HPE Compute

# HPE GreenLake for Compute Ops Management security guide

HPE GreenLake

# Contents


Executive summary ... 3
Target audience ... 3
Overview ... 4
Be prepared ... 5
- Customer accessible network connections or endpoints ... 5
- Authentication for users ... 7
- Role-based access control for users ... 8

How HPE GreenLake for Compute Ops Management and HPE GreenLake protect you in the cloud ... 10
- Risk assessments ... 10
- Protecting against vulnerabilities ... 10
- Secure architecture ... 10
- API gateway and Amazon CloudFront ... 10
- Customer data stored ... 10
- Data that HPE employees or partners can access ... 11
- Security assurance and compliance ... 11
- Open-source software license statement ... 11
- Data security and privacy statement for HPE GreenLake and Compute Ops Management ... 11


## Executive summary

Hewlett Packard Enterprise is transforming compute management with a modern experience that delivers greater simplicity, agility, and performance. HPE GreenLake for Compute Ops Management is a secure and scalable cloud-based application that delivers unified compute operations as a service from edge to cloud. It simplifies how customers manage infrastructure across the lifecycle — from simplified health status to automated firmware management across a fleet of servers. Available through HPE GreenLake platform, Compute Ops Management is built on a cloud-native architecture that transforms complex compute operations into a simplified experience from edge to cloud.

This paper describes how HPE GreenLake for Compute Ops Management enforces all aspects of user and data security. After reading this paper, you will have a better understanding of the security features of HPE GreenLake for Compute Ops Management.

HPE GreenLake for Compute Ops Management was built with a vision of security in mind, focusing on three key requirements:

- Trusted HPE GreenLake for Compute Ops Management in the cloud and HPE iLO management processor embedded in the server
  - Both offerings have HPE CA certificates that are used to verify each other's authenticity.
- Data encryption in the cloud
  - All customer data in HPE GreenLake for Compute Ops Management is encrypted using AES-256.
- Multi-tenant isolation for safety
  - The data of each HPE GreenLake for Compute Ops Management customer is logically separated from that of other tenant companies, providing privacy and data access protection.

**Important**
The HPE iLO management processor embedded in the server communicates with HPE GreenLake for Compute Ops Management. The server OS or any customer-installed applications do not communicate with or send any data to HPE GreenLake for Compute Ops Management.

HPE also offers industry-leading service capabilities that provide enterprise-level security support for establishing secure data and controlled access.

## Target audience

The target audience for this document are HPE GreenLake for Compute Ops Management customers. The customer roles include corporate security personnel, risk management personnel, and server administrative personnel, who will be working with HPE GreenLake for Compute Ops Management.

You should be familiar with computer concepts associated with management, networking, security, and HPE servers, as well as with the needs and requirements of your organization and its infrastructure.

**Table 1.** Terminology

| Term | Explanation |
|---|---|
| **COM** | Compute Ops Management |
| **CVE** | Common Vulnerabilities and Exposures are a list of records of cybersecurity vulnerabilities. The website cve.mitre.org tracks and records the workaround or remediation for any discovered CVE. |
| **DDoS** | A distributed denial-of-service attack is a malicious attempt to disrupt network communication with a cloud service. |
| **HPE iLO** | HPE Integrated Lights-Out. HPE iLO server management software that enables you to securely configure, monitor, and update HPE servers seamlessly, from anywhere in the world. In this document, HPE iLO refers to HPE iLO 5. |
| **HTTPS** | Hyper Text Transfer Protocol Secure provides secure communication for data exchange over computer networks. HTTPS traffic is encrypted through TLS and provides support for authentication via asymmetric key exchanges. |
| **mTLS** | Mutual TLS provides a cryptographic method to establish protected and secure communication tunnel over computer networks so that the server authenticates the client and the client authenticates the server. |
| **RBAC** | Role-based access control associates a unique authority to a specific user to perform allowed action for a particular component. This function allows just enough permission to support the zero trust security model. |

| Term | Explanation |
|---|---|
| **SaaS** | Software as a service is the licensing and delivery model of software on a subscription basis and is centrally hosted. |
| **SAML** | Security Assertion Markup Language provides a protocol to integrate SSO from the customer. |
| **SSO** | Single sign-on is an authentication mechanism that allows a user to log in with a single ID and password to multiple independent systems. SSO organizes multiple users under an organization so that a single authentication can be used for distributed applications. |
| **TLS** | Transport Layer Security protocol provides cryptographic methods to establish protected and secure communication tunnel over computer networks (internet) so that the client recognizes the server. |

## Overview

HPE GreenLake for Compute Ops Management is a secure and scalable cloud-based management platform built on a microservice architecture. It facilitates device onboarding, inventory, health, power control, and firmware management for HPE servers depicted in Figure 1. HPE GreenLake for Compute Ops Management is continuously enhancing and adding new features.

**Note**
HPE GreenLake for Compute Ops Management inherits the cloud security framework enforced by HPE GreenLake.

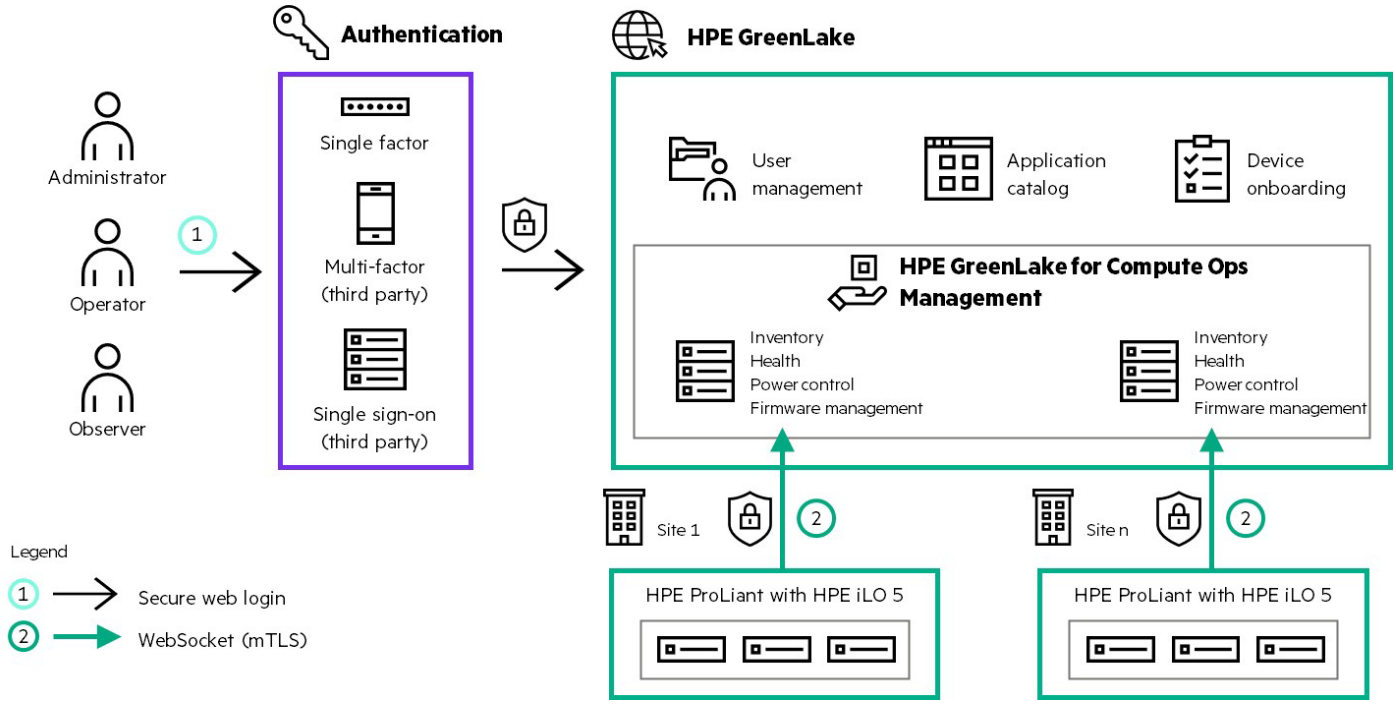


**Figure 1.** HPE GreenLake for Compute Ops Management security representation

Security for this solution is based on a shared responsibilities model applicable to customers and HPE. It considers both customers and host provider premises; the roles of users as the consumers; and HPE as the service providers. Figure 2 illustrates this shared security responsibility model. Customer and server information in the cloud belongs to the customer and HPE secures it acting as the custodian.

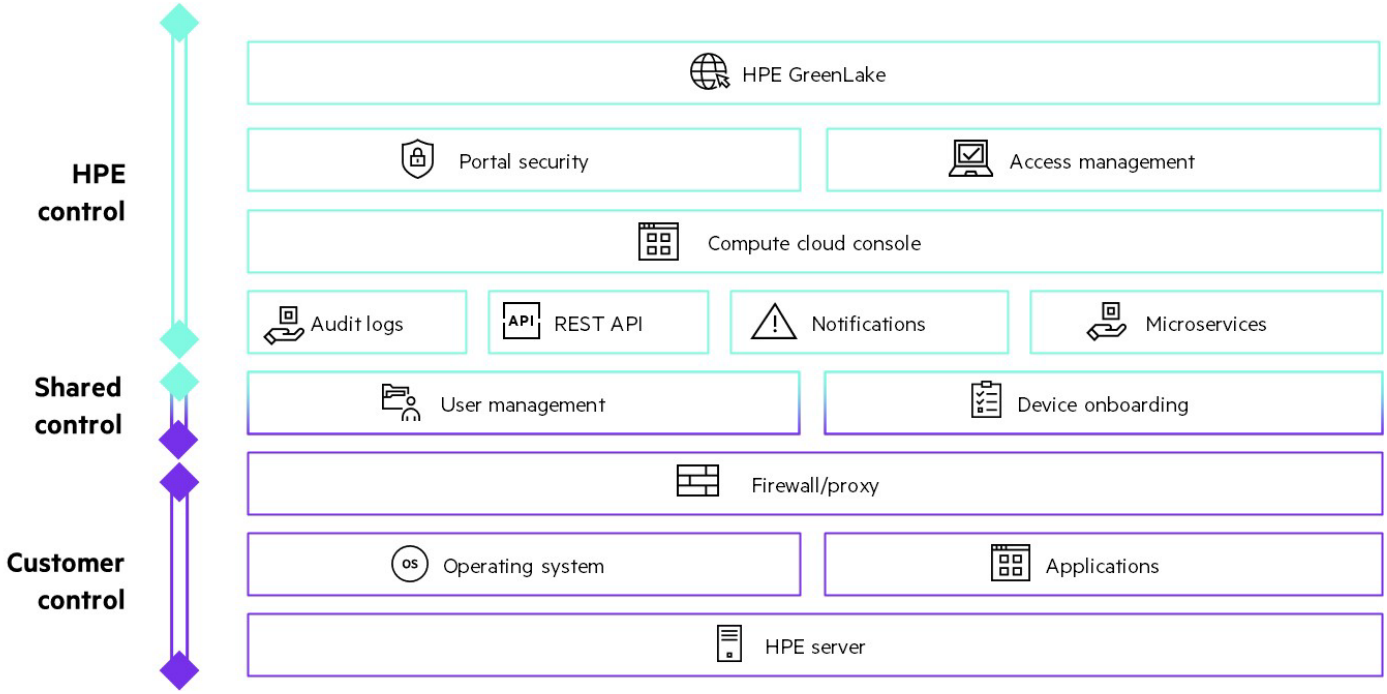


**Figure 2.** Shared security policy model

## Be prepared

HPE GreenLake for Compute Ops Management provides several features that incorporate into customer's cybersecurity processes and plans.

### Customer accessible network connections or endpoints

Customers consume HPE GreenLake for Compute Ops Management services using a TLS-secured web portal and integrate their on-premises components through mTLS connections as identified in Figure 1. These connections and port settings should be accounted for in your cybersecurity processes and documentation.

**Important**
HPE highly recommends that all HPE GreenLake for Compute Ops Management and HPE GreenLake communication be protected with adequate firewall and HTTP proxy devices.

- Webpage (HTML): You can use a standard web browser to access HPE GreenLake, which is secured using HTTPS with TLS v1.3 or 1.2, that is authenticated by an HPE CA certificate for authenticated, encrypted, and secure connection. TLS v1.0 and v1.1 are disabled. To validate the authenticity of users, HPE GreenLake requires users to provide a correct combination of their username and password. In addition, MFA and SSO with SAML 2.0 is supported as a more secure and preferred method of authentication. These are explained later in this document.

  The HPE CA Certificate uses SHA256 with key size equal to EC 384 bits. Refer to Table 2 to understand the supported TLS v1.2 and 1.3 cipher suites.

**Table 2.** Supported TLS 1.2 and 1.3 cipher suites

| | |
|---|---|
| **The following cipher suites are supported in server-preferred order:** | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 |
| | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
| | TSL_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
| | TLS_AES_128_GCM_SHA256 |
| | TLS_AES_256_GCM_SHA384 |
| | TLS_CHACHA20_POLY1305_SHA256 |

- **mTLS:** HPE iLO 5 and HPE iLO 6 management processors embedded in the customer's on-premises server connects to HPE GreenLake for Compute Ops Management via an HTTPS (port 443) secured web connection for bidirectional communication to provide onboarding, inventory, health, power control, and firmware management. This WebSocket is created during the onboarding steps and remains open with a persistent connection to HPE GreenLake for Compute Ops Management cloud. During the onboarding process, an HPE issued client certificate is used to connect to HPE GreenLake for Compute Ops Management for HPE iLO management. HPE OneView uses the same approach to connect to Compute Ops Management via HTTPS (port 442) with a mTLS secured WebSocket.

**Important**
The HPE iLO management processor embedded in the server communicates with HPE GreenLake for Compute Ops Management and is isolated from the server.

If network issues occur, this WebSocket will be closed on either side. The HPE iLO will retry to establish the WebSocket connection to HPE GreenLake for Compute Ops Management every 30 seconds in a 5-minute window; if all of those fail, the device will give up for one hour before repeating the reconnection process of one attempt every 30 seconds for 5 minutes. The retry process will continue until the connection to the WebSocket is reestablished. This allows the solution to withstand any sort of network outages between the on-premises server and cloud. The WebSocket connection and retry process will be terminated if cloud-based management is disabled in the HPE iLO.

Customers need to open only port 443 on their firewall for any outbound communication to various COM endpoints. Public interface FQDNs, ports used, and the initiator that access the internet include the following:

**Table 3.** Customer firewall requirements

| Public interface FQDN | Port | Initiator | Protocol | Direction | Description |
|---|---|---|---|---|---|
| **cloud.hpe.com** | 443 | User | TCP | Outbound | Allows communication to HPE GreenLake |
| **common.cloud.hpe.com** | 443 | User | TCP | Outbound | Allows login to HPE GreenLake for Compute Ops Management |
| **us-west2.compute.cloud.hpe.com** | 443 | User | TCP | Outbound | HPE GreenLake for Compute Ops Management US region |
| **us-west2-mtls.compute.cloud.hpe.com** | 443 | User | TCP | Outbound | Device management API |
| **us-west2-api.compute.cloud.hpe.com** | 443 | User | TCP | Outbound | Allows access to HPE GreenLake for Compute Ops Management API calls |
| **us-west2-devices.compute.cloud.hpe.com** | 443 | HPE iLO 5, HPE iLO 6, HPE OneView 8.4 | TCP | Outbound | Device management WebSocket server |
| **eu-central1.compute.cloud.hpe.com** | 443 | User | TCP | Outbound | HPE GreenLake for Compute Ops Management EU region |
| **eu-central1-mtls.compute.cloud.hpe.com** | 443 | User | TCP | Outbound | Device management API |
| **eu-central1-api.compute.cloud.hpe.com** | 443 | User | TCP | Outbound | Allows access to HPE GreenLake for Compute Ops Management API calls |
| **eu-central1-devices.compute.cloud.hpe.com** | 443 | HPE iLO 5, HPE iLO 6, HPE OneView 8.4 | TCP | Outbound | Device management WebSocket server |
| **ap-northeast1.compute.cloud.hpe.com** | 443 | User | TCP | Outbound | HPE GreenLake for Compute Ops Management APJ region |
| **ap-northeast1-mtls.compute.cloud.hpe.com** | 443 | User | TCP | Outbound | Device management API |
| **ap-northeast1-api.compute.cloud.hpe.com** | 443 | User | TCP | Outbound | Allows access to HPE GreenLake for Compute Ops Management API calls |
| **ap-northeast1-devices.compute.cloud.hpe.com** | 443 | HPE iLO 5, HPE iLO 6, HPE OneView 8.4 | TCP | Outbound | Device management WebSocket server |
| **device.cloud.hpe.com** | 443 | HPE iLO 5, HPE iLO 6, HPE OneView 8.4 | TCP | Outbound | Device activation |
| **midway.ext.hpe.com** | 443 | HPE iLO 5, HPE iLO 6, HPE OneView 8.4 | TCP | Outbound | Allows HPE iLO to obtain certificate and firmware downloads. Provide HPE OneView an HPE client certificate for mTLS and the appliance ID. |

For the mTLS connection, HPE iLO certificate will be ECDSAp384 and key size will be 384 bits.

**Table 4.** Supported TLS 1.2 cipher suites and their associated HPE iLO security mode

| Description | HPE iLO security mode | Cipher suite |
|---|---|---|
| **The following cipher suites are supported in server-preferred order** | **Production** | **ECDHE-RSA-AES256-GCM-SHA384** |
| | | **ECDHE-RSA-AES256-SHA384** |
| | | **ECDHE-RSA-AES256-SHA** |
| | | **DHE-RSA-AES256-GCM-SHA384** |
| | | **DHE-RSA-AES256-SHA256** |
| | | **DHE-RSA-AES256-SHA** |
| | | **AES256-GCM-SHA384** |
| | | **AES256-SHA256** |
| | | **AES256-SHA** |
| | | **ECDHE-RSA-AES128-GCM-SHA256** |
| | | **ECDHE-RSA-AES128-SHA256** |
| | | **ECDHE-RSA-AES128-SHA** |
| | | **DHE-RSA-AES128-GCM-SHA256** |
| | | **DHE-RSA-AES128-SHA256** |
| | | **DHE-RSA-AES128-SHA** |
| | | **AES128-GCM-SHA256** |
| | | **AES128-SHA256** |
| | | **AES128-SHA** |
| | | **ECDHE-RSA-DES-CBC3-SHA** |
| | | **EDH-RSA-DES-CBC3-SHA** |
| | | **DES-CBC3-SHA** |
| | **FIPS** | **ECDHE-RSA-AES256-GCM-SHA384** |
| | | **ECDHE-RSA-AES256-SHA384** |
| | | **DHE-RSA-AES256-GCM-SHA384** |
| | | **DHE-RSA-AES256-SHA256** |
| | | **ECDHE-RSA-AES128-GCM-SHA256** |
| | | **ECDHE-RSA-AES128-SHA256** |
| | | **DHE-RSA-AES128-GCM-SHA256** |
| | | **DHE-RSA-AES128-SHA256** |

HPE OneView connections are secured using a similar list of algorithms, ciphers, and protocols. For more details, please refer to the HPE OneView User guide located here.

## Authentication for users

This section discusses industry-standard authentication methods available for HPE GreenLake for Compute Ops Management. HPE provides three types of authentications for logging into HPE GreenLake.

- Single sign-on (SSO)
- Multi-factor authentication (MFA)
- Single-factor authentication

### Single sign-on authentication

SSO authentication enables organizations to simplify the user experience of logging into external portals by allowing users to enter their company login credentials to authenticate their identity.

Users will be able to log in to HPE GreenLake with their company's user credentials. After their login, however, HPE GreenLake will verify those credentials by sending a SAML request (digitally signed XML) to the user's trusted company IdP, which in turn will verify the credentials and send back a SAML response confirming that they are valid.

### Multi-factor authentication

Multi-factor authentication implements multiple levels of authentication for a user to gain access to HPE GreenLake. HPE supports software-based authenticators (Okta Verification, Security Key or Biometric Authenticator, Google Authenticator™) that, when combined with a traditional user login, provide an extra layer of security.

### Single-factor authentication

Single-factor authentication requires a username and password to verify a user's identity. Passwords must meet the following specifications:

- Must be between 8 and 255 characters, with a minimum of five unique characters
- Cannot have more than two repeated characters
- Must contain at least one special character, one numeric character, one uppercase letter, and a lowercase letter
- Cannot contain user account data and are checked against a list of commonly used passwords

All validated passwords adhere to a strict policy:

- New passwords cannot match the past six passwords used within the past 365 days.
- Passwords expire automatically after 182 days.
- Accounts with multiple login failures are automatically locked out for a period.

## Role-based access control for users

### HPE GreenLake

HPE GreenLake user permissions are enforced by using role-based access control (RBAC) to ensure that the correct level of access is given to each user. The administrator of an organizational unit has the option to assign predefined roles provided by HPE GreenLake or create custom roles for users. Information can be found in the HPE GreenLake user guide.

**Note**

The creator of the organizational unit within HPE GreenLake is automatically assigned administrator permissions.

### HPE GreenLake for Compute Ops Management

This section describes the RBAC for Compute Ops Management. It is recommended that you learn more about the RBAC features in HPE GreenLake, which can be found in the HPE GreenLake user guide. HPE GreenLake for Compute Ops Management supports three different roles, which should be clearly defined in your cybersecurity processes and plans.

**Table 5.** HPE GreenLake for Compute Ops Management RBAC roles

| Type | Assigned permissions |
|---|---|
| **Administrator** | Enables all privileges for the customer's organization including onboarding, asset management, creating roles, inviting users, and assigning roles for users |
| **Operator** | Enables privileges to edit servers and schedules as well as user groups in HPE GreenLake for Compute Ops Management, all other resource access is read only |
| **Observer** | Enables privileges to view components in the assigned organization without the ability to make change |

### Device onboarding into the HPE GreenLake for Compute Ops Management

This section describes security topics you need to be aware of during device onboarding.

**Important**

All device onboarding communications are always initiated by HPE iLO. There will never be a cloud-initiated device onboarding discovery request. Network communications are secured with mTLS.

Connections to HPE GreenLake are made with HTTPS and TLS v1.2. RBAC ensures that you are directed to the correct instance with the correct permissions.

When cloud-based management is enabled in the HPE iLO, a WebSocket connection using mTLS will be established between HPE iLO and Compute Ops Management. This WebSocket is permanent and would only be permanently disabled if cloud-based management is disabled.

### Onboarding HPE OneView appliances into HPE GreenLake for Compute Ops Management — HPE OneView Edition

HPE OneView appliances can be onboarded into HPE GreenLake for Compute Ops Management through a slightly different process but use the same robust security mechanisms to ensure trusted private connections. The unique HPE OneView appliance ID is taken from the HPE OneView instance and entered into HPE GreenLake for Compute Ops Management. When the appliance ID is put into the HPE GreenLake for Compute Ops Management user interface, it will respond with an Activation Key. This key is unique to the appliance and can only be used to onboard the specific appliance.

Once the activation key is put into the HPE OneView user interface to enable cloud management, the HPE OneView instance will create a persistent mTLS WebSocket connection to the HPE GreenLake for Compute Ops Management endpoint in the cloud. This connection is secured with HPE issued security certificate similar to the one used when onboarding an HPE iLO into HPE GreenLake for Compute Ops Management. Finally, with the certificate and the activation complete an mTLS connection created.

**Important**

Service subscriptions are used to control access to HPE GreenLake for Compute Ops Management — HPE OneView Edition devices. A Compute Ops Management — HPE OneView Edition subscription is needed to manage Compute Ops Management — HPE OneView Edition devices within HPE GreenLake for Compute Ops Management, and user rights further control access to manage Compute Ops Management — HPE OneView Edition devices. If a user account does not have the proper Compute Ops Management — HPE OneView Edition access added to their account they will not even see Compute Ops Management — HPE OneView Edition devices within HPE GreenLake for Compute Ops Management.

### RBAC for HPE iLO

The HPE iLO also has RBAC for the local users. Four roles are defined in HPE iLO as shown in Table 6. These roles are used only for local direct access to HPE iLO and not for communicating with HPE GreenLake for Compute Ops Management.

**Table 6.** HPE iLO RBAC roles

| Type | Assigned permissions |
|---|---|
| **Administrator** | Enables all privileges except Recovery Set (usable for onboarding) |
| **Operator** | Allows all privileges except: Configure HPE iLO 5 Settings, Administer User Accounts, and Recovery Set (usable for onboarding) |
| **Read only** | Enables only the login privilege |
| **Custom (default)** | Allows the user to define a custom privilege set (usable for onboarding with required custom role settings) |

**Note**

Only HPE authorized engineers with customer consent have access to customer accounts for support troubleshooting.

# How HPE GreenLake for Compute Ops Management and HPE GreenLake protect you in the cloud

## Risk assessments

HPE GreenLake for Compute Ops Management does a regular review of the application architecture and threat analysis for discovery of any type of risks present in the system and identifying how those risks can be mitigated or eliminated. This analysis helps HPE GreenLake for Compute Ops Management to correct any vulnerabilities before an attack occurs, protect against theft and damage against systems, avoid any fines from lack of compliance.

## Protecting against vulnerabilities

When a vulnerability is discovered, HPE engineering will perform an analysis on the CVEs and determine how the vulnerability applies to HPE GreenLake for Compute Ops Management cloud design. CVEs applicable to HPE GreenLake for Compute Ops Management cloud model will be mitigated or will have workarounds to alleviate the discovered CVE in HPE GreenLake for Compute Ops Management controlled space. Furthermore, if additional actions are required for customers to follow through on their premises, HPE will provide a bulletin that details the requirement.

To protect against breaches and incidents on the web application layer, HPE GreenLake for Compute Ops Management has integrated application security into the software development lifecycle. HPE GreenLake Compute Ops Management tests applications for vulnerabilities and weaknesses on a continuous basis using standards such as OWASP Application Security Verification Standard (ASVS) checking applications for remote code execution, SQL injection, cross-site scripting (XSS), identity and access, session validation, code injections, cryptography, and more.

## Secure architecture

HPE GreenLake for Compute Ops Management is designed and implemented with a set of containerized microservices. Its containers are built with HPE controlled minimal base images. Containers built with base images provide the developer with full control of the content, which allows HPE engineers to quickly mitigate security issues and redeploy mitigated microservices in a highly efficient manner.

HPE GreenLake for Compute Ops Management is deploying tools that identify vulnerabilities, misconfigurations, and compliance violations in Infrastructure as code templates, container images, and Git repositories. It goes through architectural reviews, network, and application penetration tests on a regular schedule.

## API gateway and Amazon CloudFront

The API gateway provides protection against DDoS attacks by authenticating at the application layer to prevent counterfeit requests, and rate limit protections prevent SYN flood attacks. Additionally, the API gateway provides obfuscation of components in the solution, allows authorization of APIs, and controls access to select endpoints in the solution. Amazon CloudFront provides the caching layer along with integration with web application firewall for additional layers of security.

## Customer data stored

Data that is stored and used by HPE GreenLake for Compute Ops Management includes HPE iLO inventory data and health status along with HPE OneView data for managed physical devices and logical resources. No HPE OneView credentials are stored by HPE GreenLake for Compute Ops Management. All data at rest is encrypted.

RBAC verifies that users have the correct access to each resource in the application. Customers can plan their IT business processes with RBAC when using HPE GreenLake for Compute Ops Management.

Data related to user accounts and customer details for each HPE GreenLake for Compute Ops Management customer are isolated from other tenant companies at the HPE GreenLake level. This provides consistent privacy and data access protection across applications.

Data stored within HPE GreenLake for Compute Ops Management remains in the region that is specified during the initial setup. For more information, see the HPE privacy statement at hpe.com/us/en/legal/privacy.html.

## Data that HPE employees or partners can access

HPE R&D teams and HPE partners do not have access to customer-related data and application data. However, a very limited number of engineers with the customer's permission will have read-only access to the customer information (such as usernames, address, server network information, and such). We maintain a separate environment for internal development, and no customer data is allowed in those environments.

## Security assurance and compliance

HPE GreenLake for Compute Ops Management recently completed CSA STAR Level 1: self-assessment to offer better transparency around the security controls put in place for securing customer data. For more information, see the HPE GreenLake for Compute Ops Management CAIQ.

HPE GreenLake for Compute Ops Management has also undergone SOC 2 Type 1 attestation.

HPE is actively working toward a FIPS 140-2 Level 1 certification. All data in transit between customer devices on-premises and HPE GreenLake for Compute Ops Management device portal is protected with FIPS 140-2 compliant encryption and ciphers. Similarly, all data in transit and at rest within the software application is protected with FIPS 140-2 encryption and ciphers. All cryptography within the application is provided by OpenSSL 1.1.1, and we are actively working toward implementing a FIPS Certified OpenSSL 3.0 provider. The HPE GreenLake for Compute Ops Management application has been built to enable the FIPS 140-2 compliance by design. Customers don't have to make any changes to the software or their account to enable FIPS 140-2 compliance.

## Open-source software license statement

See the HPE GreenLake user guide and HPE GreenLake for Compute Ops Management online help for open-source software license statements.

## Data security and privacy statement for HPE GreenLake and Compute Ops Management

HPE respects and considers the major privacy principles and frameworks around the world, including, but not limited to, the OECD Guidelines on the Protection of Privacy and Transborder Flows, the EU General Data Protection Regulation (GDPR) 2016/679, and the APEC Privacy Framework. The HPE privacy practices described in this privacy statement also comply with the APEC Cross Border Privacy Rules (CBPR) system. For more information, see the HPE privacy statement at hpe.com/us/en/legal/privacy.html.

## Learn more at

HPE.com/us/en/compute/management-software.html

Explore HPE GreenLake

Chat now (sales)



a50004539ENW, Rev. 6

Hewlett Packard Enterprise