Cisco UCS Performance Manager Getting Started Guide

First Published: October 2017

Release 2.5.1

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Contents

About this guide

Cisco UCS Performance Manager Getting Started Guide describes how to set up Cisco UCS Performance Manager Express and Cisco UCS Performance Manager and to prepare your environment for monitoring. Use this guide after completing all of the steps required for your deployment in *Cisco UCS Performance Manager Installation Guide*.

- Cisco UCS Performance Manager Express provides monitoring for Cisco UCS Central, Cisco UCS Domains, Linux and Microsoft Windows servers, hypervisor servers, and Control Center.
- Cisco UCS Performance Manager provides monitoring for Cisco UCS Central, Cisco UCS Domains, Linux and Microsoft Windows servers, hypervisor servers, network devices, storage devices, and Control Center.

For convenience, this document uses "Cisco UCS Performance Manager" generically, and notes explicitly any differences between the two licenses.

Related publications

Title	Description
Cisco UCS Performance Manager Planning Guide	Provides general and specific information for preparing to deploy Cisco UCS Performance Manager.
Cisco UCS Performance Manager Installation Guide	Provides detailed information and procedures for installing Cisco UCS Performance Manager.
Cisco UCS Performance Manager Upgrade Guide	Provides detailed procedures for upgrading your existing Cisco UCS Performance Manager 2.x instance to a newer version.
Cisco UCS Performance Manager Migration Guide	Provides detailed information about, and where applicable, procedures for migrating data from Cisco UCS Performance Manager version 1.x into a version 2.x instance.
Cisco UCS Performance Manager Getting Started Guide	Provides instructions for configuring Cisco UCS Performance Manager to monitor your environment after installation.
Cisco UCS Performance Manager User Guide	Provides specific instructions for using Cisco UCS Performance Manager in the UCS environment.
Cisco UCS Performance Manager Administration Guide	Provides an overview of Cisco UCS Performance Manager architecture and features, as well as procedures and examples to help you use the system.
Cisco UCS Performance Manager Release Notes	Describes known issues, fixed issues, and late-breaking information not already provided in the published documentation set.

Documentation feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to `ucs-docfeedback@cisco.com`. We appreciate your feedback.

Preparing for monitoring 1

Cisco UCS Performance Manager uses standard management APIs to collect performance data, and therefore does not install proprietary agents on your infrastructure devices to collect monitoring data. However, Cisco recommends that you review the information in this chapter to verify that the devices to you want to monitor are ready to respond to requests for data.

When your infrastructure is ready to monitor, the Cisco UCS Performance Manager Setup Wizard guides you through the process of accepting the EULA, providing your license key, setting up UCS Central devices, setting up UCS domains, and then adding devices by category and type.

Preparing network devices

This chapter provides instructions for preparing devices for monitoring.

Preparing switches and routers

To prepare a switch or router device for monitoring, verify that an SNMP agent is installed and currently running on the device.

Note If your license is Cisco UCS Performance Manager Express, skip this topic.

Preparing Cisco UCS network devices

Cisco UCS Performance Manager uses SNMP to provide customized or generalized support for many Cisco products.

The following table associates Cisco products with the customized Cisco UCS Performance Manager device types that support them. Device types are listed in the **Network** area of the **Add Infrastructure** wizard, which is both part of the setup wizard and available through the Cisco UCS Performance Manager browser interface.

Note The following device considerations apply:

- Some supported devices, such as the Cisco Nexus 7000 and 9000 switches, represent a large number of discrete monitoring endpoints. If you are unsure which Cisco UCS Performance Manager deployment size supports the number of high-density devices you wish to monitor, contact your Cisco representative.

- To monitor Cisco Nexus 9000 Series devices, you must first enable NX-API with the `feature` manager CLI command on the device. For detailed instructions on performing this task, refer to the *Cisco documentation* for the Nexus 9000.

Cisco product	Device type
Cisco Catalyst 6500 and 3560 Series Switches	Cisco 6500 (SNMP)
Cisco Nexus 5000 Series Switches	Cisco Nexus 5000 (SNMP + Netconf)
Cisco Nexus 7000 Series Switches	Cisco Nexus 7000 (SNMP + Netconf)
Cisco Nexus 2000 Series Fabric Extenders	Cisco Nexus 5000 (SNMP + Netconf)
Cisco Nexus 1000v Series Switches	Cisco Nexus 1000V (SNMP + Netconf)
Cisco Nexus 3000 Series Switches	Cisco Nexus 3000 (SNMP + Netconf)
Cisco Nexus 9000 Series Switches	Cisco Nexus 9000 (NX-API)
Cisco Catalyst 6500 Series Virtual Switching Systems	Cisco VSS (SNMP)
Cisco MDS 9000 Series Multilayer Switches	Cisco MDS 9000 (SNMP)

In addition, Cisco UCS Performance Manager provides two generalized device types.

Cisco product	Device type
Cisco CatOS-based switches or routers	Generic Switch/Router (SNMP)
Cisco IOS-based switches or routers	Cisco IOS (SNMP)

Preparing storage devices

This section describes how to prepare NetApp and EMC storage devices for monitoring.

Cisco UCS Performance Manager Express users can skip this topic.

Legacy NetApp filers

Cisco UCS Performance Manager uses SNMP to monitor legacy NetApp filers that do not support the Data ONTAP® API (ZAPI).

The data gathered are approximate because the values for many objects (Aggregate, Volume, Plex, and RAID group) are not exposed by the NetApp MIB.

To prepare a legacy NetApp filer for monitoring, verify that SNMPv2 is installed, and then start an SNMP agent.

Recent NetApp filers

Cisco UCS Performance Manager uses HTTP to monitor NetApp filers that support the Data ONTAP® API (ZAPI).

To prepare a recent NetApp filers for monitoring, verify the following conditions:

- The filer is running in 7-Mode or C-Mode.
- A supported version of ZAPI is installed and enabled. The minimum required version is 8.x.

- The user name and password of your account on the filer is authorized to use ZAPI.

EMC storage arrays

Cisco UCS Performance Manager uses the Web-Based Enterprise Management (WBEM) protocol to send queries to EMC Storage Management Initiative Specification (SMI-S) providers that are associated with EMC VMAX and VNX storage arrays.

To prepare EMC arrays for monitoring:

- At least one EMC SMI-S provider must be running for each type of array to monitor. (The VMAX and VNX data models are different.)
- Before adding an SMI-S provider to Cisco UCS Performance Manager, Cisco recommends that you confirm that it is responding to requests.

  SMI-S provider version 4.6 has been certified for this version of Cisco UCS Performance Manager. SMI-S provider version 8.1 is not currently supported.
- You need the following information:

  - user name and password for an account that is authorized to collect data on each SMI-S provider
  - IP address of each SMI-S provider
  - port number at which each SMI-S provider listens for requests
  - whether to use SSL

Note When statistics logging is disabled on the EMC device, graphs for component types of EMC arrays display NaN. The logging feature has a low default timeout value and must be set to a higher value or turned on again periodically.

Verifying an SMI-S provider on EMC devices

To perform this procedure, you need a Linux host that has a network path to the SMI-S providers of the arrays to monitor.

Note Do not perform this procedure on the Cisco UCS Performance Manager host.

Perform this procedure to verify that the SMI-S providers associated with EMC arrays are configured correctly, and are responding to WBEM queries from command line tools.

1. Log in to a Linux host as `root`, or as a user with superuser privileges.
2. Install a WBEM command-line interface package, such as `wbemcli`.
3. Verify the SMI-S provider. Replace the variables with values that are valid in your environment.

   ```
   wbemcli IP-Address:Port -u admin \
    -p 'Password' -n root/emc --no-sslei('EMC_DiskDrive')
   ```

   The expected result is a list of Disk Drive classes.

Preparing server devices

This section describes how to prepare Linux and Windows servers for monitoring.

Preparing Linux servers for monitoring

Cisco UCS Performance Manager uses SNMP or SSH to monitor Linux servers.

For SNMP monitoring, install an SNMP package on the server (for example, *Net-SNMP*) and start the agent.

For SSH monitoring:

- Install an SSH server package (for example, *OpenSSH*) and start the SSH daemon.
- Monitoring Linux servers requires the ability to run the `pvs`, `vgs`, `lvs`, `systemctl`, `initctl`, and `service` commands remotely on your Linux server(s) using SSH. By default, most of these commands are only allowed to be run locally by the `root` user. If you want the `root` user to remotely run these commands, perform the following:

  1. Install the `sudo` package on your server.
  2. Allow the `root` user to execute commands via SSH without a TTY.

     a. Edit the `/etc/sudoers` file.
     b. Find the line containing `root ALL=(ALL) ALL`.
     c. Add the following line beneath it:

     ```
     Defaults:root !requiretty
     ```

     d. Save the changes and exit.

  Alternately, you can also set up a non-root user to remotely run these commands. Perform the following:

  1. Create a user named `zenmonitor` on your Linux servers for monitoring purposes.
  2. Install the `sudo` package on your server.
  3. Allow the `zenmonitor` user to run the commands via SSH without a TTY.

     a. Edit `/etc/sudoers.d/zenoss` or `/etc/sudoers`, if `sudoers.d` is not supported and add the following lines to the bottom of the file:

     ```
     Defaults:zenmonitor !requiretty
     Cmnd_Alias ZENOSS_LVM_CMDS = /sbin/pvs, /sbin/vgs, /sbin/lvs, \
         /usr/sbin/pvs, /usr/sbin/vgs, /usr/sbin/lvs
     Cmnd_Alias ZENOSS_SVC_CMDS = /bin/systemctl list-units *, \
         /bin/systemctl status *, /sbin/initctl list, /sbin/service --
     status-all, \
         /usr/sbin/dmidecode
     zenmonitor ALL=(ALL) NOPASSWD: ZENOSS_LVM_CMDS, ZENOSS_SVC_CMDS
     ```

     b. Save the changes, ensuring all the paths for these commands are correct.

Preparing Windows servers for monitoring

Cisco UCS Performance Manager uses SNMP or WinRM to monitor Microsoft Windows systems as follows:

- Microsoft Windows Server 2106 - WinRM only.

  SNMP support does not exist for Windows Server 2106.
- Microsoft Windows Server 2012 and 2012 R2 - WinRM only.

  SNMP support does not exist for Windows Server 2012 .
- Microsoft Windows Server 2008 R2 - SNMP v1/v2 or WinRM.

SNMP v3 support does not exist for Windows Server 2008 R2.

To prepare a Windows 2008 system for SNMP monitoring, start the SNMP service.

To prepare a Windows system for WinRM monitoring, refer to the appendix, "Preparing Windows Systems."

Preparing hypervisor devices

This section describes how to prepare vSphere and Hyper-V hypervisors for monitoring.

vSphere endPoint

Cisco UCS Performance Manager uses SOAP to monitor VMware vSphere servers running the following versions of vSphere:

- 4.1
- 5.0
- 5.1
- 5.5
- 6.0

To prepare to monitor a VMware vSphere server:

- Verify that you are running a supported version of the software.
- Obtain the user name and password of an account on the server that is authorized to use the vSphere API.
- Determine whether to use SSL.

Hyper-V

Cisco UCS Performance Manager uses WinRM to monitor the following Microsoft Hyper-V systems:

- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V Server 2012 and 2012 R2
- Microsoft Hyper-V Server 2008 and 2008 R2

To prepare a Hyper-V system for WinRM monitoring, refer to the appendix, "Preparing Windows Systems."

Validating configuration using Inspector tool

Once you have set up your environment, you can validate your configuration using Inspector. The Inspector tool is typically installed on the Control Center master host and performs read-only checks on your environment and provides advice on resolving potential issues.

For more information on the Inspector tool, including download and installation instructions see the following knowledge base article: *Inspector: A tool to validate configuration*.

Optional: Enabling monitoring on IPv6 networks

This procedure describes how to configure Cisco UCS Performance Manager to enable monitoring of devices that are located on an IPv6 network. The network must be reachable from the IPv4 network environment in which Control Center is deployed.

Use this procedure to route an IPv6 address block to Control Center using Docker's virtual bridge interface, `docker0`. Cisco UCS Performance Manager can monitor IPv6 devices that have addresses in the routed block.

To perform this procedure, each node in a Control Center cluster needs a unique IPv6 prefix routed to it by an upstream router, and the Docker Engine service on each node in the cluster needs to be configured to forward IPv6 packets.

For example, a multi-host deployment with one master host and three delegates could have the IPv6 configuration in the following table.

Control Center host	IPv6 link prefix	IPv6 routed prefix
Master	2001:DB8:ABCD:1000::500/64	2001:DB8:ABCD:2000::/64
Delegate 1	2001:DB8:ABCD:1000::501/64	2001:DB8:ABCD:2001::/64
Delegate 2	2001:DB8:ABCD:1000::502/64	2001:DB8:ABCD:2002::/64
Delegate 3	2001:DB8:ABCD:1000::503/64	2001:DB8:ABCD:2003::/64

The following example shows how to configure the static routes in the preceding table on an upstream Cisco router:

```
ipv6 route 2001:DB8:ABCD:2000::/64 2001:DB8:ABCD:1000::500
ipv6 route 2001:DB8:ABCD:2001::/64 2001:DB8:ABCD:1000::501
ipv6 route 2001:DB8:ABCD:2002::/64 2001:DB8:ABCD:1000::502
ipv6 route 2001:DB8:ABCD:2003::/64 2001:DB8:ABCD:1000::503
```

Perform the following steps:

1. Log on to the Control Center master host as `root`, or as a user with superuser privileges.
2. Configure IPv6 packet forwarding.
   a. Open `/etc/sysctl.d/ipv6.conf` with a text editor.
   b. Add or edit the following line:

      ```
      net.ipv6.conf.all.forwarding=1
      ```

   c. Save the file, and then close the text editor.
3. Enable IPv6 packet forwarding without rebooting the host.

   ```
   sysctl -w net.ipv6.conf.all.forwarding=1
   ```

4. Configure Docker for IPv6 communications.
   a. Open `/etc/sysconfig/docker` with a text editor.
   b. Add the following flags to the end of the *OPTIONS* declaration.
      Replace *Subnet-Block* with the IPv6 subnet to route to Control Center, in CIDR notation:

      ```
      --ipv6 --fixed-cidr-v6="Subnet-Block"
      ```

   c. Change the delimiter of the *OPTIONS* declaration to the apostrophe character (`'`).

      The default delimiter of the *OPTIONS* declaration is the quotation mark character (`"`), which is the same delimiter used with the `--fixed-cidr-ipv6` flag.
   d. Save the file, and then close the text editor.
5. Restart the Docker service.

   ```
   systemctl restart docker
   ```

6 Use the Docker container of the **zenping** service to ping a known IPv6 address.

```
serviced service attach zenping ping6 -c 1 ipv6.google.com
```

If the ping is successful, Docker is able to resolve IPv6 addresses and you can monitor devices on the IPv6 network.

Enabling access to browser interfaces 2

Control Center and Cisco UCS Performance Manager have independent browser interfaces that are served by independent web servers. Both web servers are configured to use SSL/TLS communications.

The Control Center web server listens at the hostname of the Control Center master host and port 50443. For a Control Center master host with the fully qualified domain name (FQDN) `cc-master.example.com`, the hostname URL is `https://cc-master:50443`. You can substitute an IP address for the hostname portion of the URL.

The Cisco UCS Performance Manager web server listens at a *port public endpoint* and a *virtual host public endpoint*.

- The default *port public endpoint* is the hostname of the Control Center master host and port 443. For the FQDN `cc-master.example.com`, the URL of the default port public endpoint is `https://cc-master`. If the Control Center master host has more than one network interface, you can configure additional port public endpoints with different hostnames. Also, you can disable TLS communications for a port public endpoint.

  To use a port public endpoint to gain access to the Cisco UCS Performance Manager browser interface, no additional network name resolution entries are required. The default entries for the network interfaces of the Control Center master host are sufficient.
- The default *virtual host public endpoint* is the text `ucspm` prepended to the hostname of the Control Center master host and port 50443. For the FQDN `cc-master.example.com`, the URL of the default virtual host public endpoint is `https://ucspm.cc-master:50443`. You can change the name of the default virtual host and configure additional virtual host public endpoints.

  To use a virtual host public endpoint to gain access to the Cisco UCS Performance Manager browser interface, you must add name resolution entries for the virtual host to the DNS servers in your environment or to the hosts files of individual client systems.

Setting up Cisco UCS Performance Manager 3

This section describes how to use the Cisco UCS Performance Manager Setup Wizard to accept the end-user license agreement, provide your license key, define users and passwords, set up UCS Central and UCS Domains, add infrastructure, and set up SMTP.

The wizard runs the first time you log in to the Cisco UCS Performance Manager browser interface. (For more information about supported browsers and client operating systems, see the *Cisco UCS Performance Manager Release Notes*.

To open the Cisco UCS Performance Manager browser interface, navigate to the port public endpoint or virtual host port public endpoint. For more information, see *Enabling access to browser interfaces* on page 12.

Note The wizard times out after 20 minutes if you have not completed it. To start it again, close its browser window or tab, and then log in again.

To complete the Setup Wizard, you need the following items:

- Authorization to accept the Cisco UCS Performance Manager end-user license agreement on behalf of your organization.
- A password for the default administrative account (`admin`).
- A user name and password for one additional administrative account.
- The license key for your product (Cisco UCS Performance Manager Express or Cisco UCS Performance Manager). To obtain a license key, contact your Cisco representative.
- The hostnames or IP addresses of UCS Central and UCS Domains in your environment.
- The user name and password of an account on each server that is authorized for read access to the resources you plan to monitor.

The wizard includes the **Add Infrastructure** page, which is optional. The **Add Infrastructure** page is a standard part of the Cisco UCS Performance Manager interface, so you can use it at any time.

Accepting the license agreement

Perform this procedure after installing Cisco UCS Performance Manager on a virtual machine and starting it in Control Center.

1. In a web browser, navigate to the login page of the Cisco UCS Performance Manager interface.

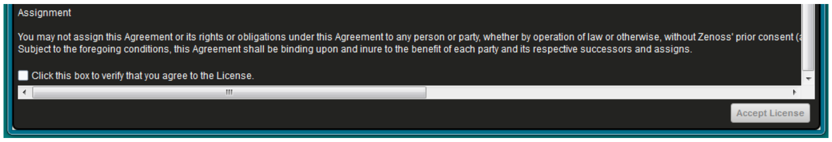
   Cisco UCS Performance Manager redirects the first login attempt to the **Setup** page, which includes the **End User License Agreement** (EULA) dialog box.

Note If you cannot resolve the hostname, check your DNS server or add an entry to the `hosts` file on the client machine. For more information, see *Enabling access to browser interfaces* on page 12.

2 Read the agreement.

3 At the bottom of the EULA dialog box, check the box to verify agreement, and then click **Accept License**.

Figure 1: Bottom of EULA dialog box



Assignment

You may not assign this Agreement or its rights or obligations under this Agreement to any person or party, whether by operation of law or otherwise, without Zenoss' prior consent (a

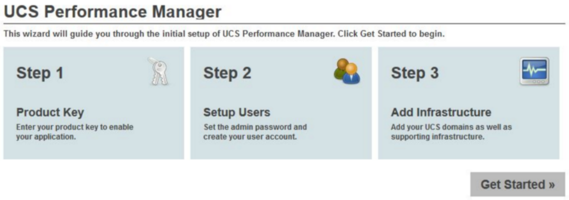
Subject to the foregoing conditions, this Agreement shall be binding upon and inure to the benefit of each party and its respective successors and assigns.

□ Click this box to verify that you agree to the License.

Providing a license key

After accepting the EULA, perform this procedure. You need a license key file for Cisco UCS Performance Manager Express or Cisco UCS Performance Manager. The license key file must be located on the workstation from which you gain access to the Cisco UCS Performance Manager browser interface. For more information about obtaining a license key file, contact your Cisco representative.

1 On the Cisco**Cisco UCS Performance Manager Setup** page, click **Get Started**.



UCS Performance Manager

This wizard will guide you through the initial setup of UCS Performance Manager. Click Get Started to begin.

Step 1

Product Key

Enter your product key to enable your application.

Step 2

Setup Users

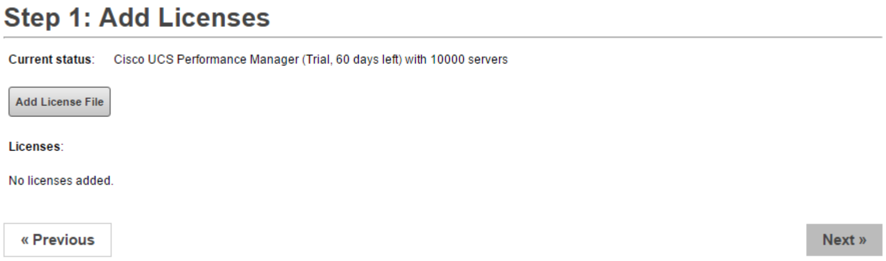
Set the admin password and create your user account.

Step 3

Add Infrastructure

Add your UCS domains as well as supporting infrastructure.

2 On the **Add Licenses** page, click **Add License File**.



Step 1: Add Licenses

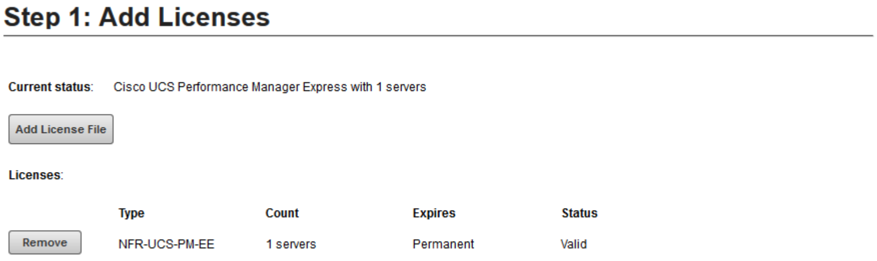
Current status: Cisco UCS Performance Manager (Trial, 60 days left) with 10000 servers

Licenses:

No licenses added.

Note If you do not have your license file yet, you can use the trial version for up to 30 days. You can enter your license file at a later date through the browser interface. For more information, refer to the "Product Licensing" section of the *Cisco UCS Performance Manager Administration Guide*.

3 In the **Open** dialog box, choose your license file, and then click **Open**.



Step 1: Add Licenses

Current status: Cisco UCS Performance Manager Express with 1 servers

Licenses:

	Type	Count	Expires	Status
Remove	NFR-UCS-PM-EE	1 servers	Permanent	Valid

4 Compare the product name and number of servers in the **Current Status** field with the product that you purchased, and then proceed as follows:

- If the information matches your purchase, click **Next** to continue to the **Setup Users** step.
- If the information does not match your purchase, click **Remove**, and then contact your Cisco representative.

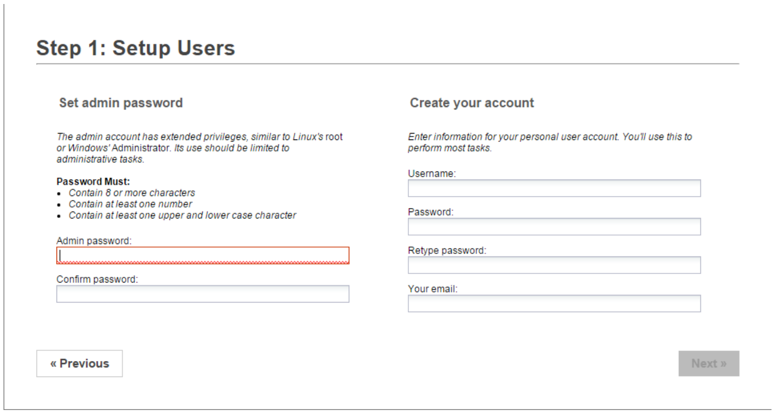
Note The Cisco UCS Performance Manager browser interface includes an option for changing your license key.

Setting up users

Complete this procedure to create a password for the `admin` user and create at least one additional user account.

1 In the **Set admin password** area, enter and confirm a password for the `admin` user account.

Passwords require eight or more characters, including one capital letter and one digit.



The admin account has extended privileges, similar to Linux's root or Windows' Administrator. *Its use should be limited to administrative tasks.*

Password Must:
- *Contain 8 or more characters*
- *Contain at least one number*
- *Contain at least one upper and lower case character*

Enter information for your personal user account. You'll use this to perform most tasks.

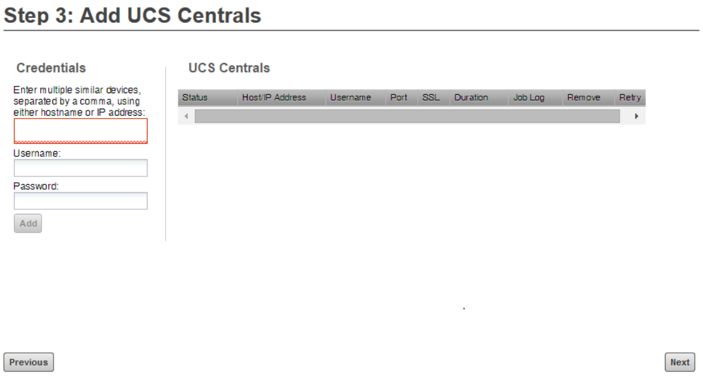
2 In the **Create your account** area, create one additional administrative user account name and password.

3 Click **Next** to go **Add UCS Centrals**.

Adding UCS Centrals

This procedure is optional. If you are not monitoring a UCS Central, click **Next** to skip to the next step. Otherwise, follow this procedure to add your UCS Centrals.

1 On the **Add UCS Centrals** page, provide connection credentials for one or more UCS Centrals.



Enter multiple similar devices, separated by a comma, using either hostname or IP address:

a Specify the fully qualified domain name or IP address of your UCS Central hosts.

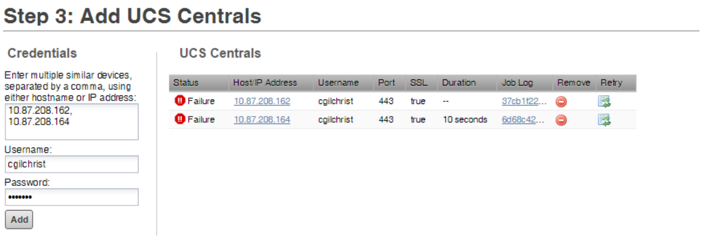
To list multiple devices, separate hostnames or IP addresses with a comma.

b In **Username**, specify the name of a user account in UCS Central that is authorized for read access to the resources that you plan to monitor.

c Specify the password for the user name that you specified.

d Click **Add**.

2 In the **UCS Centrals** table, review the **Status** column and proceed as follows:



Step 3: Add UCS Centrals

Credentials

Enter multiple similar devices, separated by a comma, using either hostname or IP address:

10.87.208.162,
10.87.208.164

Username: cgilchrist

Password: •••••••

UCS Centrals

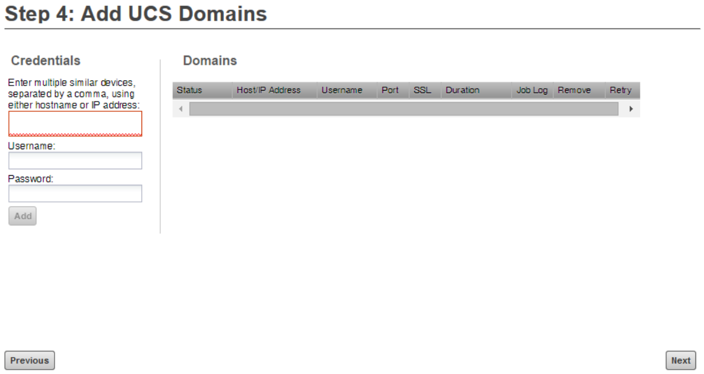
Status	Host/IP Address	Username	Port	SSL	Duration	Job Log	Remove	Retry
Failure	10.87.208.162	cgilchrist	443	true	--	37cb1f22...	⊖	
Failure	10.87.208.164	cgilchrist	443	true	10 seconds	6d68c42...	⊖	

- If the final message is `Failure`, click **Remove**, and then try again to add a domain.
- If the final message is `Success`, if needed, add another domain, and then click **Next**.

Adding UCS domains

This procedure is optional. If you do not have connection credentials or you want to enter them later, click **Next** to skip to the next step. Otherwise, follow this procedure to add UCS domains.

1 On the **Add UCS Domains** page, provide connection credentials for one or more UCS domains.



Step 4: Add UCS Domains

Credentials

Enter multiple similar devices, separated by a comma, using either hostname or IP address:

Username:

Password:

Domains

Status	Host/IP Address	Username	Port	SSL	Duration	Job Log	Remove	Retry

a Specify the fully qualified domain name or IP address of a UCS domain server.

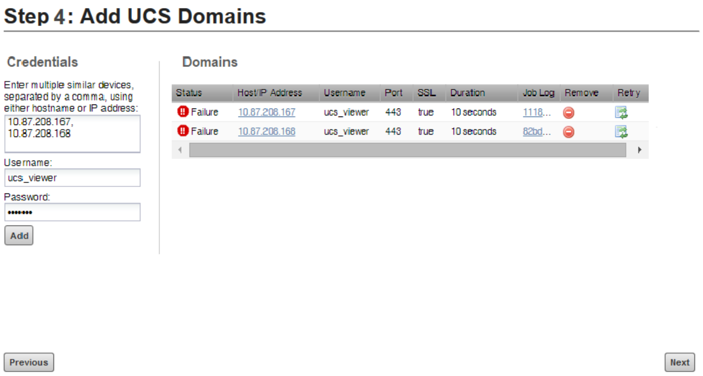
To list multiple devices, separate hostnames or IP addresses with a comma.

b In **Username**, specify the name of a user account in the UCS domain that is authorized for read access to the resources you plan to monitor.

c Specify the password for the user name that you specified.

d Click **Add**.

2 In the **Domains** table, review the **Status** column and proceed as follows:



Step 4: Add UCS Domains

Credentials

Enter multiple similar devices, separated by a comma, using either hostname or IP address:

10.87.208.167,
10.87.208.168

Username: ucs_viewer

Password: •••••••

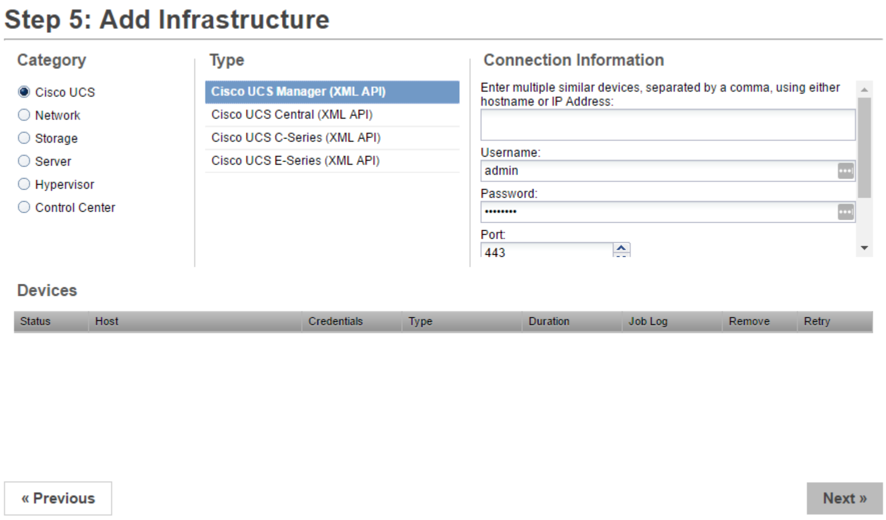
Domains

Status	Host/IP Address	Username	Port	SSL	Duration	Job Log	Remove	Retry
Failure	10.87.208.167	ucs_viewer	443	true	10 seconds	1118...	⊖	↻
Failure	10.87.208.168	ucs_viewer	443	true	10 seconds	82bd...	⊖	↻

- If the final message is `Failure`, click **Remove**, and then try again to add a domain.
- If the final message is `Success`, if needed, add another domain, and then click **Next**.

Adding Infrastructure

The **Add Infrastructure** step is optional, as you may add devices through the **Add Infrastructure** page in Cisco UCS Performance Manager at any time.



Step 5: Add Infrastructure

Category

● Cisco UCS
○ Network
○ Storage
○ Server
○ Hypervisor
○ Control Center

Type

Cisco UCS Manager (XML API)
Cisco UCS Central (XML API)
Cisco UCS C-Series (XML API)
Cisco UCS E-Series (XML API)

Connection Information

Enter multiple similar devices, separated by a comma, using either hostname or IP Address:

Username: admin

Password: ••••••••

Port: 443

Devices

Status	Host	Credentials	Type	Duration	Job Log	Remove	Retry

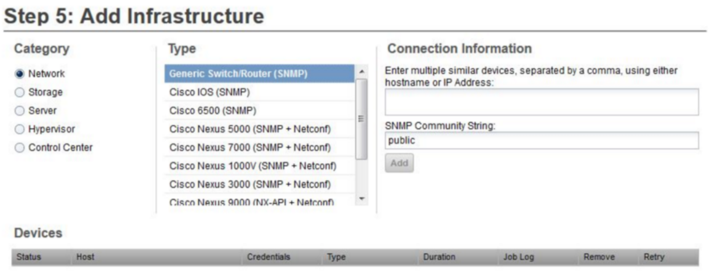
If you wish to exit the wizard and infrastructure at a later time, click **Finish**. You will then be taken to the Dashboard.

Adding Network Devices

To perform this procedure, you need a license for Cisco UCS Performance Manager. If your license is Cisco UCS Performance Manager Express, proceed to *Adding Server Devices* on page 19.

This optional procedure is for the **Add Infrastructure** step of the Setup Wizard.

1 In the **Category** area, select **Network**.



Step 5: Add Infrastructure

Category

● Network
○ Storage
○ Server
○ Hypervisor
○ Control Center

Type

Generic Switch/Router (SNMP)
Cisco IOS (SNMP)
Cisco 6500 (SNMP)
Cisco Nexus 5000 (SNMP + Netconf)
Cisco Nexus 7000 (SNMP + Netconf)
Cisco Nexus 1000V (SNMP + Netconf)
Cisco Nexus 3000 (SNMP + Netconf)
Cisco Nexus 9000 (NX-API + Netconf)

Connection Information

Enter multiple similar devices, separated by a comma, using either hostname or IP Address:

SNMP Community String: public

Add

Devices

Status	Host	Credentials	Type	Duration	Job Log	Remove	Retry

2 In the **Type** list, select the product model of the switch or router to add.

The protocol used to gather data from the device is included in the list, in parentheses.

Note Some of the devices in the **Type** list, such as the Nexus 7000 and 9000 switches, represent a large number of discrete monitoring endpoints. If you are unsure whether the Cisco UCS Performance Manager virtual machine size you have selected supports the number of high-density devices you wish to monitor, contact your Cisco representative.

---

3 In the **Connection Information** area, specify the devices to add. Depending on the type of network device you select, you will have different connection information fields to enter. If the field described below is not present, then it does not apply to your selection.

a In the **Enter multiple similar devices, separated by a comma, using either hostname or IP Address** field, enter the hostname or IP address of one or more switch or router devices on your network.

b In the **SNMP Community String** field, change the default (`public`) if necessary.

This field is not used if the selected device supports both SNMP and NETCONF, and you provide a user name and password.

c In the **Username** or **Netconf Username** field, enter the name of a user account on the device.

d In the **Password** or **Netconf Password** field, enter the password of the user account specified in the previous field.

e Click **Add**.

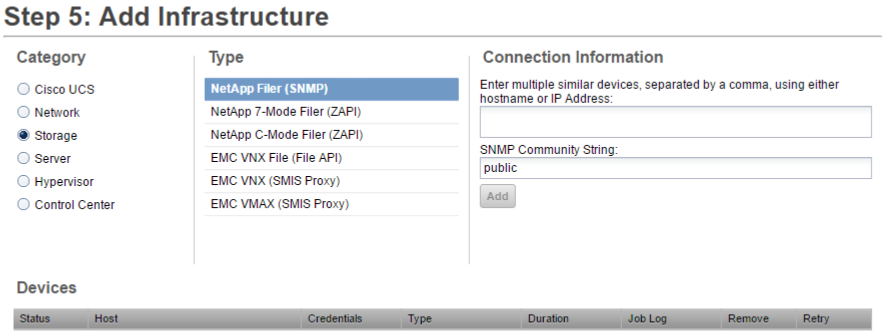
If you are finished adding network devices, click **Next**.

Adding Storage Devices

To perform this procedure, you need a license for Cisco UCS Performance Manager. If your license is Cisco UCS Performance Manager Express, proceed to *Adding Server Devices* on page 19.

This option is part of step 5 of the Setup Wizard.

1 In the **Category** area, select **Storage**.



Step 5: Add Infrastructure

Category

○ Cisco UCS
○ Network
● Storage
○ Server
○ Hypervisor
○ Control Center

Type

NetApp Filer (SNMP)
NetApp 7-Mode Filer (ZAPI)
NetApp C-Mode Filer (ZAPI)
EMC VNX File (File API)
EMC VNX (SMIS Proxy)
EMC VMAX (SMIS Proxy)

Connection Information

Enter multiple similar devices, separated by a comma, using either hostname or IP Address:

SNMP Community String: public

Add

Devices

Status	Host	Credentials	Type	Duration	Job Log	Remove	Retry

2 In the **Type** list, select the product model of the storage device to add.

The protocol used to gather data from the device is included in the list, in parentheses.

3 In the **Connection Information** area, specify the devices to add.

   a In the **Enter multiple similar devices, separated by a comma, using either hostname or IP Addresses** field, enter the hostname or IP address of one or more storage devices on your network.

   b Optional: In the **Username** field, enter the name of a user account on the device.

   This field is not present when the device protocol is SNMP.

   c Optional: In the **Password** field, enter the password of the user account specified in the previous field.

   This field is not present when the device protocol is SNMP.

   d Optional: In the **Port** field, enter the port at which the device listens for data collection requests.

   This field is present only when the device protocol is SMIS Proxy.

   e Check the **Use SSL?** check box to use secure communications to collect data, or uncheck the check box to use insecure communications.

   This field is not present when the device protocol is SNMP.

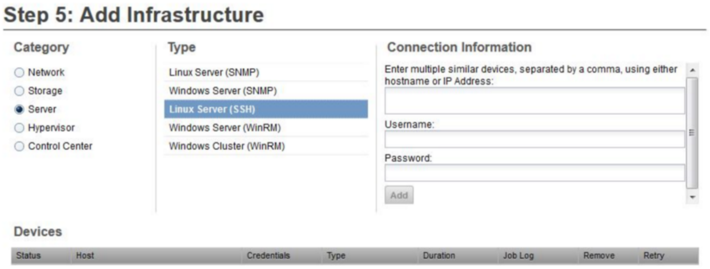
   f Click **Add**.

If you are finished adding storage devices, click **Next**.

Adding Server Devices

This option is part of step 5 of the Setup Wizard.

1 In the **Category** area, select **Servers**.



Step 5: Add Infrastructure

Category

○ Network
○ Storage
● Server
○ Hypervisor
○ Control Center

Type

Linux Server (SNMP)
Windows Server (SNMP)
Linux Server (SSH)
Windows Server (WinRM)
Windows Cluster (WinRM)

Connection Information

Enter multiple similar devices, separated by a comma, using either hostname or IP Address:

Username:

Password:

Devices

Status	Host	Credentials	Type	Duration	Job Log	Remove	Retry

2 In the **Type** list, select the operating system and monitoring protocol of the server to add.

The protocol used to gather data from the device is included in the list, in parentheses.

3 In the **Connection Information** area, specify the servers to add.

   a In the **Enter multiple similar devices, separated by a comma, using either hostname or IP Addresses** field, enter the hostname or IP address of one or more server devices on your network.

   b Optional: In the **SNMP Community String** field, change the default (`public`) if necessary.

   This field is only present when the device protocol is SNMP.

   c Optional: In the **Username** field, enter the name of a user account on the device.

   This field is not present when the device protocol is SNMP.

   d Optional: In the **Password** field, enter the password of the user account specified in the previous field.

   This field is not present when the device protocol is SNMP.

   e Optional: In the **AD Domain Controller** field, enter the IP address or hostname of the Active Directory Domain Controller on your network.

   This field is only present when the device protocol is WinRM.

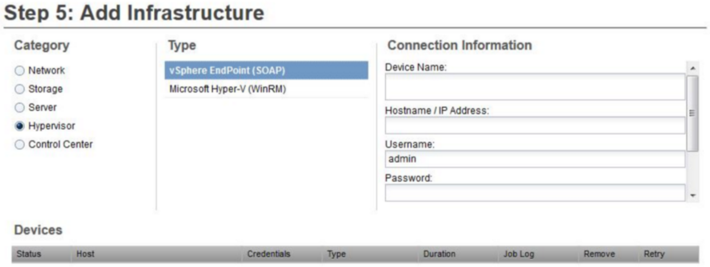
   f Click **Add**.

If you are finished adding server devices, click **Next**.

Adding Hypervisor Devices

This option is part of step 5 of the Setup Wizard.

1 In the **Category** area, select **Hypervisor**.



Step 5: Add Infrastructure

Category

○ Network
○ Storage
○ Server
● Hypervisor
○ Control Center

Type

vSphere EndPoint (SOAP)
Microsoft Hyper-V (WinRM)

Connection Information

Device Name:

Hostname / IP Address:

Username: admin

Password:

Devices

Status	Host	Credentials	Type	Duration	Job Log	Remove	Retry

2 In the **Type** list, select the hypervisor service to add.

3 In the **Connection Information** area, specify the service to add.

a In the **Device Name** field, enter the name of the hypervisor service.

b In the **Hostname / IP Address** field, enter the hostname or IP address of the hypervisor service.

c In the **Username** field, enter the name of a user account on the host.

d In the **Password** field, enter the password of the user account specified in the previous field.

e Optional: Check the **Use SSL?** check box to use secure communications to collect data (recommended).

This field is only present when the device protocol is SOAP.

f Optional: Enter information in the **AD Domain Controller**, **Version**, **HTTP or HTTPS**, and **Port** fields.

These fields are only present when the device protocol is WinRM.

g Click **Add**.

If you are finished adding hypervisor devices, click **Finish**.

Adding Control Center

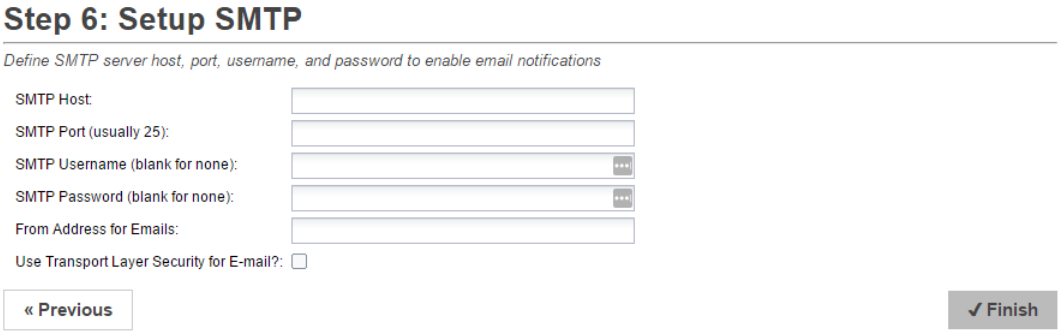
The Control Center is the internal application management and orchestration system for . It is automatically added Control Center as a managed resource so that you can see the internal components and their performance data.

Click **Finish** if you are done adding your devices. You can always add more devices at a later date.

Setting up SMTP

Use this procedure to configure Cisco UCS Performance Manager to use an existing email server.

1 On the **Setup SMTP** page, provide information about an email server for Cisco UCS Performance Manager to use.



Step 6: Setup SMTP

Define SMTP server host, port, username, and password to enable email notifications

SMTP Host:

SMTP Port (usually 25):

SMTP Username (blank for none):

SMTP Password (blank for none):

From Address for Emails:

Use Transport Layer Security for E-mail?: □

- **a** In the **SMTP Host** field, enter the IP address or host name of an existing email server.
- **b** In the **SMTP Port (usually 25)** field, enter the port at which the server listens for incoming messages.
- **c** In the **SMTP Username (blank for none)** field, enter the name of an account that is authorized to forward messages to the server.
- **d** In the **SMTP Password (blank for none)** field, enter the password of the account that is authorized to forward messages to the server.
- **e** In the **From Address for Emails** field, enter the originating address of messages forwarded to the server.
- **f** To enable TLS, click the **Use Transport Layer Security for E-mail** checkbox.

2 Click **Finish**.

Updating device authentication details

For each device added to the database and set to its proper device class, Cisco UCS Performance Manager may require additional or different authentication information before it can gather device information and monitor the device.

For example, for a device in the /Server/Windows class, you must supply your Windows user name and password before the system can monitor the device. To do this:

1. Click a device name in the devices list.
   The Device summary page appears.
2. Select Configuration Properties from the left panel.
3. Double-click the zWinRMUser configuration property to display the Edit Config Property dialog.
4. Enter your Windows user name in the Value field, and then click **Submit**.
5. Double-click the zWinRMPassword configuration property to display the Edit Config Property dialog.
6. Enter your Windows password in the Value field, and then click **Submit**.

Similarly, for a device in the /Server/SSH/GenericLinux class, you must supply your SSH user name and password. Set these values in the device's zCommandUsername and zCommandPassword configuration properties.

Note After making changes, you should remodel the device to ensure the authentication changes are valid.

Note Cisco UCS Performance Manageruses Advanced Encryption Standard (AES) with a 256-bit key size to encrypt all passwords, and stores them in the Zope object database.

Adding or editing information on a device record

You may want to add or edit details about a device.

To add or edit information:

1. Click a device name in the devices list. The Device overview page appears.
2. You can select values to change, or click the "edit" link adjacent to a label to edit that value. Enter or change information in one or more areas, and then click **Save** to save your changes.

Starting and stopping a multi-host deployment

4

Use the procedures in this chapter to start and stop a multi-host deployment of Cisco UCS Performance Manager.

Starting Cisco UCS Performance Manager

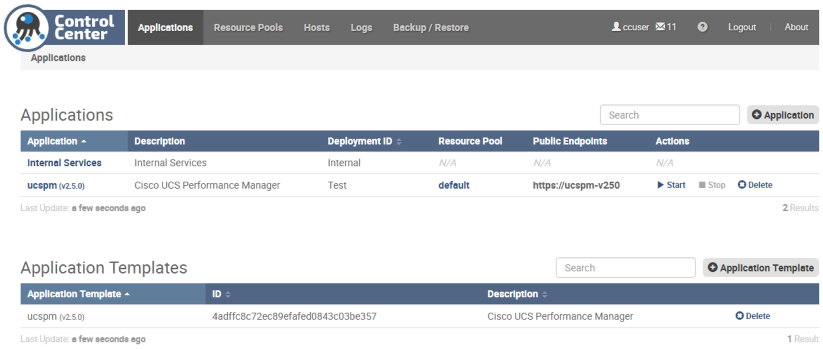
To perform this procedure, you need:

- Administrative access to the hypervisor server that hosts your Cisco UCS Performance Manager guest systems
- A supported client system and browser
- A user account on the Control Center master host with access privileges for the Control Center browser interface

For more information, refer to the *Cisco UCS Performance Manager Installation Guide*.

1. Log in to the hypervisor server that hosts your Cisco UCS Performance Manager guest systems.
2. Start each of the Cisco UCS Performance Manager guest systems as close to the same time as possible.
3. Log in to the Control Center browser interface.

   The web server that supports the browser interface takes a minute or two to start.



Applications

Application	Description	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	Internal	N/A	N/A	N/A
ucspm (v2.5.0)	Cisco UCS Performance Manager	Test	default	https://ucspm-v250	▶ Start ■ Stop Delete

Last Update: a few seconds ago 2 Results

Application Templates

Application Template	ID	Description	
ucspm (v2.5.0)	4adffc8c72ec89efafed0843c03be357	Cisco UCS Performance Manager	Delete

Last Update: a few seconds ago 1 Result

4. In the **Actions** column of the **Applications** table, click **Start** for **ucspm**.
5. In the **Start Service** dialog, click **Start Service and 33 Children**.
6. Optional: Monitor the startup, if desired.
   a. In the **Applications** table, click **ucspm**.
   b. Scroll down to the **Services** table and review the **Health** icon for each service.

As services are started the **Health** icon changes to a check mark.

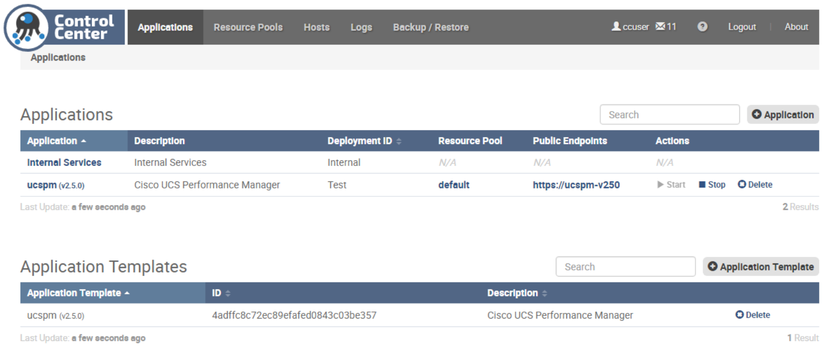
Stopping Cisco UCS Performance Manager

To perform this procedure, you need:

- Administrative access to the hypervisor server that hosts your Cisco UCS Performance Manager guest systems
- A supported client system and browser
- A user account on the Control Center master host with access privileges for the Control Center browser interface

For more information, refer to the *Cisco UCS Performance Manager Installation Guide*.

1 Log in to the Control Center browser interface.



Applications

Application	Description	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	Internal	N/A	N/A	N/A
ucspm (v2.5.0)	Cisco UCS Performance Manager	Test	default	https://ucspm-v250	▶ Start ■ Stop Delete

Last Update: a few seconds ago 2 Results

Application Templates

Application Template	ID	Description	
ucspm (v2.5.0)	4adffc8c72ec89efafed0843c03be357	Cisco UCS Performance Manager	Delete

Last Update: a few seconds ago 1 Result

2 In the **Actions** column of the **Applications** table, click **Stop** for **ucspm**.

3 In the **Stop Service** dialog, click **Stop Service and 33 Children**.

4 Optional: Monitor the stop, if desired.

   a In the **Applications** table, click **ucspm**.

   b Scroll down to the **Services** table and review the **Status** message for each service.

   As services are stopped the **Status** message changes to **Stopped**.

5 Log in to the hypervisor server that hosts your Cisco UCS Performance Manager guest systems.

6 Stop each of the Cisco UCS Performance Manager guest systems.

Default server passwords 5

Cisco UCS Performance Manager adds global configuration parameters to the run-time environments (Docker containers) of every service. The parameters include the default passwords of two MariaDB database servers, a RabbitMQ server, and a Zope authentication server. The default passwords are the same in all Cisco UCS Performance Manager distributions. To avoid security issues, Cisco recommends changing the default passwords of the preceding servers.

Note Changes to global configuration parameters persist across upgrades.

The following list associates the affected servers, their Cisco UCS Performance Manager services, and their account information.

Note The list includes both account names and passwords. Cisco recommends changing the passwords of each account and strongly discourages changing the account names.

MariaDB server for the events database

Service: **mariadb-events**

Administrator account: `global.conf.zep-admin-user`

Administrator password: `global.conf.zep-admin-password`

User account: `global.conf.zep-user`

User password :`global.conf.zep-password`

MariaDB server for the models database

Service: **mariadb-model**

Administrator account: `global.conf.zodb-admin-user`

Administrator password: `global.conf.zodb-admin-password`

User account: `global.conf.zodb-user`

User password: `global.conf.zodb-password`

RabbitMQ server

Service: **RabbitMQ**

User account: `global.conf.amqpuser`

User password: `global.conf.amqppassword`

Zope authentication server

Service: **Zauth**

User account: `global.conf.zauth-username`

User password: `global.conf.zauth-password`

Changing MariaDB passwords

Use this procedure to change the passwords of the MariaDB databases for event and model data.

To perform this procedure, the **mariadb-events** and **mariadb-model** child services of Cisco UCS Performance Manager must be running.

1 Change the passwords of the events database server.

a Log in to the Docker container of the **mariadb-events** service as `zenoss`.

```
serviced service attach mariadb-events su - zenoss
```

b Start an interactive session.

```
export TERM=dumb; mysql -u root
```

c Access the administration database.

```
USE mysql
```

d Set the password of the `root` user.
Replace *New-Password* with a new password:

```
SET PASSWORD FOR 'root'@'127.0.0.1' = PASSWORD('New-Password');
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('New-Password');
```

Record the password for use in a subsequent step.

e Update the password of the `zenoss` user.
Replace *New-Password* with a new password:

```
SET PASSWORD FOR 'zenoss'@'127.0.0.1' = PASSWORD('New-Password');
SET PASSWORD FOR 'zenoss'@'%' = PASSWORD('New-Password');
```

Record the password for use in a subsequent step.

f Exit the interactive session.

```
QUIT
```

The MariaDB server loads the grant tables into memory immediately when account management statements like `SET PASSWORD` are used, so the `FLUSH PRIVILEGES` statement is not necessary.

g Log out of the Docker container.

```
exit
```

2 Change the passwords of the model database server.

a Log in to the Docker container of the **mariadb-model** service as `zenoss`.

```
serviced service attach mariadb-model su - zenoss
```

b Start an interactive session.

```
export TERM=dumb; mysql -u root
```

c Access the administration database.

```
USE mysql
```

d Set the password of the `root` user.
Replace *New-Password* with a new password:

```
SET PASSWORD FOR 'root'@'127.0.0.1' = PASSWORD('New-Password');
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('New-Password');
```

Record the password for use in a subsequent step.

e Update the password of the `zenoss` user.
Replace *New-Password* with a new password:

```
SET PASSWORD FOR 'zenoss'@'127.0.0.1' = PASSWORD('New-Password');
SET PASSWORD FOR 'zenoss'@'%' = PASSWORD('New-Password');
```

Record the password for use in a subsequent step.

f Exit the interactive session.

```
QUIT
```

g Log out of the Docker container.

```
exit
```

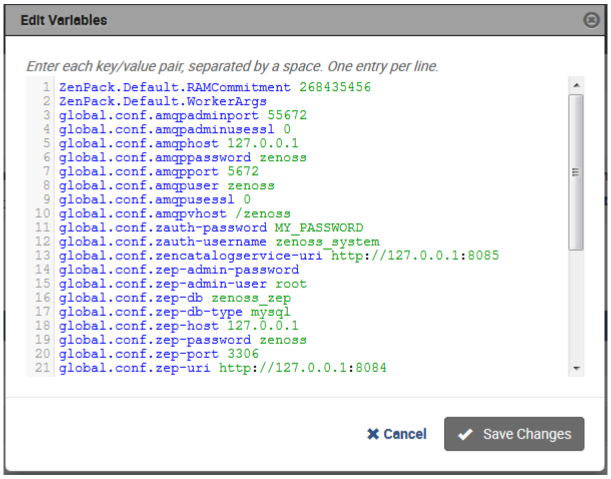
3 Log in to the Control Center browser interface.

4 In the **Applications** table, click **ucspm**.

5 In the application title line, click **Edit Variables**.

Initially, the application title line appears immediately below the Control Center banner at the top of the page. When you scroll down the page, the application title line persists at the top of the page.

Figure 2: Edit Variables dialog



Enter each key/value pair, separated by a space. One entry per line.

```
ZenPack.Default.RAMCommitment 268435456
ZenPack.Default.WorkerArgs
global.conf.amqpadminport 55672
global.conf.amqpadminusessl 0
global.conf.amqphost 127.0.0.1
global.conf.amqppassword zenoss
global.conf.amqpport 5672
global.conf.amqpuser zenoss
global.conf.amqpusessl 0
global.conf.amqpvhost /zenoss
global.conf.zauth-password MY_PASSWORD
global.conf.zauth-username zenoss_system
global.conf.zencatalogservice-uri http://127.0.0.1:8085
global.conf.zep-admin-password
global.conf.zep-admin-user root
global.conf.zep-db zenoss_zep
global.conf.zep-db-type mysql
global.conf.zep-host 127.0.0.1
global.conf.zep-password zenoss
global.conf.zep-port 3306
global.conf.zep-uri http://127.0.0.1:8084
```

6 Update the passwords of the event database server.

a In the **Edit Variables** dialog, locate the `global.conf.zep-password` variable.

b Replace its value with the password specified previously for the `zenoss` user of the events database server.

c Locate the `global.conf.zep-admin-password` variable.

d Replace its value with the password specified previously for the `root` user of the events database server.

7 Update the passwords of the model database server.

   a Locate the `global.conf.zodb-password` variable.

   b Replace its value with the password specified previously for the `zenoss` user of the model database server.

   c Locate the `global.conf.zodb-admin-password` variable.

   d Replace its value with the password specified previously for the `root` user of the model database server.

   e At the bottom of the **Edit Variables** dialog, click **Save Changes**.

8 In the application title line, click **Restart**.

Changing the RabbitMQ server password

Use this procedure to change the password of the RabbitMQ server.

To perform this procedure, the **mariadb-model** child services of Cisco UCS Performance Manager must be running.

1 Change the password of the `zenoss` user.

   a Log in to the Docker container of the **RabbitMQ** service as `root`.

```
serviced service attach rabbitmq
```

   b Change the password.
   Replace *New-Password* with a new password:

```
rabbitmqctl change_password zenoss New-Password
```

   Record the password for use in a subsequent step.

   c Log out of the Docker container.

```
exit
```

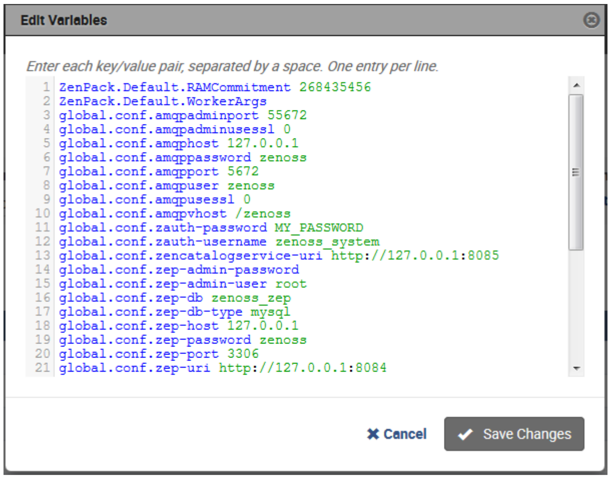
2 Log in to the Control Center browser interface.

3 In the **Applications** table, click **ucspm**.

4 In the application title line, click **Edit Variables**.

Initially, the application title line appears immediately below the Control Center banner at the top of the page. When you scroll down the page, the application title line persists at the top of the page.

Figure 3: Edit Variables dialog



Edit Variables

Enter each key/value pair, separated by a space. One entry per line.

```
ZenPack.Default.RAMCommitment 268435456
ZenPack.Default.WorkerArgs
global.conf.amqpadminport 55672
global.conf.amqpadminusessl 0
global.conf.amqphost 127.0.0.1
global.conf.amqppassword zenoss
global.conf.amqpport 5672
global.conf.amqpuser zenoss
global.conf.amqpusessl 0
global.conf.amqpvhost /zenoss
global.conf.zauth-password MY_PASSWORD
global.conf.zauth-username zenoss_system
global.conf.zencatalogservice-uri http://127.0.0.1:8085
global.conf.zep-admin-password
global.conf.zep-admin-user root
global.conf.zep-db zenoss_zep
global.conf.zep-db-type mysql
global.conf.zep-host 127.0.0.1
global.conf.zep-password zenoss
global.conf.zep-port 3306
global.conf.zep-uri http://127.0.0.1:8084
```

5 Change the password of the RabbitMQ server.

   a. In the **Edit Variables** dialog, locate the `global.conf.amqppassword` variable.
   b. Replace its value with the new password specified previously.
   c. At the bottom of the **Edit Variables** dialog, click **Save Changes**.

6. Restart the **RabbitMQ** service.
   a. Scroll down to the **Services** table, and then locate the **RabbitMQ** service.
   b. In the **Actions** column of the service, click the **Restart** control.

Changing the Zope authentication server password

Use this procedure to change the password of the Zope authentication server.

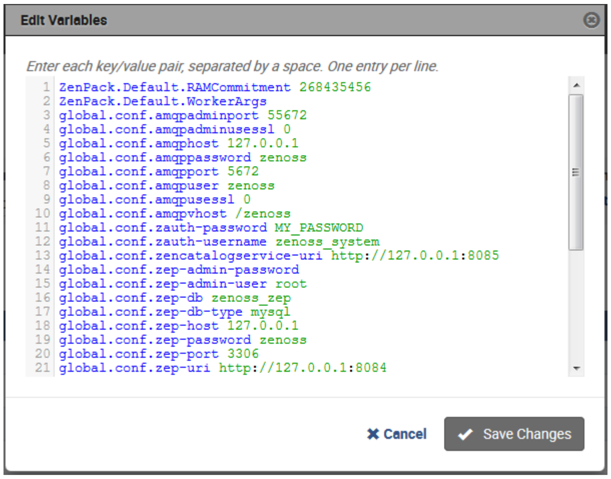
To perform this procedure, the Cisco UCS Performance Manager application must be running. During the procedure, Cisco UCS Performance Manager must be restarted.

1. Log in to the Cisco UCS Performance Manager browser interface as `zenoss_system`.

   The default password is `MY_PASSWORD`.
2. Click the **ADVANCED** tab, and then click **Settings**.
3. From the left column, select **Users**.
4. In the **UserId** table, click the **zenoss_system** link.
5. In the **USER SETTINGS** area, enter a new password in the **Set New Password** field, and then enter it again, in the **Confirm New Password** field.

   Record the password for use in a subsequent step.
6. In the **Current Password for zenoss_system** field, enter the password you used to log in as `zenoss_system`.
7. Click **Save Settings**, and then log out of the browser interface.
8. Log in to the Control Center browser interface.
9. In the **Applications** table, click **ucspm**.
10. In the application title line, click **Edit Variables**.

Figure 4: Edit Variables dialog



Enter each key/value pair, separated by a space. One entry per line.

```
ZenPack.Default.RAMCommitment 268435456
ZenPack.Default.WorkerArgs
global.conf.amqpadminport 55672
global.conf.amqpadminusessl 0
global.conf.amqphost 127.0.0.1
global.conf.amqppassword zenoss
global.conf.amqpport 5672
global.conf.amqpuser zenoss
global.conf.amqpusessl 0
global.conf.amqpvhost /zenoss
global.conf.zauth-password MY_PASSWORD
global.conf.zauth-username zenoss_system
global.conf.zencatalogservice-uri http://127.0.0.1:8085
global.conf.zep-admin-password
global.conf.zep-admin-user root
global.conf.zep-db zenoss_zep
global.conf.zep-db-type mysql
global.conf.zep-host 127.0.0.1
global.conf.zep-password zenoss
global.conf.zep-port 3306
global.conf.zep-uri http://127.0.0.1:8084
```

11. Update the password of the `zenoss_system` user account.
    a. In the **Edit Variables** dialog, locate the `global.conf.zauth-password` variable.

       This variable sets the password of the Zope authentication server.
    b. Replace its value with the password specified previously for the `zenoss_system` user account.
    c. At the bottom of the **Edit Variables** dialog, click **Save Changes**.
12. In the application title line, click the **Restart** control.