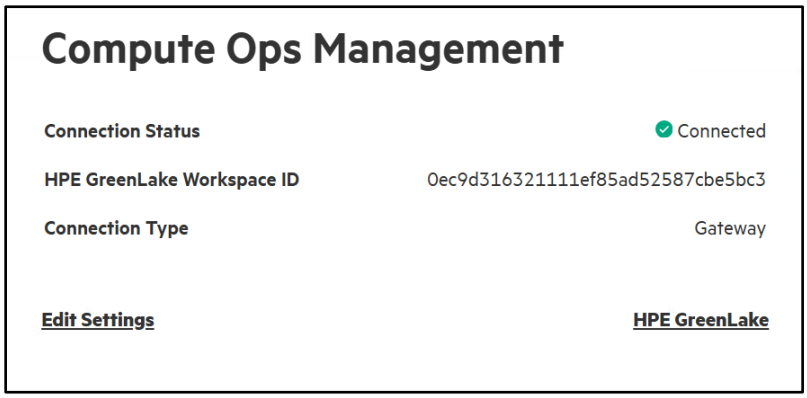
12. Return to your **Web Browser** or **Tab** which is connected to your **Server's HPE iLO**, Click on **Compute Ops Management**.



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

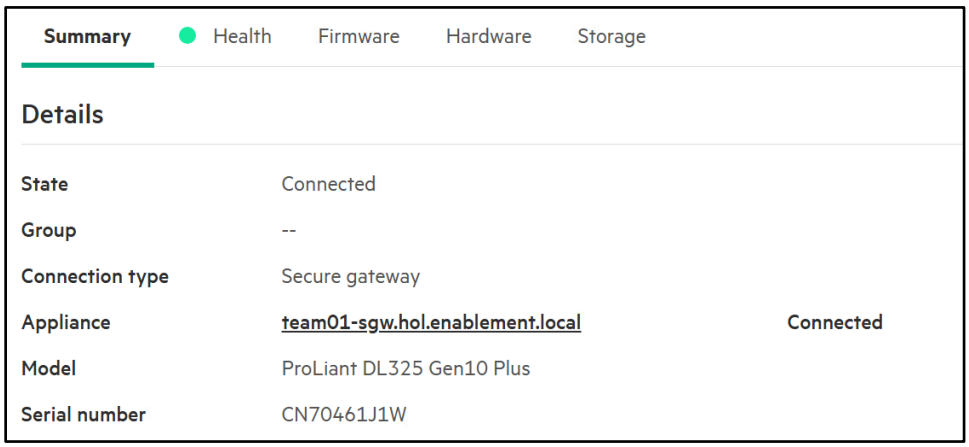


14. Give it a few seconds and it should then return with a Connection Status of **Connected**, your **workspace ID** and **Connection Type Gateway**.

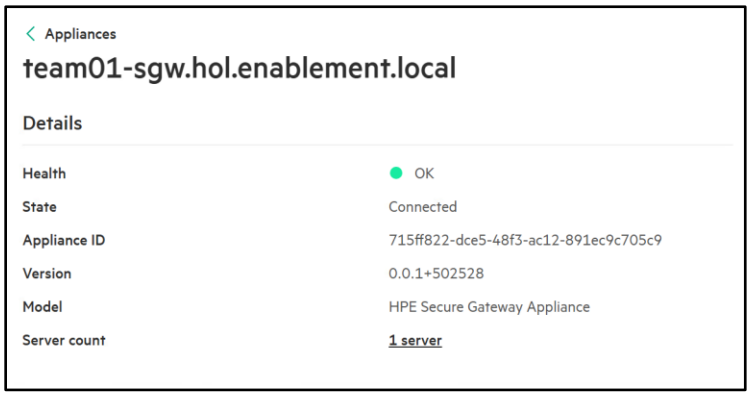


15. If we then navigate back to our Browser or Tab that's connected to COM, we will see our Server now Connected and going through it's inventory process.

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.



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



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