

# vCloud Usage Meter Deployment and Administration Guide

03 AUG 2023

vCloud Usage Meter 4.7

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

<https://docs.vmware.com/>

**VMware by Broadcom**

3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2023-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to <https://www.broadcom.com>. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. [Copyright and trademark information](#).

# Contents

- 1 VMware® vCloud® Usage Meter Deployment and Administration Guide 6**
- 2 Overview of vCloud Usage Meter 7**
- 3 Before You Begin with vCloud Usage Meter 8**
- 4 Deploying and Configuring vCloud Usage Meter 9**
  - Deploy the vCloud Usage Meter Appliance 10
  - Verify the Password Strength Compliance for a User Account in vCloud Usage Meter 13
  - Access the vCloud Usage Meter Web Interface 13
  - Accessing the vCloud Usage Meter Web Interface for the First Time 14
  - Configure a Proxy Server through the vCloud Usage Meter VAMI 14
  - Configure a Syslog Server through the vCloud Usage Meter VAMI 16
  - Configuring Active Directory Authentication for the vCloud Usage Meter Appliance 17
  - Setting Up a Second Network Adapter in vCloud Usage Meter 20
- 5 Federal Information Processing Standard (FIPS) Compliance-Based Configurations for vCloud Usage Meter 24**
  - Configure the FIPS-Compliance Mode for vCloud Usage Meter 24
- 6 vCloud Usage Meter Certificate Management 26**
  - Import an Internal Certificate Authority (CA) - Signed Certificate for a vCloud Usage Meter Appliance with Enabled FIPS Mode 27
  - Import an Internal Certificate Authority (CA) - Signed Certificate for a vCloud Usage Meter Appliance with Deactivated FIPS Mode 28
  - Install a Certificate Authority (CA) - Signed Certificate for a vCloud Usage Meter Appliance with Enabled FIPS Mode 29
  - Install a Certificate Authority (CA) - Signed Certificate for a vCloud Usage Meter Appliance with Deactivated FIPS Mode 31
  - Replace the Default Appliance Self-Signed SSL Certificate With a New Self-Signed Certificate for a vCloud Usage Meter appliance with enabled FIPS mode 34
  - Replace the Default Appliance Self-Signed SSL Certificate With a New Self-Signed Certificate for a vCloud Usage Meter appliance with deactivated FIPS mode 35
  - Import a Certificate to the vCloud Usage Meter Appliance Keystore when FIPS Mode is Enabled 37
  - Import a Certificate to the vCloud Usage Meter Appliance Keystore when FIPS Mode is Deactivated 38
- 7 Managing the Metering in vCloud Usage Meter 40**
  - Assign Permissions for vCenter Server for Metering with vCloud Usage Meter 42

- Add a vCenter Server Instance for Metering in vCloud Usage Meter 45
- Add a VMware Cloud Foundation Instance for Metering in vCloud Usage Meter 46
- Add a Site Recovery Manager Instance for Metering in vCloud Usage Meter 47
- Add a Tanzu Kubernetes Grid Management Cluster for Metering in vCloud Usage Meter 48
- Add a VMware Cloud Director Instance for Metering in vCloud Usage Meter 51
- Add a vRealize Suite Lifecycle Manager Instance for Metering in vCloud Usage Meter 51
- Metering vRealize Operations with vCloud Usage Meter 54
- Add a vRealize Automation 7 Instance for Metering in vCloud Usage Meter 57
- Add a vRealize Automation 8 Instance for Metering in vCloud Usage Meter 58
- Add an NSX Data Center for vSphere Instance for Metering in vCloud Usage Meter 59
- Add an NSX-T Data Center Instance for Metering in vCloud Usage Meter 60
- Add a vRealize Network Insight Instance for Metering in vCloud Usage Meter 60
- Add a NSX Advanced Load Balancer Instance for Metering in vCloud Usage Meter 61
- Add a VMware Cloud Director Availability Instance for Metering in vCloud Usage Meter 62
- Configure the Level of Anonymization of vCloud Usage Meter Reports 63
- Edit Product Information in vCloud Usage Meter 64
- Delete Product Servers in vCloud Usage Meter 65
- Change the vCloud Usage Meter Logging Level 65

## 8 Managing Customer Rules in vCloud Usage Meter 67

- Object and Object Types in Customer Rules in vCloud Usage Meter 69
- Add a Customer Rule in vCloud Usage Meter 70
- Edit a Customer Rule in vCloud Usage Meter 71
- Delete a Customer Rule in vCloud Usage Meter 71
- Audit Customer Rules in vCloud Usage Meter 72

## 9 License Key Management in vCloud Usage Meter 74

## 10 Managing vCloud Usage Meter Services 75

- Verify if a vCloud Usage Meter Instance Reports Usage Data 75
- Check the Status of the Services in vCloud Usage Meter 75
- Start a vCloud Usage Meter Service 76
- Stop a vCloud Usage Meter Service 76
- Generate Support Bundle Collections in vCloud Usage Meter 76

## 11 Managing vCloud Usage Meter Accounts 78

- Reset the Root Password in vCloud Usage Meter 78
- Change the Root Password in vCloud Usage Meter 79
- Unlock the **usagemeter** Account 79
- Change the User Account Passwords for the usagemeter and the umauditor User Accounts 80
- Change the Password Expiration Parameters for the vCloud Usage Meter User Accounts 81

Password Requirements for the vCloud Usage Meter User Accounts 81

## **12** Upgrading the vCloud Usage Meter Appliance 82

In-Place Upgrade of vCloud Usage Meter 82

## **13** Email Notifications for vCloud Usage Meter Instances 86

Configure the Local Email Notifications for vCloud Usage Meter 87

Troubleshooting Issues with the SMTP settings for vCloud Usage Meter 90

## **14** Product Notifications in vCloud Usage Meter 91

# VMware<sup>®</sup> vCloud<sup>®</sup> Usage Meter Deployment and Administration Guide

1

The *vCloud Usage Meter Deployment and Administration Guide* provides information about deploying, configuring, and using vCloud Usage Meter.

## Intended Audience

This guide is intended for service provider administrators with access privileges to manage vCloud Usage Meter. These individuals must be familiar with data center operations.

## VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.

# Overview of vCloud Usage Meter

# 2

vCloud Usage Meter is a virtual appliance that meters and collects product consumption data.

## What data does vCloud Usage Meter collect?

vCloud Usage Meter collects product consumption data from VMware Cloud Foundation instances and other products. For more information, see the [VMware Usage Meter Data Privacy Guide](#) on the Broadcom Partner Portal Page for VMware Cloud Service Providers.

## How does vCloud Usage Meter report monthly product consumption data?

vCloud Usage Meter collects the data on an hourly basis and sends it to VMware Cloud Services Console, which is a service that aggregates the data. VMware Cloud Services Console then sends the data to the Broadcom Support Portal, where you receive your invoices.

# Before You Begin with vCloud Usage Meter

# 3

To collect accurate usage data, vCloud Usage Meter requires a specific configuration of the metered VMware Cloud Foundation instances. To access the vCloud Usage Meter Web interface, you must allow access on the appropriate TCP ports.

## VMware Cloud Foundation Licenses

You must license every VMware Cloud Foundation host appropriately based on the number of CPU sockets and cores. Keep in mind that per core licensing requires minimum of 16 cores licensed per CPU. The hosts from the customer commit must be licensed with licenses from the customer commit pool and the hosts from the aggregate commit must be licensed with licenses from the aggregate commit pool. vCloud Usage Meter automatically detects Bring Your Own License (BYOL).

## TCP Ports

vCloud Usage Meter uses predefined TCP ports. If you manage network components from outside a firewall, you might need to configure the firewall to allow access to the appropriate ports. For information about the ports that vCloud Usage Meter requires, see [VMware Ports and Protocols](#).



# Deploying and Configuring vCloud Usage Meter

# 4

vCloud Usage Meter is a virtual appliance that you deploy with vSphere Web Client. To set up the virtual appliance, you must set the required passwords, configure your network, and add a vCenter Server instance for metering.

To manage who can use the application, you can set up an LDAP authentication.

The size of your data set and the vCenter Server inventories that vCloud Usage Meter meters affect the speed of a consumption data collection. For large data sets and vCenter Server inventories, consider deploying more than one vCloud Usage Meter appliances.

To avoid configuration problems and ensure accurate metering of products, you must synchronize the vCloud Usage Meter date and time with the date and time of the metered products. As a best practice, use the same NTP server for the vCloud Usage Meter appliance and the metered products.

- [Deploy the vCloud Usage Meter Appliance](#)

You deploy the vCloud Usage Meter appliance with vSphere Web Client.

- [Verify the Password Strength Compliance for a User Account in vCloud Usage Meter](#)

After deploying vCloud Usage Meter, you can verify if a user account password complies with the password strength restrictions.

- [Access the vCloud Usage Meter Web Interface](#)

To configure the appliance and to add product instances for metering, you log in to the vCloud Usage Meter Web interface. To access the vCloud Usage Meter Web interface, you need the vCloud Usage Meter host name or IP address.

- [Accessing the vCloud Usage Meter Web Interface for the First Time](#)

If you are accessing the vCloud Usage Meter Web interface for the first time, you must configure the initial vCloud Usage Meter web interface wizard.

- [Configure a Proxy Server through the vCloud Usage Meter VAMI](#)

You can allow connection between vCloud Usage Meter and the Internet through a proxy server. To configure the proxy server, use the vCloud Usage Meter virtual appliance management interface (VAMI).

- [Configure a Syslog Server through the vCloud Usage Meter VAMI](#)

You use the vCloud Usage Meter VAMI to configure vCloud Usage Meter to send the logging data to a third-party syslog server.

- [Configuring Active Directory Authentication for the vCloud Usage Meter Appliance](#)

To provide identity and access management services linked to an external Active Directory server to the vCloud Usage Meter appliance, you configure the local LDAP name service daemon, the Linux Pluggable Authentication Modules, and the Name Service Switch on the appliance.

- [Setting Up a Second Network Adapter in vCloud Usage Meter](#)

To meter the products in an isolated network, you can add and configure a second network adapter for the vCloud Usage Meter appliance.

## Deploy the vCloud Usage Meter Appliance

You deploy the vCloud Usage Meter appliance with vSphere Web Client.

### Prerequisites

- vCloud Usage Meter requires the following hardware resources.
  - Two virtual CPU cores
  - 8 GB of memory
  - 80 GB storage
- Download the vCloud Usage Meter OVA file from the [Broadcom Support Portal](#) download product page and save it locally.
- Verify that you have access and sufficient privileges to deploy an OVA file with vSphere Web Client.

### Procedure

- 1 Log in to the vSphere Web Client as a user who has sufficient privileges to deploy an OVA file.
- 2 In the vSphere Web Client, navigate to **Hosts and Clusters**.
- 3 Right-click a target host or cluster for your vCloud Usage Meter appliance, and select **Deploy OVF Template**.
- 4 In the **Deploy OVF Template** wizard, navigate to the vCloud Usage Meter OVA file, and click **Next**.
- 5 Enter a unique name for the vCloud Usage Meter appliance, select the target deployment location, and click **Next**.

- 6 On the **Select a compute resource** page, select the deployment target resource in which you want to run the vCloud Usage Meter appliance, and click **Next**.

You can select a cluster, a host, a vApp, or a resource pool.

- 7 Verify the OVF template details and click **Next**.
- 8 Review and accept the end-user license agreement, and click **Next**.
- 9 On the **Select storage** page, select where and how vCloud Usage Meter must store the files. Select the virtual disk format, the VM storage policy, and the datastore for the appliance.
- 10 Select a network for the deployed template and click **Next**.

---

**Note** By default, the appliance deploys with IP allocation set to Static-Manual and protocol set to IPv4. If you leave the network properties fields blank, the appliance is deployed with IP allocation set to DHCP.

---

- 11 On the **Customize template** page, set the passwords for the local user accounts, and configure how vCloud Usage Meter manages the collected product consumption data.

---

**Note** All passwords must meet a set of password requirements. For more information, see [Password Requirements for the vCloud Usage Meter User Accounts](#).

---

Deployment Property	Note
Initial <b>root</b> password	Set the <b>root</b> password and keep a record of the password. If you enter a <b>root</b> password that does not meet the security requirements, vCloud Usage Meter prompts you to change the password on your first login to the appliance. You cannot recover the <b>root</b> password, but you can reset it. See <a href="#">Reset the Root Password in vCloud Usage Meter</a> for instructions on changing the vCloud Usage Meter <b>root</b> password.
Use Federal Information Processing Standards (FIPS)	To deploy the vCloud Usage Meter appliance in FIPS-compliant mode, click the toggle button.  <b>Note</b> If you deploy the vCloud Usage Meter appliance in FIPS-compliant based mode, running the deployed vCloud Usage Meter appliance on hardware that does not support Intel® Secure Key Technology might require a significant time and lead to timeout exceptions and application failures.
Initial <b>usagemeter</b> password	Set the <b>usagemeter</b> password. After the deployment of the appliance, verify that the <b>usagemeter</b> password meets the security requirements. For information, see <a href="#">Verify the Password Strength Compliance for a User Account in vCloud Usage Meter</a> . If the password does not meet the existing security requirements, you must change the <b>usagemeter</b> password. For more information, see <a href="#">Change the User Account Passwords for the usagemeter and the umauditor User Accounts</a> .

Deployment Property	Note
Initial <b>umauditor</b> password	Set the <b>umauditor</b> password. After the deployment of the appliance, verify that the <b>umauditor</b> password meets the security requirements. For information, see <a href="#">Verify the Password Strength Compliance for a User Account in vCloud Usage Meter</a> . If the password does not meet the existing security requirements, you must change the <b>umauditor</b> password. For more information, see <a href="#">Change the User Account Passwords for the usagemeter and the umauditor User Accounts</a> .
Hostname	Enter a hostname for the vCloud Usage Meter appliance. Required in case of a static IP allocation network mode. In case of DHCP network mode, leave the field blank to try to reverse lookup the IP address.
Host Network Default Gateway	Enter the default gateway address of the vCloud Usage Meter appliance. Required in case of a static IP allocation network mode.
Domain Name	Enter the domain name of vCloud Usage Meter appliance. Required in case of a static IP allocation network mode.
Domain Search Path	Enter the domain names that you use as a domain search path for the vCloud Usage Meter appliance in a comma-separated list. Required in case of a static IP allocation network mode.
Domain Name Servers	Enter the domain name servers IP addresses for the vCloud Usage Meter appliance in a comma-separated list. Required in case of a static IP allocation network mode.
Network 1 IP Address	Enter the IP address for this interface. Required in case of a static IP allocation network mode.
Network 1 Netmask. Netmask in CIDR notation	For vCloud Usage Meter appliances with a static IP address, configure the netmask in CIDR notation. For example, enter <b>24</b> for 255.255.255.0, <b>28</b> for 255.255.255.240. Required in case of a static IP allocation network mode.

**12** On the **Ready to complete** page, review the information and click **Finish**.

- a To deactivate FIPS, deselect the **FIPS** check box.

**Important** To avoid compliance issues with Partner Connect Program, do not clone vCloud Usage Meter appliances. If you need an additional vCloud Usage Meter instance, you must deploy a new vCloud Usage Meter appliance.

## Results

The default time zone of the deployed vCloud Usage Meter appliance is UTC and you cannot change it.

## What to do next

Set the vCloud Usage Meter appliance vRAM as needed. Most service providers can run well with 8 GB. On the **Support** page, you can monitor and increase the memory use.

To register the appliance to a provider organization, see [Accessing the vCloud Usage Meter Web Interface for the First Time](#).

## Verify the Password Strength Compliance for a User Account in vCloud Usage Meter

After deploying vCloud Usage Meter, you can verify if a user account password complies with the password strength restrictions.

### Procedure

- 1 Log in to the vCloud Usage Meter console as **root**.
- 2 To verify if a user account password meets the security requirements, run the following command.

```
echo $user-name_user-password | cracklib-check
```

If you receive the following system output `user-name_user-password: OK`, your password is compliant with the security restrictions.

If the password is not complying with the security restrictions, you must configure a new password.

## Access the vCloud Usage Meter Web Interface

To configure the appliance and to add product instances for metering, you log in to the vCloud Usage Meter Web interface. To access the vCloud Usage Meter Web interface, you need the vCloud Usage Meter host name or IP address.

### Prerequisites

Verify that the virtual machine on which you deployed the vCloud Usage Meter appliance is powered on.

### Procedure

- 1 Open a Web browser and enter the URL for your vCloud Usage Meter instance: **https://vcloud\_usage\_meter\_ip\_address**.
- 2 Log in as **usagemeter** or as a user from an LDAP domain.

You configure the password for the **usagemeter** user account during the deployment of the vCloud Usage Meter appliance.

## What to do next

If you log in to the web interface for the first time, you must follow the **Usage Meter Initialization** wizard prompts.

# Accessing the vCloud Usage Meter Web Interface for the First Time

If you are accessing the vCloud Usage Meter Web interface for the first time, you must configure the initial vCloud Usage Meter web interface wizard.

The **Usage Meter Initialization** wizard guides you through the steps for registering your vCloud Usage Meter instances with VMware Cloud.

## Procedure

- 1 On the **Welcome** page, accept the term and conditions for the automatic reporting of product consumption data to VMware and click **Next**.  
By default, the check box for terms and conditions is selected.
- 2 On the **Network Connectivity** page, select the type of network connection the vCloud Usage Meter appliance uses to connect to the Internet.  
If you configure a network proxy server, you must provide the network proxy server IP address or the host name and credentials.
- 3 On the **Summary** page, register the vCloud Usage Meter appliance for an automatic reporting of product consumption data.
  - a To register the vCloud Usage Meter instance in VMware Cloud Services Console, follow the steps in [How do I register a vCloud Usage Meter instance for automatic reporting](#) in the VMware Cloud Services Console documentation.
  - b Click **Check registration**.
- 4 Click **Finish**.

# Configure a Proxy Server through the vCloud Usage Meter VAMI

You can allow connection between vCloud Usage Meter and the Internet through a proxy server. To configure the proxy server, use the vCloud Usage Meter virtual appliance management interface (VAMI).

You can configure the proxy server by using the vCloud Usage Meter virtual appliance management interface (VAMI).

## Prerequisites

- Verify that you have the proxy server settings information.

- Verify that you have access to the vCloud Usage Meter virtual appliance management interface (VAMI) as **root**.

### Procedure

- 1 Access the vCloud Usage Meter VAMI and log in as **root**.
  - ◆ In the main menu bar of the vCloud Usage Meter Web interface, select **Settings > Network Connectivity**, and click **Go to the Virtual Appliance Management Interface (VAMI)**.

---

**Note** The VAMI login page opens.

---

- ◆ Log in directly to the vCloud Usage Meter VAMI at `https://um-appliance-host-name:5480`.
- 2 In the left navigation pane, click **Networking**.  
The **Network Settings** page opens.
  - 3 Next to **Proxy Settings**, click **Edit**.  
The **Edit Proxy Settings** dialog box opens.
  - 4 To enable a proxy setting, click the toggle button next to the setting.

Option	Description
HTTPS	Enable to configure the HTTPS proxy settings.
HTTP	Enable to configure the HTTP proxy settings.

- 5 Configure the proxy settings.
  - a Enter the server host name or IP address.
  - b Enter the port.
  - c Enter the username and password.
  - d To set an anonymous proxy server, select the **Anonymous** check box.
  - e Click **Save**.
- 6 To verify the connectivity through the proxy server, run the following commands from the vCloud Usage Meter appliance.

- ```
curl -x http|https://proxy_ip:proxy_port -L https://ums.cloud.vmware.com
```

- for proxy that does not require authentication.

- ```
curl -x http|https://proxy_ip:proxy_port --proxy-user proxy_user:proxy_password -L https://ums.cloud.vmware.com
```

- for proxy that requires authentication.

---

**Note** If you use proxy over HTTPS, you must import the proxy certificate. For more information, see [Chapter 6 vCloud Usage Meter Certificate Management](#).

---

## Configure a Syslog Server through the vCloud Usage Meter VAMI

You use the vCloud Usage Meter VAMI to configure vCloud Usage Meter to send the logging data to a third-party syslog server.

### Prerequisites

- Verify that you have access to the vCloud Usage Meter console as **root**.
- Verify that the remote syslog server is configured.
- Activate a network connection between vCloud Usage Meter and the syslog server.

### Procedure

- 1 Access the vCloud Usage Meter VAMI and log in as **root**.
  - ◆ In the main menu bar of the vCloud Usage Meter Web interface, select **Settings > Network Connectivity**, and click **Go to the Virtual Appliance Management Interface (VAMI)**.

---

**Note** You are redirected to the VAMI login page.

---

- ◆ Log in directly to the vCloud Usage Meter VAMI at `https://um-appliance-host-name:5480`.
- 2 In the left navigation pane, click **Syslog**.  
The **Forwarding Configuration** page opens.
  - 3 To configure new syslog server, click **Configure**.  
The **Create Forwarding Configuration** dialog box opens.
  - 4 Enter the syslog server information, and click **Save**.



# Configuring Active Directory Authentication for the vCloud Usage Meter Appliance

To provide identity and access management services linked to an external Active Directory server to the vCloud Usage Meter appliance, you configure the local LDAP name service daemon, the Linux Pluggable Authentication Modules, and the Name Service Switch on the appliance.

- [Configure the Local LDAP Name Service Daemon on the vCloud Usage Meter Appliance](#)

The vCloud Usage Meter appliance ships with a local LDAP name service daemon. To provide identity management and authentication services through an external Active Directory service, you edit the `/etc/nslcd.conf` file with the Active Directory connection configuration and additional properties. To provide authentication through both Active Directory and local user account, you then configure the local Name Service Switch.

- [Configure the Pluggable Authentication Module on the vCloud Usage Meter Appliance](#)

To activate authentication for Active Directory accounts and local accounts, you configure the Pluggable Authentication Module on the vCloud Usage Meter appliance.

## Configure the Local LDAP Name Service Daemon on the vCloud Usage Meter Appliance

The vCloud Usage Meter appliance ships with a local LDAP name service daemon. To provide identity management and authentication services through an external Active Directory service, you edit the `/etc/nslcd.conf` file with the Active Directory connection configuration and additional properties. To provide authentication through both Active Directory and local user account, you then configure the local Name Service Switch.

You configure the `/etc/nslcd.conf` based on the configuration of your Active Directory server. The provided settings are reference values, reconfigure these settings according to your environment.

### Procedure

- 1 Login to the vCloud Usage Meter console as **usagemeter**.
- 2 Reconfigure the local LDAP name service daemon.
  - a Navigate to the `/etc` folder.

```
cd /etc
```

- b Open the `nslcd.conf` file for editing.

```
sudo vi nslcd.conf
```

- c Add the Active Directory connection properties.

```
uri ldap://ldap.acme.com
base dc=acme,dc=com
binddn <your username>@acme.com
bindpw <your AD password>
```

- d Configure the Active Directory mappings.

```
# Mappings for Active Directory
referrals off
idle_timelimit 800
filter passwd (&(objectClass=user)(objectClass=person)(!(objectClass=computer)))
map passwd uid cn
```

- e Save the `/etc/nslcd.conf` file.

```
:wq!
```

- f Restart the `nslcd` service.

```
sudo systemctl restart nslcd
```

### 3 Activate Active Directory as a Name Service Switch source.

- a Open the `/etc/nsswitch.conf` file for editing.

```
sudo vi nsswitch.conf
```

- b Add LDAP as a source after local lookups for at least the `passwd`, `group`, and `shadow` types.

```
passwd: files ldap
group: files ldap
shadow: files ldap
```

- c Save the `/etc/nsswitch.conf` file.

```
:wq!
```

## Configure the Pluggable Authentication Module on the vCloud Usage Meter Appliance

To activate authentication for Active Directory accounts and local accounts, you configure the Pluggable Authentication Module on the vCloud Usage Meter appliance.

You edit several configuration files under the `/etc/pam.d` directory based on your environment. The provided configuration contains the minimal required settings.

### Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter**.

## 2 Configure the common authentication providers in the `/etc/pam.d/system-auth` configuration file.

- a Open the `/etc/pam.d/system-auth` file for editing.

```
sudo vi /etc/pam.d/system-auth
```

- b Add the following line to the file.

```
auth    sufficient  pam_ldap.so
auth    required    pam_unix.so
```

- c Save the `/etc/pam.d/system-auth` file.

```
:wq!
```

## 3 Configure the common account settings in the `/etc/pam.d/system-account` configuration file.

- a Open the `/etc/pam.d/system-account` file for editing.

```
sudo vi /etc/pam.d/system-account
```

- b Add the following lines to the file.

```
account sufficient pam_ldap.so
account required   pam_unix.so
account required   pam_permit.so
```

- c Save the `/etc/pam.d/system-account` file.

```
:wq!
```

## 4 Configure the common passwords settings in the `/etc/pam.d/system-password` configuration file.

- a Open the `/etc/pam.d/system-password` file for editing.

```
sudo vi /etc/pam.d/system-password
```

- b Add the following lines to the file.

```
password sufficient pam_ldap.so try_first_pass
password requisite  pam_cracklib.so
password required   pam_unix.so          sha512 shadow try_first_pass
```

- c Save the `/etc/pam.d/system-password` file.

```
:wq!
```

- 5 Configure the common session settings in the `/etc/pam.d/system-session` configuration file.

- a Open the `/etc/pam.d/system-session` file for editing.

```
sudo vi /etc/pam.d/system-session
```

- b Add the following lines to the file.

```
session    required    pam_unix.so
session    required    pam_limits.so
session    optional    pam_systemd.so
session    optional    pam_loginuid.so
session    optional    pam_ldap.so
```

- c Save the `/etc/pam.d/system-session` file.

```
:wq!
```

- 6 Configure the common authentication and account settings for the vCloud Usage Meter appliance.

- a Open the `/etc/pam.d/vmware-um-pam` file for editing.

```
sudo vi /etc/pam.d/vmware-um-pam
```

- b Add the following lines to the file.

```
auth       sufficient /lib64/security/pam_ldap.so
auth       required   /lib64/security/pam_unix_auth.so
account    sufficient /lib64/security/pam_ldap.so
account    required   /lib64/security/pam_unix_acct.so
```

- c Save the `/etc/pam.d/vmware-um-pam` file.

```
:wq!
```

## Setting Up a Second Network Adapter in vCloud Usage Meter

To meter the products in an isolated network, you can add and configure a second network adapter for the vCloud Usage Meter appliance.

During the deployment of the vCloud Usage Meter appliance, you configure the settings of the primary network adapter. You can then add a second network adapter, and configure it manually or by running a script. The second network adapter can support both DHCP or static IP allocation.

## Add a Second Network Adapter in vCloud Usage Meter

After successfully deploying vCloud Usage Meter, you can add a second network adapter.

### Procedure

- 1 Log in to vSphere Client as the user that deployed the vCloud Usage Meter appliance.
- 2 Navigate to the vCloud Usage Meter appliance.
- 3 Right-click the vCloud Usage Meter appliance and select **Edit Settings** from the drop-down menu.

The **Edit Settings** window opens.

- 4 Navigate to **Add new device > Network Adapter**.
- 5 Configure the network adapter.
  - a Select the network.
  - b Select the adapter type and the MAC address.
  - c Verify that the **Connected** check box is checked.

## Configure a Second Network Adapter for vCloud Usage Meter Manually

After you add a new network adapter for the deployed vCloud Usage Meter appliance, you can configure the network adapter manually.

### Procedure

- 1 Create and configure a `.network` file inside `/etc/systemd/network/` that contains the settings for the new network adapter.

---

**Note** Consider the following factors:

- Ensure that the name of the new network interface does not match the name of any of the existing adapters.
  - The permissions for the `.network` file must be 644. Check the permissions with the `chmod` command.
- 

- 2 Restart the `systemd-networkd` and `daemon-reload` services.

```
systemctl daemon-reload
```

```
systemctl restart systemd-networkd
```

## Configure the Second Network Adapter for vCloud Usage Meter by Using a Script

After you add a new network adapter for the deployed vCloud Usage Meter appliance, you can configure the second network adapter by using a script.

You can use the `configure_additional_nic.sh` script that is part of the vCloud Usage Meter deliverables. The script can operate with both static and DHCP IP addresses.

### Procedure

- 1 Transfer the script to the vCloud Usage Meter appliance using SSH (SCP).
- 2 Log in to the vCloud Usage Meter Web console or the vCloud Usage Meter remote Web console as **root**.
- 3 Run the `configure_additional_nic.sh` script.

For more information about the script, run the following command.

```
--h
```

After the script finishes execution, a new `.network` file is created at `/etc/systemd/network`. The file contains the network settings for the new network adapter.

## Configure Static Routing Tables for vCloud Usage Meter

If you have a second network adapter for vCloud Usage Meter, you can configure static routing tables and route the network packets through a specific gateway.

You can configure the network interfaces and routing with the `systemd-networkd` service used by Photon OS v3.

### Prerequisites

Ensure that you successfully configured a second network adapter either manually or by script. To set up the routing tables, you must use the `.network` files of the network interfaces you want to configure.

## Procedure

- 1 To route the network packets through a specific gateway, you can configure static routes by adding a Route section in the created `.network` files created for the network adapter. Here are some of the attributes you can configure.

Attribute	Description
Destination	Enter the specific IP address or the whole subnet of the target network.
Gateway	Enter the IP address of the specific gateway is configured to route the traffic.  <b>Note</b> The gateway attribute might already be populated in the Network section. Make sure to remove the attribute from the Network section and place the attribute in the Route section.
Metric	Enter a lower value to prioritize the route or a higher value to deprioritize the route.

- 2 To apply the changes, reload the `systemd-networkd` service.

```
systemctl daemon-reload
```

```
systemctl restart systemd-networkd
```

- 3 Verify that the static route has been added successfully by running the following command.

```
ip route
```

The static route appears as an output of the command.

# Federal Information Processing Standard (FIPS) Compliance-Based Configurations for vCloud Usage Meter

## 5

vCloud Usage Meter uses FIPS 140-2 validated cryptographic modules to run in FIPS-compliant mode. The NIST Cryptographic Module Validation Program (CMVP) validates the cryptographic modules compliant with the FIPS 140-2 standards.

The CPU of the vCloud Usage Meter appliance must support Intel Secure Key Technology.

When you deploy the vCloud Usage Meter appliance, FIPS 140-2 is activated by default. You can then enable or deactivate FIPS 140-2.

The following validated modules are used:

- BC-FJA (Bouncy Castle FIPS Java API) version 1.0.2: [Certificate #3673](#)
- VMware OpenSSL FIPS Object Module version 2.0.20: [Certificate #3550](#)

For more information about the cryptographic modules that VMware has validated against the FIPS 140-2 standard, see: <https://www.vmware.com/security/certifications/fips.html>.

Read the following topics next:

- [Configure the FIPS-Compliance Mode for vCloud Usage Meter](#)

## Configure the FIPS-Compliance Mode for vCloud Usage Meter

Starting from vCloud Usage Meter 4.7, you can enable or deactivate the FIPS-compliance mode for the vCloud Usage Meter appliance.

### Procedure

- 1 Log in to the vCloud Usage Meter Web interface.
- 2 Navigate to **Settings > Security**.



### 3 Enable or deactivate the FIPS-compliance mode.

Option	Description
Enable	Click <b>Enable</b> . <hr/> <b>Note</b> Ensure that all the products that the vCloud Usage Meter appliance meters are FIPS-compliant. Otherwise you might encounter issues when metering products which are not FIPS-compliant.
Disable	Click <b>Disable</b> .

### 4 To apply the changes in the FIPS-compliance based mode configuration, confirm the restart of the vCloud Usage Meter appliance.

A reboot of the vCloud Usage Meter appliance starts and might take some time.

#### What to do next

Log in to the vCloud Usage Meter appliance and verify that you successfully enabled or deactivated the FIPS-compliance mode.

# vCloud Usage Meter Certificate Management

# 6

After you deploy vCloud Usage Meter, the appliance generates a self-signed SSL certificate. When you access the vCloud Usage Meter Web interface over HTTPS for the first time, you are prompted to manually trust the self-signed certificate.

You can secure the connection to vCloud Usage Meter by replacing the vCloud Usage Meter self-signed certificate with by using an external or internal Certification Authority (CA) - signed certificate.

When running, all vCloud Usage Meter applications use the same keystore and CA certificate store. The NGINX certificates are updated on OS startup. Unless specifically noted, you can run commands on the vCloud Usage Meter console as **usagemeter**.

To allow remote interaction with the vCloud Usage Meter console, you can activate SSH or invoke the commands in a vSphere web console.

The vCloud Usage Meter appliance stores the certificates in a Java key store at `/opt/vmware/cloudusagemetering/platform/security/keystore`.

The CA certificate key store is located at `/opt/vmware/cloudusagemetering/platform/security/cacerts`.

---

**Note** The certificate CN and Subject Alternative Name (SAN) must match the hostname of the vCloud Usage Meter appliance.

---

Read the following topics next:

- [Import an Internal Certificate Authority \(CA\) - Signed Certificate for a vCloud Usage Meter Appliance with Enabled FIPS Mode](#)
- [Import an Internal Certificate Authority \(CA\) - Signed Certificate for a vCloud Usage Meter Appliance with Deactivated FIPS Mode](#)
- [Install a Certificate Authority \(CA\) - Signed Certificate for a vCloud Usage Meter Appliance with Enabled FIPS Mode](#)
- [Install a Certificate Authority \(CA\) - Signed Certificate for a vCloud Usage Meter Appliance with Deactivated FIPS Mode](#)
- [Replace the Default Appliance Self-Signed SSL Certificate With a New Self-Signed Certificate for a vCloud Usage Meter appliance with enabled FIPS mode](#)

- Replace the Default Appliance Self-Signed SSL Certificate With a New Self-Signed Certificate for a vCloud Usage Meter appliance with deactivated FIPS mode
- Import a Certificate to the vCloud Usage Meter Appliance Keystore when FIPS Mode is Enabled
- Import a Certificate to the vCloud Usage Meter Appliance Keystore when FIPS Mode is Deactivated

## Import an Internal Certificate Authority (CA) - Signed Certificate for a vCloud Usage Meter Appliance with Enabled FIPS Mode

If you want to replace the vCloud Usage Meter certificate with a certificate signed by an internal Certificate Authority (CA), you must first import the CA to the vCloud Usage Meter appliance with enabled FIPS mode.

### Prerequisites

- Verify that you have access to the vCloud Usage Meter console as **usagemeter**.
- Verify that FIPS is enabled for the vCloud Usage Meter appliance by navigating to **Settings > Security**.

### Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter** and stop all appliance services.

```
cd /opt/vmware/cloudusagemetering
```

```
./scripts/stop.sh All
```

```
sudo systemctl stop vmware-um-journal.service
```

```
sudo systemctl stop vmware-um-login.service
```

```
sudo systemctl stop vmware-um-schedule.service
```

- 2 Export the environment variables.

```
export $(grep -v '^#' "/opt/vmware/cloudusagemetering/platform/conf/env.properties" | xargs)
```

- 3 Establish a trust between the vCloud Usage Meter appliance with enabled FIPS mode and the certificate that is signed by the internal certificate authority.

Enter a name that identifies the certificate within the keystore under the **alias** property in the following command.

---

**Note** If FIPS mode is deactivated for the vCloud Usage Meter appliance, see [Import an Internal Certificate Authority \(CA\) - Signed Certificate for a vCloud Usage Meter Appliance with Deactivated FIPS Mode](#).

---

```
keytool -import -trustcacerts -file filepath-to-the-certificate -alias custom-internal-certificate-authority -keystore /opt/vmware/cloudusagemetering/platform/security/cacerts -storetype BCFKS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath /opt/vmware/cloudusagemetering/platform/lib/bc-fips-1.0.2.1.jar -storepass "$ {TRUST_STORE_PASSWORD}"
```

- 4 Reboot the vCloud Usage Meter appliance with enabled FIPS mode.

```
sudo reboot
```

## Import an Internal Certificate Authority (CA) - Signed Certificate for a vCloud Usage Meter Appliance with Deactivated FIPS Mode

If you want to replace the certificate of a vCloud Usage Meter appliance with deactivated FIPS mode with a certificate signed by an internal Certificate Authority (CA), you must first import the CA to the appliance.

### Prerequisites

- Verify that you have access to the vCloud Usage Meter console as **usagemeter**.
- Verify that FIPS is deactivated for the vCloud Usage Meter appliance by navigating to **Settings > Security**.

### Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter** and stop all appliance services.

```
cd /opt/vmware/cloudusagemetering
```

```
./scripts/stop.sh All
```

```
sudo systemctl stop vmware-um-journal.service
```

```
sudo systemctl stop vmware-um-login.service
```

```
sudo systemctl stop vmware-um-schedule.service
```

## 2 Export the environment variables.

```
export $(grep -v '^#' "/opt/vmware/cloudusagemetering/platform/conf/env.properties" |
xargs)
```

## 3 Establish a trust between the vCloud Usage Meter appliance with deactivated FIPS mode and the certificate that is signed by the internal certificate authority.

Enter a name that identifies the certificate within the keystore under the **alias** property in the following command.

```
keytool -import -trustcacerts -file filepath-to-the-certificate -alias custom-internal-
certificate-authority -keystore /opt/vmware/cloudusagemetering/platform/security/cacerts
-storepass "${TRUST_STORE_PASSWORD}"
```

## 4 Reboot the vCloud Usage Meter appliance with deactivated FIPS mode.

```
sudo reboot
```

# Install a Certificate Authority (CA) - Signed Certificate for a vCloud Usage Meter Appliance with Enabled FIPS Mode

To establish a secure network connection to the vCloud Usage Meter Web interface, you can install a CA-signed SSL certificate on the vCloud Usage Meter appliance with enabled FIPS mode.

To obtain a CA-signed certificate and private key, you must generate a certificate signing request. The certificate authority uses the request to generate the official certificate.

### Prerequisites

- Verify that you have access to the vCloud Usage Meter console as **usagemeter**.
- From the certificate authority, obtain both the private key and the signed certificate. Both files must be in PEM format.
- Verify that FIPS is enabled for the vCloud Usage Meter appliance by navigating to **Settings > Security**.

### Procedure

- 1 If the certificate is signed by an internal certificate authority, you must first import the certificate authority in the vCloud Usage Meter appliance. For information, see [Import an Internal Certificate Authority \(CA\) - Signed Certificate for a vCloud Usage Meter Appliance with Enabled FIPS Mode](#).

- 2 Log in to the vCloud Usage Meter console as **usagemeter** and stop all appliance services.

```
cd /opt/vmware/cloudusagemetering

./scripts/stop.sh All

sudo systemctl stop vmware-um-journal.service

sudo systemctl stop vmware-um-login.service

sudo systemctl stop vmware-um-schedule.service
```

- 3 Export the environment variables.

```
export $(grep -v '^#' "/opt/vmware/cloudusagemetering/platform/conf/env.properties" |
xargs)
```

- 4 Back up the existing vCloud Usage Meter appliance certificate.

- a Back up the existing keystore.

```
mv /opt/vmware/cloudusagemetering/platform/security/keystore /opt/vmware/
cloudusagemetering/platform/security/keystore.backup
```

- b Move the existing keystore entry from the specified alias to a new alias that is under the *destalias* parameter.

---

**Note** If FIPS mode is deactivated for the vCloud Usage Meter, see [Install a Certificate Authority \(CA\) - Signed Certificate for a vCloud Usage Meter Appliance with Deactivated FIPS Mode](#).

---

```
keytool -changealias -alias "usage-meter-platform" -destalias "usage-meter-platform-
backup" -keystore /opt/vmware/cloudusagemetering/platform/security/cacerts -storetype
BCFKS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
-providerpath /opt/vmware/cloudusagemetering/platform/lib/bc-fips-1.0.2.1.jar
-storepass "${TRUST_STORE_PASSWORD}"
```

- 5 Import the CA-signed certificate and private key to the vCloud Usage Meter appliance.

- a Create a temporary directory and set the directory path to the *NGINX\_FOLDER* environment variable.

```
export NGINX_FOLDER=$(mktemp -d)
```

- b Create two temporary sub-directories within the temporary directory.

```
mkdir ${NGINX_FOLDER}/private
```

```
mkdir ${NGINX_FOLDER}/certs
```

- c Upload the CA - signed certificate to the `${NGINX_FOLDER}/certs/` folder and rename the file to `nginx-selfsigned.crt`.
  - d Upload the CA - signed private key to the `${NGINX_FOLDER}/private/` folder and rename the file to `nginx-selfsigned.key`.
- 6 Create a new keystore for the CA-signed certificate.

---

**Note** Make sure that you are in the `/opt/vmware/cloudusagemetering` directory.

---

```
./platform/bin/create-keystore.sh
```

- 7 (Optional) Remove all temporary and backup folders, and delete the old vCloud Usage Meter certificate.

```
rm -rf $NGINX_FOLDER
```

```
rm /opt/vmware/cloudusagemetering/platform/security/keystore.backup
```

```
keytool -delete -alias "usage-meter-platform-backup" -keystore /opt/vmware/
cloudusagemetering/platform/security/cacerts -storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath /opt/vmware/
cloudusagemetering/platform/lib/bc-fips-1.0.2.1.jar -storepass "${TRUST_STORE_PASSWORD}"
```

- 8 Configure the permissions for the keystore.

```
chmod 0640 /opt/vmware/cloudusagemetering/platform/security/keystore
```

- 9 Reboot the vCloud Usage Meter appliance.

```
sudo reboot
```

If the installation of the CA-signed SSL certificate on the vCloud Usage Meter appliance is successful, no security warning is displayed the next time you log in to the vCloud Usage Meter Web interface.

## Install a Certificate Authority (CA) - Signed Certificate for a vCloud Usage Meter Appliance with Deactivated FIPS Mode

To establish a secure network connection to the vCloud Usage Meter Web interface, you can install a CA-signed SSL certificate on the vCloud Usage Meter appliance with deactivated FIPS mode.

To obtain a CA-signed certificate and private key, you must generate a certificate signing request. The certificate authority uses the request to generate the official certificate.

### Prerequisites

- Verify that you have access to the vCloud Usage Meter console as **usagemeter**.

- From the certificate authority, obtain both the private key and the signed certificate. Both files must be in PEM format.
- Verify that FIPS is deactivated for the vCloud Usage Meter appliance by navigating to **Settings > Security**.

### Procedure

- 1 If the certificate is signed by an internal certificate authority, you must first import the certificate authority in the vCloud Usage Meter appliance with deactivated FIPS. For information, see [Import an Internal Certificate Authority \(CA\) - Signed Certificate for a vCloud Usage Meter Appliance with Deactivated FIPS Mode](#).

- 2 Log in to the vCloud Usage Meter console as **usagemeter** and stop all appliance services.

```
cd /opt/vmware/cloudusagemetering
```

```
./scripts/stop.sh All
```

```
sudo systemctl stop vmware-um-journal.service
```

```
sudo systemctl stop vmware-um-login.service
```

```
sudo systemctl stop vmware-um-schedule.service
```

- 3 Export the environment variables.

```
export $(grep -v '^#' "/opt/vmware/cloudusagemetering/platform/conf/env.properties" | xargs)
```

- 4 Back up the existing vCloud Usage Meter appliance certificate.

- a Back up the existing keystore.

```
mv /opt/vmware/cloudusagemetering/platform/security/keystore /opt/vmware/cloudusagemetering/platform/security/keystore.backup
```

- b Move the existing keystore entry from the specified alias to a new alias that is under the *destalias* parameter.

```
keytool -changealias -alias "usage-meter-platform" -destalias "usage-meter-platform-backup" -keystore /opt/vmware/cloudusagemetering/platform/security/cacerts -storepass "${TRUST_STORE_PASSWORD}"
```



- 5 Import the CA-signed certificate with deactivated FIPS mode and private key to the vCloud Usage Meter appliance with deactivated FIPS mode.

- a Create a temporary directory and set the directory path to the `NGINX_FOLDER` environment variable.

```
export NGINX_FOLDER=$(mktemp -d)
```

- b Create two temporary sub-directories within the temporary directory.

```
mkdir ${NGINX_FOLDER}/private
```

```
mkdir ${NGINX_FOLDER}/certs
```

- c Upload the CA - signed certificate to the `${NGINX_FOLDER}/certs/` folder and rename the file to `nginx-selfsigned.crt`.
- d Upload the CA - signed private key to the `${NGINX_FOLDER}/private/` folder and rename the file to `nginx-selfsigned.key`.

- 6 Create a new keystore for the CA-signed certificate.

---

**Note** Make sure that you are in the `/opt/vmware/cloudusagemetering` directory.

---

```
./platform/bin/create-keystore.sh
```

- 7 (Optional) Remove all temporary and backup folders, and delete the old vCloud Usage Meter certificate.

```
rm -rf $NGINX_FOLDER
```

```
rm /opt/vmware/cloudusagemetering/platform/security/keystore.backup
```

```
keytool -delete -alias "usage-meter-platform-backup" -keystore /opt/vmware/cloudusagemetering/platform/security/cacerts -storepass "${TRUST_STORE_PASSWORD}"
```

- 8 Configure the permissions for the keystore.

```
chmod 0640 /opt/vmware/cloudusagemetering/platform/security/keystore
```

- 9 Reboot the vCloud Usage Meter appliance with deactivated FIPS mode.

```
sudo reboot
```

If the installation of the CA-signed SSL certificate on the vCloud Usage Meter appliance with deactivated FIPS mode is successful, no security warning is displayed the next time you log in to the vCloud Usage Meter Web interface.

# Replace the Default Appliance Self-Signed SSL Certificate With a New Self-Signed Certificate for a vCloud Usage Meter appliance with enabled FIPS mode

You can replace the default self-signed certificate for a vCloud Usage Meter appliance with enabled FIPS mode by generating and installing a new self-signed certificate.

## Prerequisites

- Verify that you have access to the vCloud Usage Meter console as **usagemeter**.
- Verify that FIPS is enabled for the vCloud Usage Meter appliance by navigating to **Settings > Security**.

## Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter** and stop all appliance services.

```
cd /opt/vmware/cloudusagemetering

./scripts/stop.sh All

sudo systemctl stop vmware-um-journal.service

sudo systemctl stop vmware-um-login.service

sudo systemctl stop vmware-um-schedule.service
```

- 2 Export the environment variables.

```
export $(grep -v '^#' "/opt/vmware/cloudusagemetering/platform/conf/env.properties" |
xargs)
```

- 3 Back up the existing vCloud Usage Meter appliance certificate.

- a Back up the existing keystore.

```
mv /opt/vmware/cloudusagemetering/platform/security/keystore /opt/vmware/
cloudusagemetering/platform/security/keystore.backup
```

- b Move the existing keystore entry from the specified alias to a new alias that is under the *destalias* parameter.

```
keytool -changealias -alias "usage-meter-platform" -destalias "usage-meter-platform-
backup" -keystore /opt/vmware/cloudusagemetering/platform/security/cacerts -storetype
BCFKS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
-providerpath /opt/vmware/cloudusagemetering/platform/lib/bc-fips-1.0.2.1.jar
-storepass "${TRUST_STORE_PASSWORD}"
```

- 4 Create a temporary directory and set the directory path to the `NGINX_FOLDER` environment variable.

```
export NGINX_FOLDER=$(mktemp -d)
```

- 5 Create a keystore for the new self-signed certificate.

---

**Note** Make sure that you are in the `/opt/vmware/cloudusagemetering` directory.

---

```
./platform/bin/create-keystore.sh
```

- 6 (Optional) Remove all temporary and backup folders, and delete the old vCloud Usage Meter certificate.

```
rm -rf $NGINX_FOLDER
```

```
rm /opt/vmware/cloudusagemetering/platform/security/keystore.backup
```

```
keytool -delete -alias "usage-meter-platform-backup" -keystore /opt/vmware/
cloudusagemetering/platform/security/cacerts -storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath /opt/vmware/
cloudusagemetering/platform/lib/bc-fips-1.0.2.1.jar -storepass "${TRUST_STORE_PASSWORD}"
```

- 7 Configure the permissions for the keystore.

```
chmod 0640 /opt/vmware/cloudusagemetering/platform/security/keystore
```

- 8 Reboot the vCloud Usage Meter appliance with enabled FIPS mode.

```
sudo reboot
```

## Replace the Default Appliance Self-Signed SSL Certificate With a New Self-Signed Certificate for a vCloud Usage Meter appliance with deactivated FIPS mode

You can replace the default self-signed certificate for a vCloud Usage Meter appliance with deactivated FIPS mode by generating and installing a new self-signed certificate.

### Prerequisites

- Verify that you have access to the vCloud Usage Meter console as **usagemeter**.
- Verify that FIPS is deactivated for the vCloud Usage Meter appliance by navigating to **Settings > Security**.

## Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter** and stop all appliance services.

```
cd /opt/vmware/cloudusagemetering
```

```
./scripts/stop.sh All
```

```
sudo systemctl stop vmware-um-journal.service
```

```
sudo systemctl stop vmware-um-login.service
```

```
sudo systemctl stop vmware-um-schedule.service
```

- 2 Export the environment variables.

```
export $(grep -v '^#' "/opt/vmware/cloudusagemetering/platform/conf/env.properties" |
xargs)
```

- 3 Back up the existing vCloud Usage Meter appliance certificate.

- a Back up the existing keystore.

```
mv /opt/vmware/cloudusagemetering/platform/security/keystore /opt/vmware/
cloudusagemetering/platform/security/keystore.backup
```

- b Move the existing keystore entry from the specified alias to a new alias that is under the *destalias* parameter.

```
keytool -changealias -alias "usage-meter-platform" -destalias "usage-meter-platform-
backup" -keystore /opt/vmware/cloudusagemetering/platform/security/cacerts -storepass
"${TRUST_STORE_PASSWORD}"
```

- 4 Create a temporary directory and set the directory path to the *NGINX\_FOLDER* environment variable.

```
export NGINX_FOLDER=$(mktemp -d)
```

- 5 Create a keystore for the new self-signed certificate.

---

**Note** Make sure that you are in the `/opt/vmware/cloudusagemetering` directory.

---

```
./platform/bin/create-keystore.sh
```

- 6 (Optional) Remove all temporary and backup folders, and delete the old vCloud Usage Meter certificate.

```
rm -rf $NGINX_FOLDER
```

```
rm /opt/vmware/cloudusagemetering/platform/security/keystore.backup
```

```
keytool -delete -alias "usage-meter-platform-backup" -keystore /opt/vmware/  
cloudusagemetering/platform/security/cacerts -storepass "${TRUST_STORE_PASSWORD}"
```

- 7 Configure the permissions for the keystore.

```
chmod 0640 /opt/vmware/cloudusagemetering/platform/security/keystore
```

- 8 Reboot the vCloud Usage Meter appliance with deactivated FIPS mode.

```
sudo reboot
```

## Import a Certificate to the vCloud Usage Meter Appliance Keystore when FIPS Mode is Enabled

If the instance you want to add for metering uses network and security configuration entities such as load balancer, proxy, or firewall, or you use proxy over HTTPS or SMTP over SSL/TLS, you must import their certificates to the vCloud Usage Meter appliance keystore.

To import the certificate of a network and security configuration entity to the vCloud Usage Meter appliance keystore, you must obtain the password of the truststore. The password is located at `/opt/vmware/cloudusagemetering/conf/env.properties`.

### Prerequisites

- Verify that you have access to the vCloud Usage Meter appliance as **usagemeter**.
- Verify that FIPS is enabled for the vCloud Usage Meter appliance by navigating to **Settings > Security**.

## Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter** and stop all appliance services.

```
cd /opt/vmware/cloudusagemetering
```

```
./scripts/stop.sh All
```

```
sudo systemctl stop vmware-um-journal.service
```

```
sudo systemctl stop vmware-um-login.service
```

```
sudo systemctl stop vmware-um-schedule.service
```

- 2 To extract the truststore password in an environment variable, run the following command.

```
export $(grep -v '^#' "/opt/vmware/cloudusagemetering/platform/conf/env.properties" | xargs)
```

- 3 To import the certificate to the vCloud Usage Meter appliance keystore, run the following command.

```
keytool -import -trustcacerts -alias certificate-alias -file certificate-file -keystore /opt/vmware/cloudusagemetering/resources/cacerts -storetype bcfks -storepass "${TRUST_STORE_PASSWORD}" -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath /opt/vmware/cloudusagemetering/jars/bc-fips-*.jar
```

- 4 Reboot the vCloud Usage Meter appliance with enabled FIPS mode.

```
sudo reboot
```

## Import a Certificate to the vCloud Usage Meter Appliance Keystore when FIPS Mode is Deactivated

If the instance you want to add for metering uses network and security configuration entities such as load balancer, proxy, or firewall, or you use proxy over HTTPS or SMTP over SSL/TLS and FIPS is disabled for the appliance, you must import their certificates to the vCloud Usage Meter appliance keystore.

To import the certificate of a network and security configuration entity to the vCloud Usage Meter appliance keystore, you must obtain the password of the truststore. The password is located at `/opt/vmware/cloudusagemetering/conf/env.properties`.

### Prerequisites

- Verify that you have access to the vCloud Usage Meter appliance as **usagemeter**.

- Verify that FIPS is deactivated for the vCloud Usage Meter appliance by navigating to **Settings > Security**.

#### Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter** and stop all appliance services.

```
cd /opt/vmware/cloudusagemetering
```

```
./scripts/stop.sh All
```

```
sudo systemctl stop vmware-um-journal.service
```

```
sudo systemctl stop vmware-um-login.service
```

```
sudo systemctl stop vmware-um-schedule.service
```

- 2 To extract the trustore password in an environment variable, run the following command.

```
export $(grep -v '^#' "/opt/vmware/cloudusagemetering/platform/conf/env.properties" |  
xargs)
```

- 3 To import the certificate to the vCloud Usage Meter appliance keystore, run the following command.

```
keytool -import -trustcacerts -alias certificate-alias -file certificate-file -keystore  
/opt/vmware/cloudusagemetering/resources/cacerts -storepass "${TRUST_STORE_PASSWORD}"
```

- 4 Reboot the vCloud Usage Meter appliance with deactivated FIPS mode.

```
sudo reboot
```

# Managing the Metering in vCloud Usage Meter

# 7

You must provide and maintain certain details for vCloud Usage Meter to collect product consumption data from vCenter Server instances. These details include the host name and credentials.

vCloud Usage Meter automatically detects and meters vSAN product consumption data after you add the vCenter Server instance on which you activated vSAN. vCloud Usage Meter also detects the vSAN edition based on a use of features. vCloud Usage Meter collects usage information on an hourly basis at the cluster level and it is averaged over the month in which the use occurs. The consumption information for individual virtual machines is not available. For information about adding a vCenter Server instance, see [Assign Permissions for vCenter Server for Metering with vCloud Usage Meter](#) and [Add a vCenter Server Instance for Metering in vCloud Usage Meter](#).

vCloud Usage Meter automatically detects vSphere with Tanzu after you add the vCenter Server instance on which you activated vSphere with Tanzu. The default selected edition for vSphere with Tanzu is **Basic**. For information about adding a vCenter Server instance, see [Assign Permissions for vCenter Server for Metering with vCloud Usage Meter](#) and [Add a vCenter Server Instance for Metering in vCloud Usage Meter](#).

## Reverse Proxy

vCloud Usage Meter 4.7 supports the registration and metering of product servers with different FQDN but using the same IP address behind a reverse proxy. The metering of such product servers is redirected to different endpoints located behind the proxy.

## Certificate Management

If the instance you want to add for metering uses network and security configuration entities such as load balancer, proxy, or firewall, or you use proxy over HTTPS, you must import their certificates to the vCloud Usage Meter appliance keystore. For more information, see [Chapter 6 vCloud Usage Meter Certificate Management](#).

- [Assign Permissions for vCenter Server for Metering with vCloud Usage Meter](#)

To begin metering with vCloud Usage Meter, you must add at least one vCenter Server instance. You must assign additional profile-driven storage privileges to your read-only vCenter Server user beforehand.



- [Add a vCenter Server Instance for Metering in vCloud Usage Meter](#)

To begin metering with vCloud Usage Meter, you must add at least one vCenter Server instance.

- [Add a VMware Cloud Foundation Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of VMware Cloud Foundation in vCloud Usage Meter, you must add the vCenter Server instance associated with the VMware Cloud Foundation instance.

- [Add a Site Recovery Manager Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of Site Recovery Manager in vCloud Usage Meter, you must add the vCenter Server instance associated with the Site Recovery Manager instance.

- [Add a Tanzu Kubernetes Grid Management Cluster for Metering in vCloud Usage Meter](#)

To meter the product consumption data of Tanzu Kubernetes Grid in vCloud Usage Meter, you must add the Tanzu Kubernetes Grid management cluster for metering.

- [Add a VMware Cloud Director Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of vCloud Director 9.7 or a later version, you must add the product instance to vCloud Usage Meter.

- [Add a vRealize Suite Lifecycle Manager Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of vRealize Automation 8.x, vRealize Operations, and vRealize Network Insight, you must add the associated vRealize Suite Lifecycle Manager instance (rebranded as VMware Aria Suite Lifecycle) to vCloud Usage Meter.

- [Metering vRealize Operations with vCloud Usage Meter](#)

If you associate a vRealize Operations (rebranded to Aria Operations) server with a vCenter Server instance that you added for metering, vCloud Usage Meter detects the vRealize Operations and displays the servers in the vCloud Usage Meter Web interface.

- [Add a vRealize Automation 7 Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of vRealize Automation, you must add the vRealize Automation 7.x instance to vCloud Usage Meter.

- [Add a vRealize Automation 8 Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of vRealize Automation 8.x, you must add the vRealize Suite Lifecycle Manager associated with the vRealize Automation 8.x instance in vCloud Usage Meter.

- [Add an NSX Data Center for vSphere Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of NSX Data Center for vSphere, you must add the NSX-V Manager instance to vCloud Usage Meter.

- [Add an NSX-T Data Center Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of NSX-T Data Center, you must add the NSX-T Manager instance to vCloud Usage Meter.

- [Add a vRealize Network Insight Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of vRealize Network Insight (rebranded as Aria Operations for Networks), you must add the vRealize Network Insight instance to vCloud Usage Meter.

- [Add a NSX Advanced Load Balancer Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of NSX Advanced Load Balancer, you must add the NSX Advanced Load Balancer instance to vCloud Usage Meter.

- [Add a VMware Cloud Director Availability Instance for Metering in vCloud Usage Meter](#)

To meter the product consumption data of VMware Cloud Director Availability, you must add the product instance to vCloud Usage Meter.

- [Configure the Level of Anonymization of vCloud Usage Meter Reports](#)

To hide sensitive data like virtual machine name, host name, and user name, you can anonymize the data transferred between vCloud Usage Meter and VMware Cloud Services Console. In the vCloud Usage Meter Web interface, you can configure the hashing level of the generated vCloud Usage Meter product consumption reports.

- [Edit Product Information in vCloud Usage Meter](#)

After you added product instances for metering in vCloud Usage Meter , you can edit the username and the password for the instance.

- [Delete Product Servers in vCloud Usage Meter](#)

You can delete product servers that are no longer in use.

- [Change the vCloud Usage Meter Logging Level](#)

You can change the logging level of vCloud Usage Meter to collect more details.

## Assign Permissions for vCenter Server for Metering with vCloud Usage Meter

To begin metering with vCloud Usage Meter, you must add at least one vCenter Server instance. You must assign additional profile-driven storage privileges to your read-only vCenter Server user beforehand.

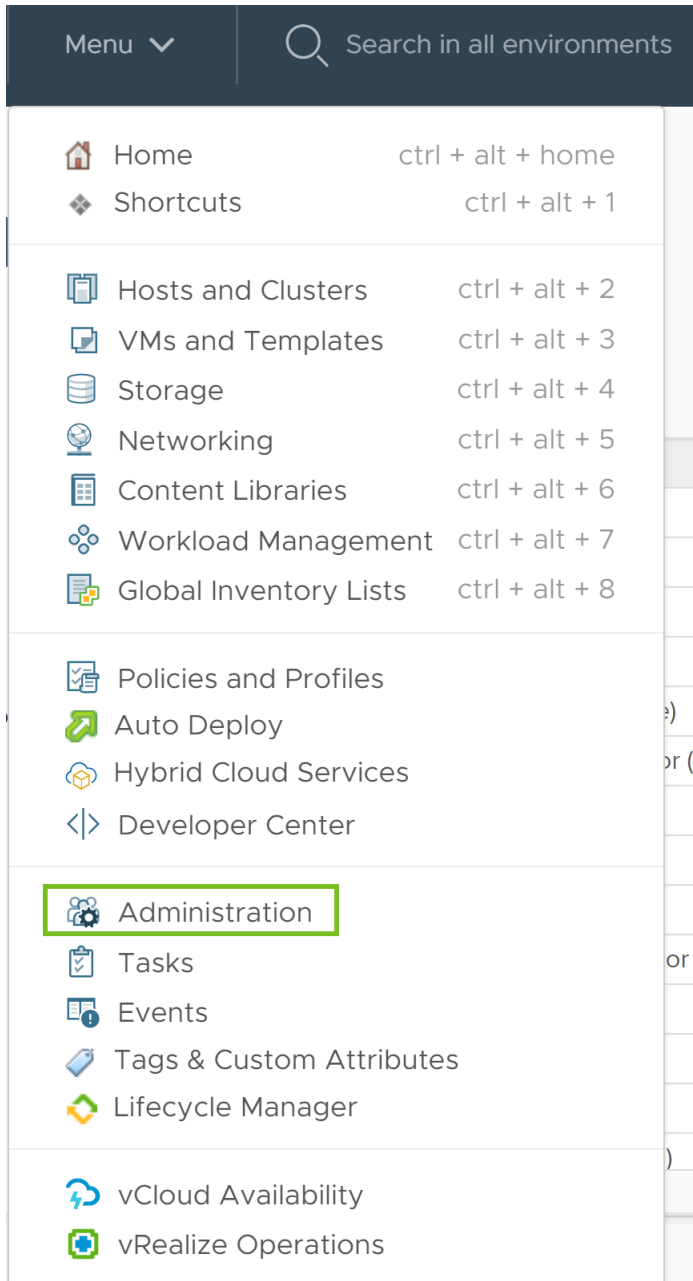
### Prerequisites

- Verify that the vSphere administrator is not assigned with conflicting vCenter Server roles.
- Assign vCenter Server permissions at either a Global level or to an object in the object hierarchy.

To ensure the successful billing, you must assign a permission for viewing and managing product license keys. For full information and best practices about authorization in vSphere Web Client, see *vSphere Permissions and User Management Tasks* in the *vSphere Security* guide.

**Procedure**

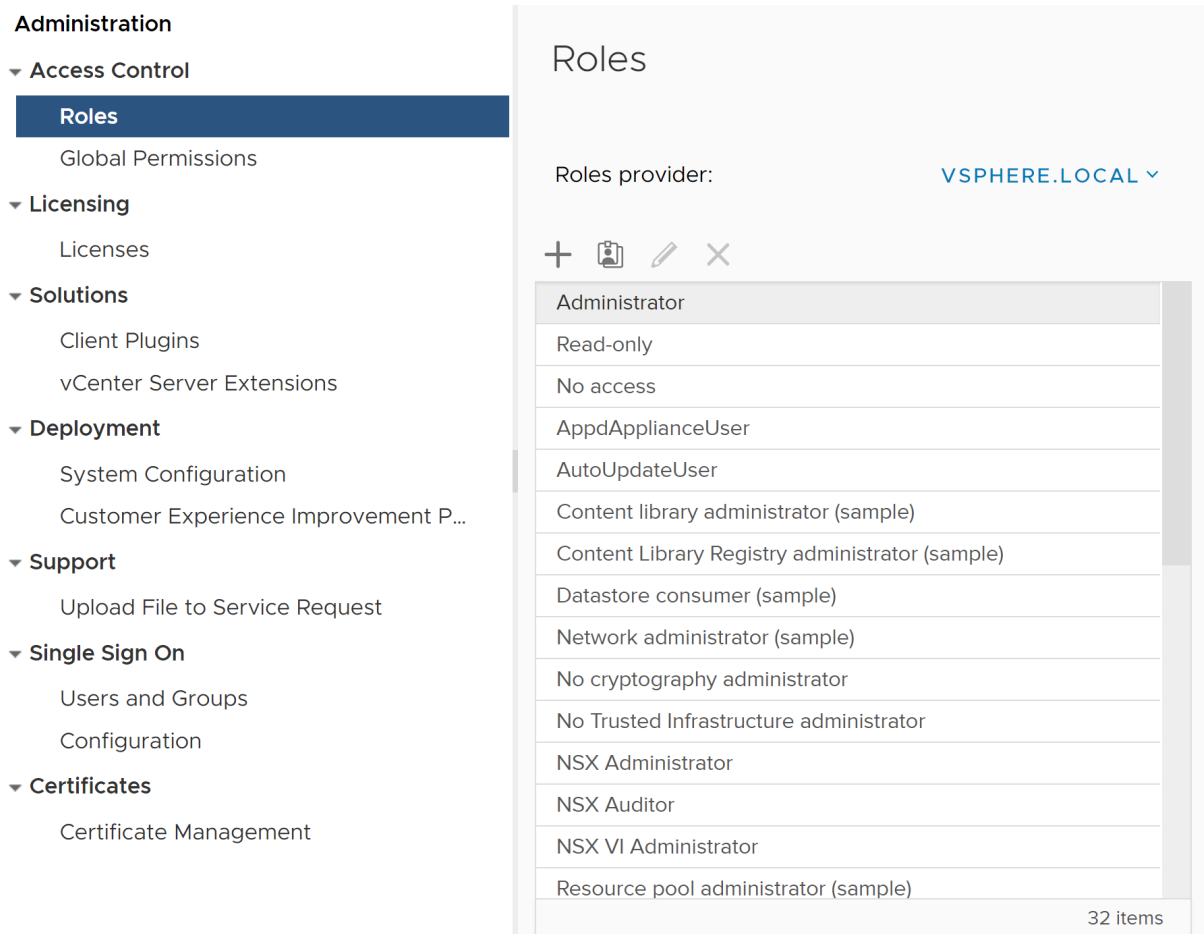
- 1 Log in to the vSphere Web Client with your administrator credentials.
- 2 Navigate to **Menu > Administration**.



The **Roles** page opens.

- 3 (Optional) From the **Administration** left pane, select **Roles**.

- 4 Click the **Create role** (  ) action button.






**Administration**

- ▼ Access Control
  - Roles**
  - Global Permissions
- ▼ Licensing
  - Licenses
- ▼ Solutions
  - Client Plugins
  - vCenter Server Extensions
- ▼ Deployment
  - System Configuration
  - Customer Experience Improvement P...
- ▼ Support
  - Upload File to Service Request
- ▼ Single Sign On
  - Users and Groups
  - Configuration
- ▼ Certificates
  - Certificate Management

**Roles**

Roles provider: **VSPHERE.LOCAL** ▼

+   

Administrator
Read-only
No access
AppdApplianceUser
AutoUpdateUser
Content library administrator (sample)
Content Library Registry administrator (sample)
Datastore consumer (sample)
Network administrator (sample)
No cryptography administrator
No Trusted Infrastructure administrator
NSX Administrator
NSX Auditor
NSX VI Administrator
Resource pool administrator (sample)

32 items

- 5 Assign the following permissions.
- a Set the storage privileges.
    - For vCenter Server versions 8.x, select **VM storage policies > View VM storage policies**
    - For vCenter Server versions 7.x, select **Profile-driven storage > Profile-driven storage view.** >
  - b To allow managing and viewing license keys, select **Global > Licences.**
  - c If the vCenter Server instance has vSAN enabled, select **Cns > Searchable.**
  - d Click **Next.**
- 6 Enter a name and a description for the new role and click **Finish.**
- 7 Assign the new role to the user which you use for vCloud Usage Meter collection.

### Results

The server adds the selected permissions to the vCenter Server user.

# Add a vCenter Server Instance for Metering in vCloud Usage Meter

To begin metering with vCloud Usage Meter, you must add at least one vCenter Server instance.

## Prerequisites

- Verify that a single vRealize Operations Manager instance manages the vCenter Server instance that you add. vCloud Usage Meter cannot collect accurate product consumption data when multiple vRealize Operations Manager servers manage a single vCenter Server instance.
- To activate vCloud Usage Meter for metering of vSphere with Tanzu product consumption data, configure the respective permissions. For information, see the <https://kb.vmware.com/s/article/85481>.

## Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, select **Cloud > vCenter / Cloud Foundation**.
- 3 On the **vCenter / Cloud Foundation** page, click **Add**.
- 4 In the **Endpoint** text box, enter the host name or IP address of the vCenter Server instance.  
The default port number is 443.
- 5 In the **Username** and **Password** text boxes, enter the credentials of a vCenter Single Sign-On user, such as administrator@vsphere.local.
- 6 (Optional) If you use an external Platform Services Controller, select the **Use External Platform Services Controller (PSC)** check box.
  - a In the **PSC Endpoint** text box, enter the IP address or host name of the external Platform Services Controller.
  - b Enter the port number for the external Platform Services Controller.  
The default port number is 7444.
- 7 (Optional) From the **Managed by VMware Cloud Foundation (VCF) Edition** drop-down menu, select the VMware Cloud Foundation edition.
  - **Not managed by VCF**
  - **SDDC Manager (vRAM)**
  - **Standard (core)**
  - **Advanced (core)**
  - **Enterprise(core)**
  - **Standard w/o vSAN (core)**

- **Advanced w/o vSAN (core)**
- **Enterprise w/o vSAN (core)**

If you select **Not managed by VCF**, vCloud Usage Meter does not meter the product consumption data of VMware Cloud Foundation.

- 8 (Optional) Confirm if vCloud Usage Meter must meter the virtual machines that are protected by all Site Recovery Manager instances, associated with the registered vCenter Server instance.

To deactivate the metering of Site Recovery Manager, deselect the **Meter VMs protected by all SRMs** check box.

- 9 (Optional) If vSphere with Tanzu is activated on the vCenter Server instance, select the Tanzu edition and whether vCloud Usage Meter must meter based on vRAM or CPU.

- Basic
- Standard
- Advanced

By default, the **Basic** edition is selected.

- 10 Click **Add**.

For each vCenter Server instance that you add, vCloud Usage Meter presents a certificate that you must accept before proceeding.

- 11 To accept the certificate, on the **vCenter / Cloud Foundation** page, select the vCenter Server instance, and in the **Status** column, click **Please accept certificate**.

### Results

The vCenter Server instance is added for metering to the list of vCenter Server instances.

If an error occurs, the **vCenter / Cloud Foundation** page displays an error message and vCloud Usage Meter does not collect product consumption data from the vCenter Server instance.

vCloud Usage Meter collects product consumption data from all vCenter Server instances that you add.

## Add a VMware Cloud Foundation Instance for Metering in vCloud Usage Meter

To meter the product consumption data of VMware Cloud Foundation in vCloud Usage Meter, you must add the vCenter Server instance associated with the VMware Cloud Foundation instance.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, select **Cloud > vCenter / Cloud Foundation**.

- 3 On the **vCenter / Cloud Foundation** page, click **Add**.
- 4 In the **Endpoint** text box, enter the host name or IP address of the vCenter Server instance.  
The default port number is 443.
- 5 In the **Username** and **Password** text boxes, enter the credentials of a vCenter Single Sign-On user, such as administrator@vsphere.local.
- 6 (Optional) If you use an external Platform Services Controller, select the **Use External Platform Services Controller (PSC)** check box.
  - a In the **PSC Endpoint** text box, enter the IP address or host name of the external Platform Services Controller.
  - b Enter the port number for the external Platform Services Controller.  
The default port number is 7444.
- 7 From the **Managed by VMware Cloud Foundation (VCF) Edition** drop-down menu, select the VMware Cloud Foundation edition.
  - **Not managed by VCF**
  - **SDDC Manager (vRAM)**
  - **Standard (core)**
  - **Advanced (core)**
  - **Enterprise(core)**
  - **Standard w/o vSAN (core)**
  - **Advanced w/o vSAN (core)**
  - **Enterprise w/o vSAN (core)**
- 8 Click **Add**.

## Add a Site Recovery Manager Instance for Metering in vCloud Usage Meter

To meter the product consumption data of Site Recovery Manager in vCloud Usage Meter, you must add the vCenter Server instance associated with the Site Recovery Manager instance.

If Site Recovery Manager is protecting a vCenter Server instance that you add for metering, vCloud Usage Meter automatically detects the Site Recovery Manager instance.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, select **Cloud > vCenter / Cloud Foundation**.
- 3 On the **vCenter / Cloud Foundation** page, click **Add**.

- 4 In the **Endpoint** text box, enter the host name or IP address of the vCenter Server instance.  
The default port number is 443.
- 5 In the **Username** and **Password** text boxes, enter the credentials of a vCenter Single Sign-On user, such as administrator@vsphere.local.
- 6 (Optional) If you use an external Platform Services Controller, select the **Use External Platform Services Controller (PSC)** check box.
  - a In the **PSC Endpoint** text box, enter the IP address or host name of the external Platform Services Controller.
  - b Enter the port number for the external Platform Services Controller.  
The default port number is 7444.
- 7 From the **Managed by VMware Cloud Foundation (VCF) Edition** drop-down menu, select **Not Managed by VCF**.
- 8 Confirm if virtual machines protected by all Site Recovery Manager instances, associated with the vCenter Server instance, must be metered.  
By default, the checkbox is selected.
- 9 Click **Add**.

## Add a Tanzu Kubernetes Grid Management Cluster for Metering in vCloud Usage Meter

To meter the product consumption data of Tanzu Kubernetes Grid in vCloud Usage Meter, you must add the Tanzu Kubernetes Grid management cluster for metering.

### Prerequisites

- Verify that the vCenter Server instance associated with the Tanzu Kubernetes Grid management cluster is part of the vCloud Usage Meter list of vCenter Server instances.
- Obtain a bearer token by setting up a service account metering user with Tanzu Kubernetes Grid. For information, see [Obtain a Bearer Token for a Tanzu Kubernetes Grid Management Cluster](#).

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, navigate to **Cloud > Tanzu Kubernetes Grid Multi-cloud**.
- 3 Click **Add**.  
The **Add a Tanzu Kubernetes Grid Multi-cloud (TKGm)** wizard opens.
- 4 From the **vCenter Endpoint** drop-down menu, select the IP address of the vCenter Server instance associated with the Tanzu Kubernetes Grid management cluster.



- 5 In the **Endpoint** text box, enter the host name or the IP address of a control plane virtual machine that is part of the management cluster.

---

**Note** Consider the following factors:

- A load balancer IP rotates the certificates depending on the destination node. If you enter a load balancer IP, you must accept the product certificate every time vCloud Usage Meter collects product consumption data.
  - Ensure that the control plane virtual machine will not be deleted during a scale down of the cluster.
- 
- 6 In the **Bearer token** text box, enter the bearer token you obtain from the Tanzu Kubernetes Grid management cluster.
  - 7 From the **Edition** drop-down menu, select the Tanzu Kubernetes Grid edition.
    - Basic
    - Standard
    - Advanced
  - 8 From the **Metric** drop-down menu, select whether vCloud Usage Meter must meter based on vRAM or CPU cores.

#### Results

Tanzu Kubernetes Grid is now part of the management clusters vCloud Usage Meter meters. If an error occurs, an error message appears in the **Status** column in the Tanzu Kubernetes Grid list of management clusters.

## Obtain a Bearer Token for a Tanzu Kubernetes Grid Management Cluster

To add a Tanzu Kubernetes Grid management cluster for metering, you must obtain a bearer token.

To obtain a bearer token for a Tanzu Kubernetes Grid management cluster, you must set up a service metering user with a cluster role. You must create two separate YAML files for the user and the cluster role.

#### Prerequisites

Obtain the credentials of the Tanzu Kubernetes Grid management cluster. For information, see *Retrieve Tanzu Kubernetes Cluster kubeconfig* in *VMware Tanzu Kubernetes Grid 1.5 Documentation*.

## Procedure

- 1 Create a YAML file and enter the user metadata.

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: user
  namespace: tkg-system
```

- 2 To update the resources of the Tanzu Kubernetes Grid management cluster with the created user, run the command.

```
kubectl apply -f user-filename.yaml
```

- 3 To grant a cluster role to the user, create a YAML file.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: user
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: user
  namespace: tkg-system
```

- 4 To update the resources of the Tanzu Kubernetes Grid management cluster with the granted cluster role to the user, run the command.

```
kubectl apply -f user-role-filename.yaml
```

- 5 List all the secrets in the *tkg-system* namespace.

```
kubectl get secret -n tkg-system
```

You can see the list of all the secrets in the *tkg-system* namespace. The created bearer token has the following name pattern *user-token-Kubernetes-generated-string* and type *kubernetes.io/service-account-token*, where *user* is the entered name for the user and *Kubernetes-generated-string* is a Kubernetes-system generated string that uniquely identifies the bearer token.

- 6 To get the bearer token, run the command.

```
kubectl get secret user-token-Kubernetes-generated-string -o yaml -n tkg-system
```

## 7 Decode the bearer token.

```
echo bearer-token | base64 --decode
```

# Add a VMware Cloud Director Instance for Metering in vCloud Usage Meter

To meter the product consumption data of vCloud Director 9.7 or a later version, you must add the product instance to vCloud Usage Meter.

For the most recent information about compatibility between vCloud Usage Meter and VMware Cloud Director, see the [VMware Product Interoperability Matrix](#).

### Prerequisites

- Verify that you have system administrator privileges.
- Register in vCloud Usage Meter the vCenter Server instance associated with the vCloud Director instance that you want to add for metering.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, select **Cloud > Cloud Director**.
- 3 On the **Cloud Director** page, click **Add**.
- 4 In the **Endpoint** text box, enter the host name or IP address of the vCloud Director or VMware Cloud Director instance that you want to add.
- 5 In the **Username** and **Password** text boxes, enter the credentials of a **VMware Cloud Director** user.
- 6 Click **Add**.

### Results

The product is part of the list of instances. If an error occurs, a message appears in the Status column in the **Cloud Director** list of instances.

# Add a vRealize Suite Lifecycle Manager Instance for Metering in vCloud Usage Meter

To meter the product consumption data of vRealize Automation 8.x, vRealize Operations, and vRealize Network Insight, you must add the associated vRealize Suite Lifecycle Manager instance (rebranded as VMware Aria Suite Lifecycle) to vCloud Usage Meter.

## Prerequisites

- Verify that you have a local vRealize Suite Lifecycle Manager user account with the **LCM Admin** or the **LCM Cloud Admin** supported role available.

---

**Note** vCloud Usage Meter supports only local user accounts for the metering of vRealize Suite Lifecycle Manager.

---

- Verify that you can log in to the administration user interface of the vRealize Suite Lifecycle Manager appliance.

## Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left navigation pane, click **Management > vRealize Suite Lifecycle Manager**.
- 3 On the **vRealize Suite Lifecycle Manager (vRSLCM)** page, click **Add** .  
The **Add Endpoint for vRealize Suite Lifecycle Manager (vRSLCM)** wizard opens.
- 4 Provide the endpoint for the vRealize Suite Lifecycle Manager instance.
  - a In the **Endpoint** text box, enter the host name or IP address for the vRealize Suite Lifecycle Manager instance.  
The default port number is 443.
  - b In the **Username** and **Password** text boxes, provide the credentials for a vRealize Suite Lifecycle Manager user with an **LCM Admin** or an **LCM Cloud Admin** role.

---

**Note** Provide the full username with the local domain, such as *user@local*.

---

  - c Click **Next**.
- 5 On the **Accept Certificate** page, verify the SSL certificate details for the vRealize Suite Lifecycle Manager instance and click **Accept & Next**.
- 6 On the **Discovering Products and Environments** page, verify the details for the discovered products and click **Next**.

Status	Description
Test Credentials	vCloud Usage Meter validates the username and password that you enter when you provide endpoint for the vRealize Suite Lifecycle Manager instance. If the validation is successful, you proceed with the wizard. In case of a failure, you receive an alert message. You must go back and provide the correct credentials.
Get Deployed Environments & Products	vCloud Usage Meter fetches list of environment(s) created in the vRealize Suite Lifecycle Manager instance and the installed or imported product(s) in the environment(s). If the fetching is successful, you proceed with the wizard. In case of a failure, you receive an alert message.

Status	Description
Get Product(s) Certificates	vCloud Usage Meter fetches the details about the SSL certificate(s) for the managed products from the vRealize Suite Lifecycle Manager instance locker. If the vRealize Suite Lifecycle Manager instance locker can provide the SSL certificate(s) for the product then the the system automatically accepts the certificate. If the vRealize Suite Lifecycle Manager instance locker cannot provide the certificate(s) for the product they must be trusted and accepted explicitly after the addition of the managed product to the vCloud Usage Meter. If the fetching is successful, you proceed with the wizard. In case of a failure, you receive an alert message.
Preparing Product Registration	vCloud Usage Meter collects and prepares the managed product instance(s) metadata to be used while metering the product consumption data of the supported vRealize Suite Products. vCloud Usage Meter identifies existing product instance(s) added to the vCloud Usage Meter and the new ones being imported through the vRealize Suite Lifecycle Manager instance. If the validation is successful, you proceed with the wizard. In case of a failure, you receive an alert message.

- 7 On the **Review Environment** page, verify the information about the discovered products that vRealize Suite Lifecycle Manager manages and click **Next**.

Consider the following factors:

- The discovered products must be associated with the respective vRealize Suite Lifecycle Manager instance.
- Check the total number of environments and the total number of unique products across the environments for the vRealize Suite Lifecycle Manager instance.
- The wizard must display the following information for every discovered product.

Parameter	Description
Product	The name of the vCloud Usage Meter supported product type. If vCloud Usage Meter does not support the product and does not meter the product consumption data, the displayed product type is what vRealize Suite Lifecycle Manager provides.
Endpoint	The FQDN/IP and the port of the managed product instance.
Registration Type	<p>The registration type can have the following values: <code>New Registration</code> (indicating a new supported product), <code>Existing Registration</code> (indicating an existing supported product) and <code>Not Supported</code> (indicating an unsupported product).</p> <p><b>Note</b> vRealize Suite Lifecycle Manager does not support vRealize Automation 7.x . The displayed registration type value is <code>Not Supported</code>. To add a vRealize Automation 7.x instance for metering, see <a href="#">Add a vRealize Automation 7 Instance for Metering in vCloud Usage Meter</a>.</p>

- 8 On the **Summary** page of the wizard, review the details and click **Submit**.

Check the number of product instances pending for user actions. For example - entering the managed product credentials or accepting certificates.

### Results

vRealize Suite Lifecycle Manager and its managed products are now part of the list of instances that vCloud Usage Meter supports.

Update the credentials for the managed product instances in the user task list, view the details panel of vRealize Suite Lifecycle Manager added, or the listing page of the discovered managed product instances.

If an error occurs, an error message appears on the vRealize Suite Lifecycle Manager page.

## Metering vRealize Operations with vCloud Usage Meter

If you associate a vRealize Operations (rebranded to Aria Operations) server with a vCenter Server instance that you added for metering, vCloud Usage Meter detects the vRealize Operations and displays the servers in the vCloud Usage Meter Web interface.

vCloud Usage Meter also detects all vCenter Server servers that a vRealize Operations instance monitors. To avoid configuration issues, configure the metered vCenter Server instances, the associated vRealize Operations instances, and vCloud Usage Meter to use the same time zone.

## Reporting of managed and unmanaged vCenter Server line items

If the added vRealize Operations monitors a vCenter Server instance, which is added for metering, vCloud Usage Meter reports the product consumption for this vCenter Server instance as `Managed vCenter` line items.

If the added vRealize Operations monitors a vCenter Server instance, which is not added for metering, vCloud Usage Meter reports the product consumption for this vCenter Server as `Unmanaged vCenter Servers` line items.

If vRealize Operations monitors a virtual machine that runs on `Unmanaged vCenter Servers`, vCloud Usage Meter reports the virtual machine as standalone.

## vRealize Operations Edition-based reporting

The vRealize Operations Standard, Advanced, and Enterprise editions are reported as Flex add-on or standalone depending on your preference.

## vRealize Operations license groups

For vRealize Operations 8.6 and later, vCloud Usage Meter supports license-based metering on a virtual machine level by using the vRealize Operations license groups.

To ensure accurate metering and reporting of vRealize Operations, review the following considerations.

- Every license must be a member of only one license group. If you add a license to two or more license groups, vCloud Usage Meter considers it as a member of the first license group returned by vRealize Operations API.
- When configuring the vRealize Operations license groups, do not include in the same group licenses with different license editions. If you configure a license group that includes licenses with different license editions, the highest license is applied to all license group objects.

## Add a vRealize Operations Instance for Metering in vCloud Usage Meter

To meter the product consumption data of vRealize Operations (rebranded as Aria Operations), you must add the vRealize Operations Manager instance to vCloud Usage Meter.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, select **Management > vRealize Operations**.
- 3 On the **vRealize Operations** page, click **Add**.
- 4 In the **Endpoint** text box, enter the host name or IP address of the vRealize Operations Manager instance.

The default port number is 443.

- 5 In the **Username** and **Password** text boxes, enter the credentials for the vRealize Operations Manager instance.

Provide the credentials for a user with access to the objects in the corresponding license group.

The vRealize Operations Manager administrator user has access to all objects in all license groups.

If you use a different vRealize Operations Manager local user, verify that this local user has access to the objects in the license groups created by him. If this user needs access to the objects in a license groups created by another user, assign access to the container view as well as to the objects in vSphere Storage.

- 6 Click **Add**.

## Configure the Metering for a Subset of Virtual Machines in vCloud Usage Meter

vCloud Usage Meter can generate reports for a subset of virtual machines that vRealize Operations controls. To support such a topology, you must create a specific user for vRealize Operations and add it to vCloud Usage Meter.

### Prerequisites

Verify that you have administrator privileges for the vRealize Operations user interface.

### Procedure

- 1 Log in to the administration interface of vRealize Operations.
- 2 Navigate to **Administration > Access Control** and on the **User Accounts** tab, click the **Add** button.  
The **Add User** window opens.
- 3 Enter the basic user information and click **Next**.
- 4 To assign role and allocate resources, in the **Assign Groups and Permissions** window, click **Objects**.
- 5 From the **Select Role** drop-down menu, select **Administrator** and select the **Assign this role to the user** check box.
- 6 In the **Select Object Hierarchies** pane, select the **vSphere Storage** check box.  
The vSphere inventory tree appears in the **Select Object** pane.
- 7 In the **Select Object** pane, select the virtual machines to be metered and click **Finish**.
- 8 Go to the vCloud Usage Meter Web interface and add or update the user credentials for vRealize Operations.

For more information about adding credentials for vRealize Operations, see [Add a vRealize Operations Instance for Metering in vCloud Usage Meter](#).



## Results

You can now add the new vRealize Operations credentials and generate reports only for the subset of virtual machines you selected.

# Add a vRealize Automation 7 Instance for Metering in vCloud Usage Meter

To meter the product consumption data of vRealize Automation, you must add the vRealize Automation 7.x instance to vCloud Usage Meter.

## Prerequisites

- Verify that you have an IaaS service user account.
- Verify that you can log in to the browser-based administration interface that the vRealize Automation appliance hosts, or to the vRealize Automation appliance operating system command line console as `root`. For information, see *Deploy the vRealize Automation Appliance* in the *Installing and Upgrading vRealize Automation* guide.
- Verify that you have a vSphere endpoint in your vRealize Automation appliance. For information, see *Create a vSphere Endpoint* in the *vRealize Automation Product Documentation* guide.
- Verify that vRealize Automation manages the virtual machines on the vSphere endpoint. For information, see *Bulk Import, Update, or Migrate Virtual Machines* in the *vRealize Automation* guide.

## Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, navigate to **Management > vRealize Automation 7 (legacy)**.
- 3 On the **vRealize Automation 7 (legacy)** page, click **Add**.
- 4 Under **Cafe appliance**, enter the vRealize Automation 7.x appliance details.
  - a In the **Endpoint** text box, enter the host name or IP address of the vRealize Automation 7.x instance.  
The default port number is 443.
  - b In the **Username** and **Password** text boxes, enter the credentials of a vRealize Automation administrator.  
  
Enter the user name without domain, for example *administrator*. This name must be from the *vsphere.local* domain.

- 5 Under **IaaS Server**, enter the details for the IaaS Web Server.
  - a In the **Endpoint** text box, enter the host name or IP address of the IaaS Web Server.
  - b In the **Username** and **Password** text boxes, enter the credentials of the IaaS Web Server user account.  
  
This user is the system user that you used to do the initial vRealize Automation installation. Provide the user name in the *user* format.
  - c (Optional) In the **Domain** text box, enter the domain name of the IaaS Web Server.
- 6 Click **Add**.

### Results

vRealize Automation 7.x is now part of the list of instances. If an error occurs, an error message appears on the **vRealize Automation 7 (legacy)** page.

## Add a vRealize Automation 8 Instance for Metering in vCloud Usage Meter

To meter the product consumption data of vRealize Automation 8.x, you must add the vRealize Suite Lifecycle Manager associated with the vRealize Automation 8.x instance in vCloud Usage Meter.

After registering the vRealize Suite Lifecycle Manager instance, vCloud Usage Meter automatically discovers and starts collecting product consumption data from the associated vRealize Automation 8.x instance.

### Prerequisites

- Verify that the vRealize Automation 8.x instance is associated with vRealize Suite Lifecycle Manager.
- Verify that the authentication and authorization is setup correctly with the VMware Identity Manager instance associated with vRealize Suite Lifecycle Manager.
- Verify that you can log in to the browser-based administration interface hosted by the vRealize Automation appliance.
- Verify that you have a VMware vCenter Server or Cloud (AWS, Azure, GCP etc.) account endpoint added to your vRealize Automation 8.x instance.
- Verify that you have added the associated vRealize Suite Lifecycle Manager instance to vCloud Usage Meter. For more information, see [Add a vRealize Suite Lifecycle Manager Instance for Metering in vCloud Usage Meter](#).
- Verify that vCloud Usage Meter can find the vRealize Automation 8.x instance.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.

- 2 Add the credentials for the vRealize Automation 8.x instance.
  - a In the left pane, navigate to **Management > vRealize Automation 8**.
  - b From the list with instances, select the vRealize Automation instance and review its status. The status can be `Please accept certificate`, `Please enter credentials`, or `Connection error`.
  - c (Optional) If the status is `Please accept certificate`, click to accept the product certificate. The status must change to `Please enter credentials`.
  - d Click `Please enter credentials` and provide the credentials for the vRealize Automation instance as configured in the VMware Identity Manager of the associated vRealize Suite Lifecycle Manager instance.
- 3 Click **Save**.

### Results

You successfully added the vRealize Automation to the list of instances. If an error occurs, an error message appears on the **vRealize Automation** page.

## Add an NSX Data Center for vSphere Instance for Metering in vCloud Usage Meter

To meter the product consumption data of NSX Data Center for vSphere, you must add the NSX-V Manager instance to vCloud Usage Meter.

### Prerequisites

- Register the NSX-V Manager appliance with vCenter Server. For more information, see *Register vCenter Server with NSX Manager* in the *VMware NSX Data Center for vSphere Documentation*.
- Verify that the vCenter Server instance associated with the NSX-V Manager is part of the vCloud Usage Meter list of vCenter Server instances.
- Verify that you have the **CLI Admin** user name and password for the NSX-V Manager appliance that you want to add.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, select **Networking > NSX-V**.
- 3 On the **NSX-V** page, click **Add**.
- 4 In the **vCenter Host Name** text box, enter the vCenter Server host name or IP address.
- 5 In the **Endpoint** text box, enter the host name or IP address of the NSX-V Manager appliance.
- 6 In the **Username** and **Password** text boxes, enter the NSX-V Manager **CLI Admin** credentials.

7 Click **Add**.

### Results

You successfully added NSX-V Manager to the list of instances. If an error occurs, a message appears in the Status column in the **NSX-v** list of instances.

## Add an NSX-T Data Center Instance for Metering in vCloud Usage Meter

To meter the product consumption data of NSX-T Data Center, you must add the NSX-T Manager instance to vCloud Usage Meter.

### Prerequisites

- Register the NSX-T Manager appliance with vCenter Server. For more information, see *Add a Compute Manager* in the *VMware NSX-T Data Center Product Documentation*.
- Add the vCenter Server instance associated with the NSX-T Manager to the vCloud Usage Meter list of vCenter Server instances.
- Verify that you have the **CLI Admin** user name and password for the NSX-T Manager instance that you want to add.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, select **Networking > NSX-T**.
- 3 On the **NSX-T** page, click **Add**.
- 4 In the **Endpoint** text box, enter the host name or IP address of the NSX-T Manager instance.
- 5 In the **Username** and **Password** text boxes, enter the NSX-T Manager **CLI Admin** credentials.
- 6 Click **Add**.

### Results

You successfully added NSX-T Manager to the list of instances. If an error occurs, a message appears in the Status column in the **NSX-T** list of instances.

## Add a vRealize Network Insight Instance for Metering in vCloud Usage Meter

To meter the product consumption data of vRealize Network Insight (rebranded as Aria Operations for Networks), you must add the vRealize Network Insight instance to vCloud Usage Meter.

## Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, select **Networking > vRealize Network Insight**.
- 3 On the **vRealize Network Insight** page, click **Add** .
- 4 In the **Endpoint** text box, enter the host name or IP address of your vRealize Network Insight instance.
- 5 Select the authorization type of a vRealize Network Insight user.
- 6 In the **Username** and **Password** text boxes, enter the credentials of a vRealize Network Insight user.
- 7 Click **Add**.

## Results

You successfully added vRealize Network Insight to the list of instances. If an error occurs, a message appears in the Status column in the **vRealize Network Insight** list of instances.

# Add a NSX Advanced Load Balancer Instance for Metering in vCloud Usage Meter

To meter the product consumption data of NSX Advanced Load Balancer, you must add the NSX Advanced Load Balancer instance to vCloud Usage Meter.

vCloud Usage Meter supports the metering of standalone NSX Advanced Load Balancer instances, NSX Advanced Load Balancer management clusters, and NSX Advanced Load Balancer instances associated with VMware Cloud Director.

---

**Note** To meter NSX Advanced Load Balancer management cluster, add only one of the instances that are part of the cluster.

---

## Prerequisites

Verify that the NSX Advanced Load Balancer roles have the following permissions.

- **read tenant**
- **read SEG**
- **read systemsettings**
- **read controller**
- **read cloud**

---

**Note** You must grant the permissions to every tenant that has service engines.

---

For more information, see the *User Roles* section in the *VMware NSX Advanced Load Balancer Administration Guide*.

## Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left pane, select **Networking > NSX Advanced Load Balancer**.
- 3 On the **NSX Advanced Load Balancer** page, click **Add**.
- 4 In the **Endpoint** text box, enter the host name or IP address of the NSX Advanced Load Balancer instance.
- 5 In the **Username** and **Password** text boxes, enter the NSX Advanced Load Balancer credentials.
- 6 Click **Add**.

## Results

You successfully added NSX Advanced Load Balancer to the list of instances. If an error occurs, a message appears in the Status column in the NSX Advanced Load Balancer list of instances.

# Add a VMware Cloud Director Availability Instance for Metering in vCloud Usage Meter

To meter the product consumption data of VMware Cloud Director Availability, you must add the product instance to vCloud Usage Meter.

For information about the compatibility between vCloud Usage Meter and VMware Cloud Director Availability, see the [VMware Product Interoperability Matrix](#).

## Connectivity

If you deploy vCloud Usage Meter as a part of the same network segment as VMware Cloud Director Availability that has direct access to the Cloud Director Replication Management Appliance or the vCenter Replication Management Appliance, provide the Cloud Replication Management Appliance address as `Endpoint`.

If vCloud Usage Meter cannot access the private IP address of the Cloud Director Replication Management Appliance or the vCenter Replication Management Appliance because of deployment specifics, you must provide the Service Endpoint address or the TCP Load Balancer address (if VMware Cloud Director Availability operates with a second Tunnel Appliance for High Availability) as `Endpoint`. For a Cloud Replication Management Appliance, set the **Restrict Admin APIs by source IP** configuration to **Allow admin access from anywhere**.

## Prerequisites

- Verify that vCloud Usage Meter can connect to VMware Cloud Director Availability.
- Verify that you have an account with sufficient privileges for the VMware Cloud Director Availability appliance.

## Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 Navigate to **Migration & Recovery > Cloud Director Availability**.
- 3 On the **Cloud Director Availability** page, click **Add**.
- 4 In the **Endpoint** text box, enter the host name or IP address of the VMware Cloud Director Availability instance.

For more information, see the *Connectivity* section.

- 5 From the **Authentication provider** radio button, select one of the authentication mechanisms.

Authentication mechanism	Description
Cloud Director Availability	Select if you use a Cloud Director Replication Management Appliance or a vCenter Replication Management Appliance. Requires the <b>root</b> user account credentials of the VMware Cloud Director Availability appliance.
vSphere SSO	Select if you use the vCenter Replication Management Appliance. Requires vSphere SSO credentials. The user must be a member of the VrMonitoringAdministrators SSO group in vSphere.
Cloud Director	Select if you use the Cloud Director Replication Management Appliance. The user must have a provider account with the VCDA_READ_RIGHT role assigned in VMware Cloud Director.

For information about setting up vSphere SSO or VMware Cloud Director accounts with the right permissions for VMware Cloud Director Availability, see *Users roles rights and sessions* in the *VMware Cloud Director Availability Security Guide* documentation.

- 6 In the **Username** and **Password** text boxes, enter the credentials of the selected **VMware Cloud Director Availability** authentication provider.
- 7 Click **Add**.

## Results

The product is part of the list of instances. If an error occurs, a message appears in the Status column in the **Cloud Director Availability** list of instances.

## Configure the Level of Anonymization of vCloud Usage Meter Reports

To hide sensitive data like virtual machine name, host name, and user name, you can anonymize the data transferred between vCloud Usage Meter and VMware Cloud Services Console. In the vCloud Usage Meter Web interface, you can configure the hashing level of the generated vCloud Usage Meter product consumption reports.

You can define which data is anonymized and the string for the anonymization.

**Attention** vCloud Usage Meter applies the configuration changes from the moment the changes are saved. If you change the level of anonymization after the first day of the month, only the report for this month is displayed with mixed hashing. The consecutive reports are representing the hashing as per the last configuration.

#### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Settings**.
- 2 In the left navigation pane, click **Data Hashing**.

The **Data Hashing** page opens.

- 3 From the **Select level for Hashing** drop-down menu, select the level of anonymization.

Option	Description
<b>Anonymizable fields are Hashed</b>	Fields with a name or IP address are anonymized. <b>Note</b> This option is selected by default.
<b>Anonymizable fields are Redacted</b>	Enter a specific label for the anonymized fields and select which product fields to use this label. <b>Note</b> The label is applied for the fields which you select.
<b>No Hashing</b>	No fields are anonymized.

- 4 (Optional) In [Step 3](#), if you selected **Anonymizable fields are Hashed** or **Anonymizable fields are Redacted**, select the fields you want to anonymize.

**Note** When you turn on the anonymization, you can deactivate and activate each category and attribute within a category. If you deactivate a whole category, vCloud Usage Meter considers all attributes within this category as deactivated.

- 5 Click **Save**.

#### Results

The configuration changes are applied on the next collection of product consumption data.

## Edit Product Information in vCloud Usage Meter

After you added product instances for metering in vCloud Usage Meter, you can edit the username and the password for the instance.

#### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left navigation pane, select the product.



- 3 On the product page, locate the product instance you want to edit and click **Edit**.
- 4 Enter the new name and the new password for the instance.
- 5 Click **Save**.

## Delete Product Servers in vCloud Usage Meter

You can delete product servers that are no longer in use.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Products**.
- 2 In the left navigation pane, select the product that you want to delete.
- 3 On the corresponding product page, select the instance you want to delete and click **Delete**.

### Results

The product is removed from the list of product servers. After deletion, wait for the hourly collection to ensure that the change in metering is successful. Any data collected before the deletion remains in the vCloud Usage Meter appliance.

## Change the vCloud Usage Meter Logging Level

You can change the logging level of vCloud Usage Meter to collect more details.

### Prerequisites

Verify that you have user privileges.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Settings**.
- 2 In the left navigation pane, click **Logging Level**.
- 3 On the **Logging Level** page, select a log and stat level from the **Log Level** and the **Stat Level** drop-down menus.

Option	Description
<b>Error</b>	Select to include Error and Fatal messages.
<b>Debug</b>	Select to include more log details than Info. This option causes the log capacity to fill faster.
<b>Info</b>	Select to include <b>Warn</b> , <b>Error</b> , <b>Fatal</b> , and <b>Info</b> messages. This level is the default logging level for the vCloud Usage Meter libraries.
<b>Trace</b>	Select to include more refined events information than the <b>Debug</b> logging level.
<b>Warn</b>	Select to include <b>Warn</b> , <b>Error</b> , and <b>Fatal</b> messages.

4 Click **Save**.

# Managing Customer Rules in vCloud Usage Meter



vCloud Usage Meter meters compute resource consumption of an vCenter Server or an VMware Cloud Director inventory. With customer rules, you have control over the consumption reporting from customers.

When you are ready to organize consumption reporting by a customer, you can create a customer rule that associates objects in your inventory for an entire vCenter Server or VMware Cloud Director instance.

By creating customer rules in vCloud Usage Meter, you associate customers with virtual machines that the appliance meters.

vCloud Usage Meter rebuilds customer rules on every collection. If you create, change, or remove a rule, it will be applied to reports after a subsequent collection run.

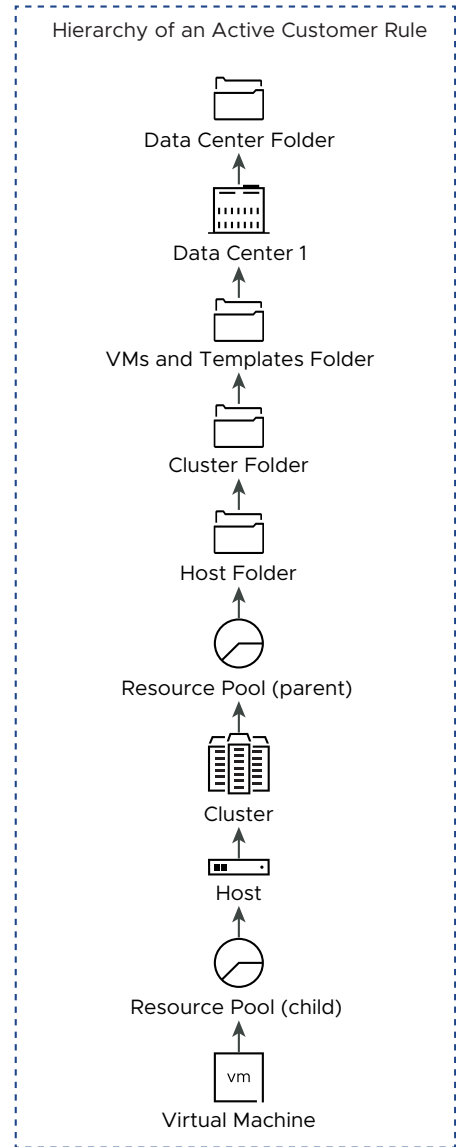
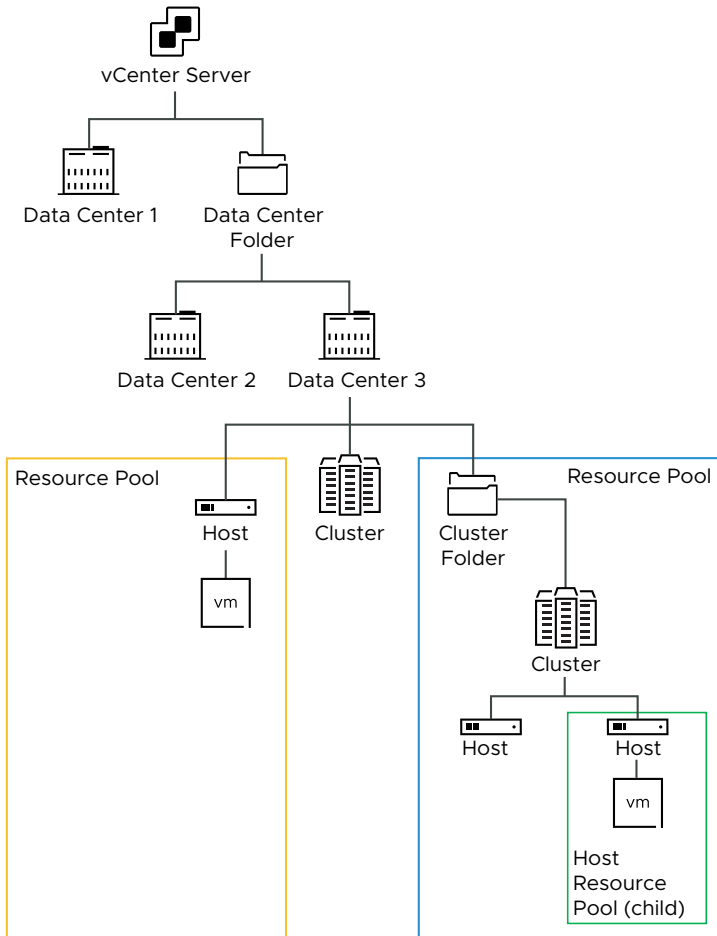
## Overlapping of Customer Rules

You can associate a customer rule with objects on different object levels in the inventory. Configuring customer rules on different object types in the same inventory might result in overlapping of the customer rules in which case vCloud Usage Meter applies only the active customer rule. As a best practice, consider always configuring the customer rules on the same object type.

## Active Customer Rules

In case of overlapping rules, vCloud Usage Meter applies an algorithm to find an active customer rule to meter the customer product consumption data. An active customer rule is the customer rule that is the closest to the virtual machine level.

If vCenter Server customer rules are overlapping with VMware Cloud Director customer rules, precedence has VMware Cloud Director.



Read the following topics next:

- [Object and Object Types in Customer Rules in vCloud Usage Meter](#)
- [Add a Customer Rule in vCloud Usage Meter](#)
- [Edit a Customer Rule in vCloud Usage Meter](#)
- [Delete a Customer Rule in vCloud Usage Meter](#)
- [Audit Customer Rules in vCloud Usage Meter](#)

## Object and Object Types in Customer Rules in vCloud Usage Meter

You can add a customer rule in vCloud Usage Meter by linking a customer label to specific objects in your vCenter Server and VMware Cloud Director inventory. When you construct a customer rule, the object type varies, depending on the product.

### Object Type Definitions

Object types aid you in metering and reporting specific customer activity.

Object Type in Inventory	Definition
vCenter Server	A vCenter Server is identified by a unique ID, holds all object types.
vCenter Server Cluster	Server group in the virtual environment.
Data center	A required structure in vCenter Server under which hosts and their associated virtual machines are added.
Host	Physical computer on which virtualization or other software is installed.
Resource Pool	Divisions of computing resources used to manage allocations between virtual machines in your inventory.
Folder	Grouped objects of the same type. For example, you can apply a common set of permissions to the folder and these permissions apply to all objects grouped in the folder.
VMware Cloud Director	A VMware Cloud Director is identified by a unique ID, holds all object types.
VMware Cloud Director Organization	A unit of administration for a collection of users, groups, and computing resources.

### Products and bundles that vCloud Usage Meter reports with customer rules

vCloud Usage Meter reports the following products and bundles:

- VMware Cloud Foundation
- VMware Tanzu Kubernetes Grid
- VMware vSAN Enterprise
- VMware vSphere Enterprise
- VMware vCenter Server Standard
- VMware Aria Operations for Networks
- VMware Aria Suite Enterprise
- VMware Data Services Manager
- VMware HCX Advanced

- VMware HSC Enterprise
- NSXNetworking
- VMware SDDC Manager

## Add a Customer Rule in vCloud Usage Meter

To tag the collected product consumption data per customers, you add customer rules in vCloud Usage Meter.

### Prerequisites

- Review your vCenter Server and VMware Cloud Director inventory for object types that correspond to your customers. See [Object and Object Types in Customer Rules in vCloud Usage Meter](#).
- The vCenter Server and VMware Cloud Director for which you want to configure a customer rule must be registered with vCloud Usage Meter.

### Procedure

1 In the main menu bar of the vCloud Usage Meter Web interface, click **Customers**.

2 From the navigation pane, select **Rules** and click **Add**.

The **Rules Configuration** wizard opens.

3 On the **Customer Label** page, enter a unique name for the customer label and click **Next**.

---

**Note** Do not enter n/a, No Customer Label, and - as the customer label. vCloud Usage Meter uses the **Customer Label** string as a technical key and accounts the product consumption data for objects for which no customer rule is configured to the default No Customer Label.

---

**Important** The **Customer Label** name is exposed to the cloud. To obfuscate the customer name, enter a customer identifier or hash as the **Customer Label**.

---

4 From the **Product** drop-down menu, select the vCenter Server or VMware Cloud Director endpoint.

The options for **Object Type** vary according to the product that you select.

5 From the **Object Type** drop-down menu, select the target type of object.

All objects of the selected object type are populated in the **Available Objects** table.

6 From the **Available Objects** table, select the object and click the right arrow button.

7 (Optional) You can add multiple objects to the same customer rule.

- To add another object from the same product endpoint, repeat [Step 5](#) through [Step 6](#).

- To add an object from another product endpoint, repeat [Step 4](#) through [Step 6](#).

---

**Note** If you add a customer rule for a VMware Cloud Director organization, the **Available Objects** table displays a higher number of organizations. This happens because vCloud Usage Meter lists the VMware Cloud Director system organization as an available choice.

---

If the selected object contains other objects, the customer label is mapped to all objects in the main object.

- 8 Click **Next**.
- 9 On the **Ready to Complete** page, review the configurations settings, and click **Finish**.

## Edit a Customer Rule in vCloud Usage Meter

In vCloud Usage Meter, you can change the customer rules that tag the collected product consumption data per customers.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Customers**.
- 2 From the navigation pane, select **Rules** and click **Edit**.  
The **Rules Configuration** wizard opens.
- 3 To update the customer rule, follow the prompts of the wizard and click **Finish**.

## Delete a Customer Rule in vCloud Usage Meter

In vCloud Usage Meter, to remove the mapping between the inventory object and the customer, you can delete customer rules from the rules list. All product consumption data is maintained.

### Prerequisites

If you want to delete a customer rule mapped to a VMware Cloud Director instance, verify that:

- the **Object type** is **Organization**.
- the only item in the **Selected Objects** list is **System**.

Object Type

Available Objects (1)

<input type="checkbox"/>	Name	Existing Label
<input checked="" type="checkbox"/>	System	
<input type="checkbox"/>	org	

1 - 2 of 2 Objects

Selected Objects (1)

<input type="checkbox"/>	Name	Product
<input type="checkbox"/>	System	

1 - 1 of 1 Objects

If the customer rule does not meet any of the described requirements, edit the rule and wait for the collection for the VMware Cloud Director instance to finish and then delete the rule.

#### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Customers**.
- 2 From the navigation pane, select **Rules**.
- 3 From the table with configured customer labels, select the label you want to delete and click **Delete**.
- 4 In the **Delete** wizard, confirm that you want to delete the selected customer label.

## Audit Customer Rules in vCloud Usage Meter

In vCloud Usage Meter, you can audit the customer rules associated with a registered vCenter Server or VMware Cloud Director instance.

#### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Customers**.
- 2 From the navigation pane, select **Audit**.
- 3 From the **Product** drop-down menu, select the product endpoint for which you want to audit the customer rules.
- 4 Review the audit data for the objects within the selected product endpoint.

The page displays a table with the first 100 results. To review the full list with audit data, click **Download TSV**.



Tab	Description
<b>Mapped Virtual Machines</b>	Displays a table with the mapped virtual machines associated with a customer rule and their corresponding customer label.
<b>Not Mapped Virtual Machines</b>	Displays a table of virtual machines that are not mapped to any customer label.
<b>Missing Target Objects</b>	Displays a table of configured customer labels for which the target object is deleted from the product inventory.
<b>Virtual Machines with Overlapping Rules</b>	Displays a table of virtual machines with overlapping customer rules for a product. To select a product, from the <b>Product</b> drop-down menu, select the endpoint for the product server.

# License Key Management in vCloud Usage Meter

## 9

After the transition to the new Broadcom Advantage Partner Program, vCloud Usage Meter automatically collects the license keys.

vCloud Usage Meter sends the information about the license keys to Broadcom Support Portal. Broadcom Support Portal classifies the license key in the following categories.

- part of customer commit
- part of aggregate commit
- part of Bring Your Own License (BYOL) program

# Managing vCloud Usage Meter Services

# 10

To ensure that vCloud Usage Meter collects and reports data properly, you can check the status of the services. You can either start or stop a specific service or all running services.

To reduce the consumed memory by the appliance, vCloud Usage Meter 4.7 introduces a new scheduling service for the collectors of product consumption data. Instead of having separate collector services for each product metered by vCloud Usage Meter, each collector is now a standalone application that the scheduling service runs once every hour.

## Verify if a vCloud Usage Meter Instance Reports Usage Data

You can verify if your vCloud Usage Meter instance reports usage data to VMware Cloud Services Console.

### Procedure

- 1 In the main menu bar of the vCloud Usage Meter Web interface, click **Settings**.
- 2 In the left navigation bar, click **Send Update to Cloud Partner Navigator**.  
The **Send Update to Cloud Partner Navigator** page opens.
- 3 Click **Send Update to Cloud Partner Navigator**.

---

**Note** If vCloud Usage Meter detects usage data that is available for upload, you receive the following notification entry - Successfully uploaded product data to Cloud Partner Navigator. If vCloud Usage Meter does not detect such data, you receive the following notification entry - No product consumption data available for upload to Cloud Partner Navigator.

---

If the operation completes successfully, the following message displays All Data Sent Successfully.

## Check the Status of the Services in vCloud Usage Meter

You can check if the services in vCloud Usage Meter are running.

### Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter**.

- 2 To check the status of the services in vCloud Usage Meter, run the `status.sh` script. .

```
status.sh all
```

If the metered instances are running, you receive a `Running` status back. For example,

```
Process service-name status: Running
```

## Start a vCloud Usage Meter Service

You log in to the vCloud Usage Meter to start a vCloud Usage Meter service.

You can start a specific vCloud Usage Meter service or all running services.

### Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter**.
- 2 Start the vCloud Usage Meter service.

```
start.sh service-name
```

## Stop a vCloud Usage Meter Service

You log in to the vCloud Usage Meter to stop a vCloud Usage Meter service.

You can stop a specific vCloud Usage Meter service or all running services.

### Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter**.
- 2 Stop the vCloud Usage Meter service.

```
stop.sh service-name
```

## Generate Support Bundle Collections in vCloud Usage Meter

You can generate a support bundle for your vCloud Usage Meter instance. The support bundle contains the log files that you can use for troubleshooting purposes.

### Procedure

- 1 Log in to the vCloud Usage Meter console as **usagemeter**.
- 2 Navigate to the `cloudusagemetering` directory.

```
/opt/vmware/cloudusagemetering
```

- 3 To generate the support bundle, run the following script.

```
./scripts/bundle.sh
```

This process takes a few minutes. The generated support bundle file `bundle.tar.gz` is saved to the `cloudusagemetering` directory.

# Managing vCloud Usage Meter Accounts

# 11

Administrative and management tasks occur after you deploy and configure the vCloud Usage Meter appliance. They include changes to the provisioned environment and routine administration and maintenance procedures.

Read the following topics next:

- [Reset the Root Password in vCloud Usage Meter](#)
- [Change the Root Password in vCloud Usage Meter](#)
- [Unlock the \*\*usagemeter\*\* Account](#)
- [Change the User Account Passwords for the usagemeter and the umauditor User Accounts](#)
- [Change the Password Expiration Parameters for the vCloud Usage Meter User Accounts](#)
- [Password Requirements for the vCloud Usage Meter User Accounts](#)

## Reset the Root Password in vCloud Usage Meter

In vCloud Usage Meter, if you lost or forgot the **root** account password, you can reset it.

If you know the **root** account password and want to change it due to security or other reasons, see [Change the Root Password in vCloud Usage Meter](#).

### Procedure

- 1 In the vSphere Web Client, restart the guest operating system of the vCloud Usage Meter appliance.
- 2 Click the console and wait for the **Photon** screen to appear.
- 3 Press **e** to go to the **GNU GRUB** boot menu editor.  
The **GNU GRUB** menu remains on the screen for several seconds before it starts the boot sequence.
- 4 Use the arrow keys to go to the line that begins with `linux` and append the `rw init=/bin/bash` string at the end of the line.
- 5 To boot the system, press **Ctrl+X** or **F10**.
- 6 To reset the **root** account password, enter the `passwd` commands in the console.

- 7 To confirm the change, enter a new password, then reenter the same password.

---

**Note** All passwords must meet a set of password requirements. For more information, see [Password Requirements for the vCloud Usage Meter User Accounts](#).

---

- 8 Restart the vCloud Usage Meter appliance by using the vSphere Web Client.

## Change the Root Password in vCloud Usage Meter

In vCloud Usage Meter, you can change the **root** account password due to security restrictions or other reasons.

### Prerequisites

Verify that you can log in to the vCloud Usage Meter console as **root**.

### Procedure

- 1 Log in to the virtual machine console as **root**.
- 2 To change the **root** password, run the `passwd` command.
- 3 To confirm the change, enter a new password, then reenter the same password.

---

**Note** All passwords must meet a set of password requirements. For more information, see [Password Requirements for the vCloud Usage Meter User Accounts](#).

---

- 4 Log out from the vCloud Usage Meter console.

## Unlock the usagemeter Account

If you enter a wrong password for the **usagemeter** account three times, the account locks. To unlock the user account, you can either reset the user password or wait 15 minutes for the user account to get unlocked.

### Prerequisites

- Verify that you can log in as **root** in the vCloud Usage Meter console. To change the **root** account password, see [Change the Root Password in vCloud Usage Meter](#).
- Verify that you can log in to vCloud Usage Meter with an **usagemeter** account. This procedure is about unlocking the account. If you want to change the password of the **usagemeter** account, see [Change the User Account Passwords for the usagemeter and the umauditor User Accounts](#).

### Procedure

- 1 Log in to the virtual machine console as **root**.

- 2 To unlock the **usagemeter** account, run the following command.

```
pam_tally2 --user=usagemeter --reset
```

This operation resets the count for failed login attempts for the **usagemeter** account.

- 3 Log out from the vCloud Usage Meter console.

## Change the User Account Passwords for the usagemeter and the umauditor User Accounts

You can change the **usagemeter** and **umauditor** user account passwords due to security restrictions or other reasons.

---

**Important** Passwords for your **usagemeter** and **umauditor** user accounts expire after 90 days. To change the expiration parameters for the **root**, **usagemeter**, and **umauditor** user accounts, see [Change the Password Expiration Parameters for the vCloud Usage Meter User Accounts](#).

---

### Prerequisites

Verify that you have access to vCloud Usage Meter console as **root**.

### Procedure

- 1 Log in to the virtual machine console as **root**.
- 2 To change the **usagemeter** or **umauditor** user account passwords, run the `passwd user-account` command.

```
passwd user-account
```

- 3 To confirm the change, enter a new password, then reenter the same password to verify it.

---

**Note** All passwords must meet a set of password requirements. For more information, see [Password Requirements for the vCloud Usage Meter User Accounts](#).

---

- 4 Log out from the virtual machine console.
- 5 (Optional) To update the user account password for the current user account, run the `passwd` command.

```
passwd
```

Enter a new password, then reenter the same password to verify it.

---

**Note** All passwords must meet a set of password requirements. For more information, see [Password Requirements for the vCloud Usage Meter User Accounts](#).

---



## Change the Password Expiration Parameters for the vCloud Usage Meter User Accounts

You log in to the vCloud Usage Meter console to update the password expiration parameter for the **root**, **usagemeter**, and the **umauditor** user accounts.

### Procedure

- 1 Log in to the virtual machine console as the vCloud Usage Meter user, for which you want to change the password expiration parameter.
- 2 View the current configuration for the password expiration.

```
chage -l user-account-name
```

- 3 Change the password expiration parameters.
  - Configure a maximum number of days the user is allowed to use the password.

```
chage -M expiration-daysuser-account-name
```

- Deactivate password expiration.

```
chage -M -1 user-account-name
```

## Password Requirements for the vCloud Usage Meter User Accounts

To ensure that vCloud Usage Meter user accounts are safe and secure, the passwords must meet certain requirements.

- Passwords must be at least eight characters long.
- Passwords must contain at least one uppercase letter.
- Passwords must contain at least one lowercase letter.
- Passwords must contain at least one numeral from 0 through 9.
- Passwords must contain at least one special character.
- Passwords must contain at least four different characters in comparison to the old password.
- Passwords must be different from the last five passwords.
- Passwords must be verified against the existing password dictionary list.

# Upgrading the vCloud Usage Meter Appliance

# 12

You can upgrade the vCloud Usage Meter appliance by using an `.iso` image that includes a complete Photon OS update.

If you want to upgrade from vCloud Usage Meter 3.6.x, you must install vCloud Usage Meter 4.7 as a new appliance.

If you want to run in parallel both old and new appliances for a full reporting period, set the vCloud Usage Meter 4.7 instance to **Test** mode. You can still collect, aggregate, and reference the product consumption data from the vCloud Usage Meter 4.7 instances. For more information, see the [https://kb.vmware.com/s/article/82529?lang=en\\_US](https://kb.vmware.com/s/article/82529?lang=en_US) KB.

Then if you want to activate vCloud Usage Meter 4.7 for reporting, through the VMware Cloud Services Console, update the mode of the vCloud Usage Meter 4.7 instance from **Test** to **Production**.

To upgrade the vCloud Usage Meter appliance, you must install only the official vCloud Usage Meter updates that VMware provides.

Read the following topics next:

- [In-Place Upgrade of vCloud Usage Meter](#)

## In-Place Upgrade of vCloud Usage Meter

You can install vCloud Usage Meter 4.7 as an in-place upgrade on top of vCloud Usage Meter 4.3 and later.

## Prerequisites

Prerequisite	Description
Source vCloud Usage Meter appliance	<ul style="list-style-type: none"> <li>Back up or take a snapshot of the source vCloud Usage Meter appliance that you want to upgrade.</li> <li>As <b>root</b>, activate and start SSH on the source vCloud Usage Meter appliance by running the following commands.           <pre>systemctl enable sshd</pre> <pre>systemctl start sshd</pre> </li> </ul>
Authentication	Verify that you can access the vCloud Usage Meter console as <b>root</b> .

## Procedure

- 1 Locally on your computer, download the following upgrade files from the [Broadcom Support Portal](#) download product page.

File Name	Description
<code>Usage_Meter_Agent-4.7.0.1- &lt;BUILD_NUMBER&gt;_Upgrade.iso</code>	The ISO upgrade file containing the upgrade script and the YUM repository.
(Optional) <code>Usage_Meter_Agent-4.7.0.1- &lt;BUILD_NUMBER&gt;_Upgrade.mf</code>	Contains the sha1checksum of the upgrade ISO file.
(Optional) <code>Usage_Meter_Agent-4.7.0.1- &lt;BUILD_NUMBER&gt;_Upgrade.crt</code>	Contains the public certificate that signs the ISO file.
(Optional) <code>Usage_Meter_Agent-4.7.0.1- &lt;BUILD_NUMBER&gt;_Upgrade.sign</code>	Contains the signature for the ISO file.

- 2 From the terminal of your computer, log in to the vCloud Usage Meter appliance and run the following commands.

- a Verify that the checksum of the download matches the checksum posted on the download page.

```
shasum -c Usage_Meter_Agent-4.7.0.1-<BUILD_NUMBER>_Upgrade.mf
```

- b Verify the certificate.

```
openssl x509 -in Usage_Meter_Agent-4.7.0.1-<BUILD_NUMBER>_Upgrade.crt -text
```

```
openssl verify Usage_Meter_Agent-4.7.0.1-<UM_NEW_BUILD>_Upgrade.crt
```

- c Obtain the certificate public key and verify the signature of the ISO file.

```
openssl x509 -pubkey -in Usage_Meter_Agent-4.7.0.1-<BUILD_NUMBER>_Upgrade.crt \  
> Usage_Meter_Agent-4.7.0.1-<BUILD_NUMBER>_Upgrade.key
```

```
openssl dgst -sha1 -verify Usage_Meter_Agent-4.7.0.1-<BUILD_NUMBER>_Upgrade.key \  
-signature Usage_Meter_Agent-4.7.0.1-<BUILD_NUMBER>_Upgrade.sign \  
Usage_Meter_Agent-4.7.0.1-<BUILD_NUMBER>_Upgrade.mf
```

- 3 Connect the CD-ROM drive of vCloud Usage Meter to the Usage\_Meter\_Agent-4.7.0.1-<BUILD>\_Upgrade.iso file.

For information, see *Add or Modify a Virtual Machine CD or DVD Drive* in the *vSphere Virtual Machine Administration* documentation.

- 4 Log in to the source vCloud Usage Meter console as **root**.
- 5 Create an upgrade directory.

```
mkdir /root/upgrade
```

- 6 Mount the CD drive.

---

**Note** If you upload the `.iso` file inside the vCloud Usage Meter appliance manually, enter the full `.iso` path location in the command.

---

```
mount -o loop /dev/cdrom /root/upgrade
```

- 7 To start the in-place upgrade, run the command.

```
bash /root/upgrade/upgrade-um.sh
```

You are prompted to confirm if a snapshot of the source vCloud Usage Meter appliance that you want to upgrade exists.

```
Has a snapshot of the vCloud Usage Meter appliance VM been created on the  
vCenter Server environment that it's running on? (y/n):
```

- 8 To complete the in-place upgrade, you are prompted to reboot the appliance.

```
Reboot is recommended after an upgrade. Reboot now? (y/n)
```

If you enter y (yes), a reboot of the appliance starts. If you enter n (no), you must manually reboot the appliance by running the following command.

```
sudo reboot
```

The system generates a newly created `cloudusagemetering` folder under `/opt/vmware` pointing to the upgraded vCloud Usage Meter installation.

- 9 (Optional) If vCloud Usage Meter detects an incorrectly set hostname, you receive the following message.

```
Detected wrong hostname. Expected hostname: ${host}, but found: ${current_hostname}. This will most probably result in issues after upgrade with the existing vCloud Usage Meter certificates.
Please change the hostname and then you can either generate a new self-signed certificate or import an internal Certification Authority (CA) - Signed Certificate.
Note: The certificate CN must match the hostname of the vCloud Usage Meter appliance.
For information, see vCloud Usage Meter Certificate Management.
```

If you ignore the message, you might encounter the

```
Failed to process journal=>read
```

error in the vCloud Usage Meter Web interface. Follow the instructions provided in the message. For more information, see [Chapter 6 vCloud Usage Meter Certificate Management](#).

- 10 Verify that the vCloud Usage Meter services are up and running.
- a Verify the status of the vCloud Usage Meter services.

```
bash status.sh
```

If the services are running, you receive a `Running` status. In case you receive a `Running` status that has errors, check the latest log files. The errors might not be related to the in-place upgrade.

### What to do next

---

**Note** To ensure the automatic aggregation and reporting of the monthly product consumption data, after a successful upgrade, do not revert to the snapshot of the source vCloud Usage Meter appliance.

---

# Email Notifications for vCloud Usage Meter Instances

# 13

There are two types of email notifications for vCloud Usage Meter instances - local email notifications and VMware Cloud Services Console notifications.

The email notifications from VMware Cloud Services Console might include information about the reporting status of a registered vCloud Usage Meter instance, an issue with a certificate or with the collection of product consumption data, or information about issues with the vCloud Usage Meter appliance. The local email notifications might include information about product collection issues, resource issues, or connectivity issues with the vCloud Usage Meter appliance. For more information about configuring the local email notifications, see [Configure the Local Email Notifications for vCloud Usage Meter](#).

**Important** VMware Cloud Services Console sends email notifications for vCloud Usage Meter instances that are actively reporting the product consumption data to the cloud. You can receive local email notifications for VMware Cloud Services Console appliances in online mode.

VMware Cloud Services Console types of email notification	Description	Required Action
Usage Meter instance UM name ( <i>UUID</i> ) has not been uploading product consumption data to VMware in the past 24 hours/the past month!	vCloud Usage Meter failed to upload product consumption data for 24 hours for an instance in online mode.	To resolve the issue, see the following <a href="https://kb.vmware.com/s/article/82023">https://kb.vmware.com/s/article/82023</a> KB.
Usage Meter instance UM name ( <i>UUID</i> ) is uploading product consumption data to VMware.	After previous issues with uploading data for a specific instance, vCloud Usage Meter is back to uploading product consumption data.	No action needed.
No product is added for metering to Usage Meter instance UM name ( <i>UUID</i> ).	vCloud Usage Meter does not detect any products for metering and is not sending any product consumption data to the cloud.	To resolve the issue, see the following <a href="https://kb.vmware.com/s/article/82022">https://kb.vmware.com/s/article/82022</a> KB.
Product is successfully added for metering to Usage Meter instance UM name ( <i>UUID</i> ).	vCloud Usage Meter detects a product that is registered for metering and is sending product consumption data to the cloud. You receive the notification only if vCloud Usage Meter did not detect any products previously.	No action needed.

VMware Cloud Services Console types of email notification	Description	Required Action
Product metering status changed for Usage Meter	<p>You receive this notification on two scenarios:</p> <ul style="list-style-type: none"> <li>Some of the registered vCloud Usage Meter instances have a failed status for reasons such as product server certificate issues, invalid credentials, or partial collection issues.</li> <li>Statuses of registered vCloud Usage Meter instances changed from failed to successful.</li> </ul>	If some of the registered vCloud Usage Meter instances have a failed status, check the provided resolution in the Remediation section of each issue.
Summary of Usage Meter statuses	A list of all encountered issues in the last 24 hours for the registered vCloud Usage Meter instances to the provider.	No action needed.

Table 13-1.

vCloud Usage Meter types of email notifications	Description	Required action
Summary of Usage Meter product issues	A list of product issues, grouped by product type and product ID.	Check the provided resolution in the Remediation section of each issue.
Issues with Usage Data Upload to Cloud Partner Navigator	vCloud Usage Meter does not upload data to VMware Cloud Services Console.	Check the provided resolution in the Remediation section of the issue.
Appliance Storage/Memory/CPU usage alert	vCloud Usage Meter detects high storage, memory, or CPU usage.	Check your storage, memory, or CPU usage and increase the respective resource if needed.
Additional notifications	You can receive notifications related to the health of the services, FIPS mode configuration issues, and so on.	

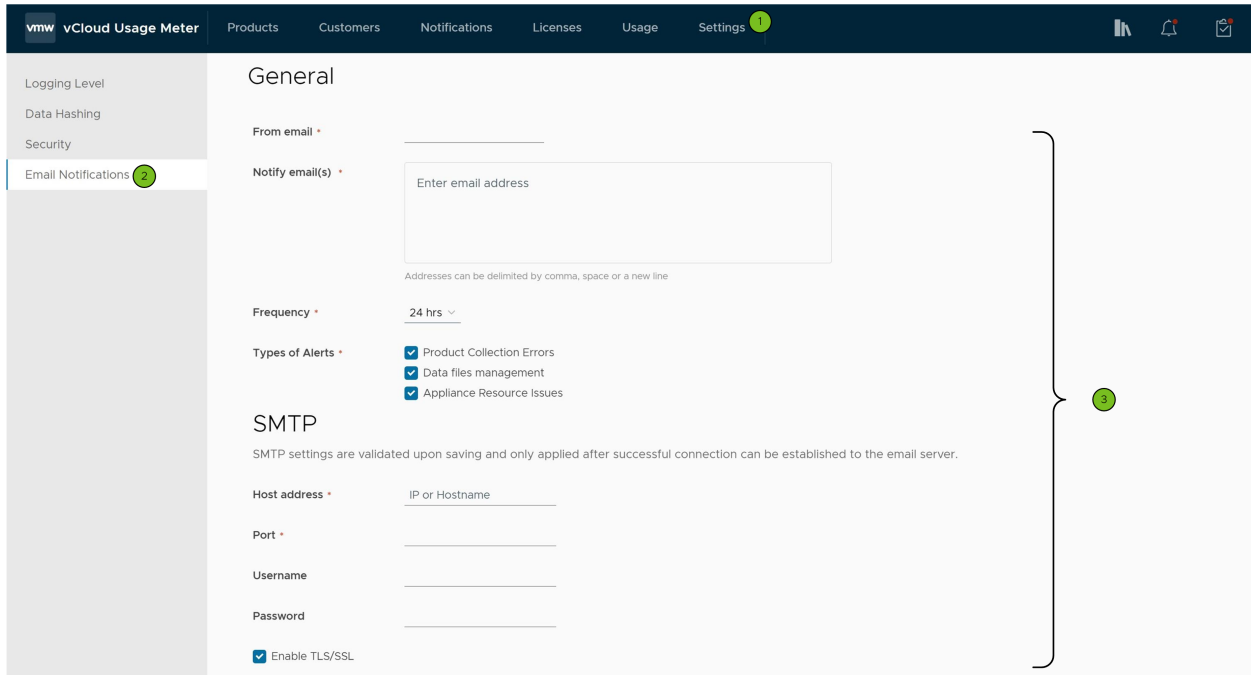
Read the following topics next:

- [Configure the Local Email Notifications for vCloud Usage Meter](#)
- [Troubleshooting Issues with the SMTP settings for vCloud Usage Meter](#)

## Configure the Local Email Notifications for vCloud Usage Meter

To notify to a set of recipients about issues with vCloud Usage Meter, you must configure the local email notifications.

You can configure local email notifications about product collection issues, connectivity issues, or resource issues with the vCloud Usage Meter appliance.



**Procedure**

- 1 Log in to the vCloud Usage Meter Web interface.
- 2 Navigate to **Settings > Email Notifications**.
- 3 Configure the following settings.

General Settings	Description
From email	Enter the sender of the email notifications.
Notify email(s)	Enter the recipients of the email notifications.  <b>Note</b> Ensure that you enter the email addresses in the correct format: <i>username@domain</i> . Otherwise, the comments will be marked in red.



General Settings	Description
Frequency	From the <b>Frequency</b> check box, select how often the recipients will receive email notifications. You can select between <b>1 hour</b> , <b>6 hours</b> , <b>12 hours</b> , and <b>24 hours</b> . The <b>Frequency</b> check box defines a temporary limit that serves as a threshold and groups multiple alerts into a single email.
Types of Alerts	<p>Select the types of alerts that the recipients will receive email notifications for. You must select at least one type of an alert.</p> <ul style="list-style-type: none"> <li>■ <b>Product Collection Errors</b></li> <li>■ <b>Appliance Connectivity Issues with VMware</b></li> <li>■ <b>Appliance Resource Issues</b></li> <li>■ <b>Data files management</b></li> </ul> <p><b>Note</b> Appliance Resource issues types of alerts do not take into account the selected frequency for the email notifications.</p>

#### 4 Configure the SMTP settings.

- a In the **Host address** text box, enter the SMTP server IP or hostname.
- b In the **Port** text box, enter the SMTP port number.
- c (Optional) If the SMTP server requires authentication, enter the SMTP user name and password.
- d (Optional) If the provided server supports SMTP over TLS/SSL, select the **Enable TLS/SSL** check box.
- e (Optional) Click **Save**.

All email recipients receive an email notification with information about the applied settings. A message in the vCloud Usage Meter Web interface appears and informs you that the recipients received a notification. If you encounter issues while and after configuring the SMTP settings, see [Troubleshooting Issues with the SMTP settings for vCloud Usage Meter](#).

## Example:

### What to do next

To pause the email notifications, click the **Pause** button. vCloud Usage Meter notifies all email recipients about the paused notifications. To reset the notification settings, click the **Reset** button.

## Troubleshooting Issues with the SMTP settings for vCloud Usage Meter

Troubleshoot issues you encountered while and after configuring the SMTP settings for the local email notifications.

Issue	Suggested solution
The SMTP host address is incorrect or unreachable	Log in to the vCloud Usage Meter appliance and check if the provided SMTP server address is correct and reachable.
Incorrect SMTP port	Check whether the SMTP port accepts the connections.
SMTP server authentication issues	If your SMTP server requires authentication, make sure that you enter the correct username and password. The vCloud Usage Meter appliance protects the stored password.
SMTP over SSL/TLS issues	If your SMTP server requires SSL/TLS, make sure that you enable the option while configuring the local email notifications and verify that the port you entered is correct. You can find more information about the issue in the <code>/opt/vmware/cloudusagemetering/platform/log/vmware-um-journal.log</code> file.

# Product Notifications in vCloud Usage Meter

# 14

The **Notifications** tab in the vCloud Usage Meter Web interface displays an overall system status and event notification alerts about the metered products.

## System Status

**System Status** displays a per-day aggregated information for 7 days going back about the status of the metered products.

**System Status** displays the following message types.

Message type	Description
Green	vCloud Usage Meter did not detect any error events about a metered product server.
Red	vCloud Usage Meter detected at least one error event for the specified day.
Orange	Contains warning event messages.
Grey	No event notifications for the specified day.

To view the notifications for a specific day, under **System Status**, click on the date. All notifications are displayed in the **Notifications** list.

## Notifications

The **Notifications** list displays a list with event messages about the metered product servers. You can either view the notifications for all product servers, or for a selected product. You can filter the notifications list by a notification ID, product ID, product type or by notification type.