PowerKEY CAS Gateway 4.1 Installation and Configuration Guide

Please Read

Important

Read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide

Purpose

This ***PowerKEY CAS Gateway 4.1 Installation and Configuration Guide*** provides an overview of the PowerKEY® Conditional Access System (CAS) and describes the PowerKEY CAS Gateway (PCG) server. The PCG is a DVB SimulCrypt-compliant Entitlement Control Message (ECM) generator (ECMG) that performs real-time PowerKEY ECM generation. Visit ***www.cisco.com*** (***http://www.cisco.com***) for data sheets and white papers describing the benefits and features of the PCG server and its role in the Cisco PowerKEY CAS.

Audience

This document is written for system operators. Field service engineers and Cisco Services engineers may also find the information in this document helpful.

Required Skills and Expertise

System operators or engineers who upgrade the PCG software need the following skills:

- Advanced knowledge of Linux.
  - Experience with the vi editor. Several times throughout the system upgrade process, system files are edited using the vi editor. The vi editor is not intuitive. The instructions provided in this guide are no substitute for an advanced working knowledge of vi.
  - The ability to review and edit cron files.
- Knowledge of VMware.
- Extensive EC, DTACS, PCG and DBDS system expertise.

Migration Paths

There is no supported upgrade path from PCG 4.0 or earlier to PCG 4.1 due to the new operating system on PCG 4.1. All sites running PCG 4.0 or earlier must build a new PCG virtual machine using the current PCG OVA (i.e. PCG-4.1.0-4.ova).

Supported EC and DTACS Versions

EC:

- SR 9.0
- SR 8.0

DTACS:

- SR 5.2
- SR 5.0

1

System Requirements

Before you deploy the PCG VM, make sure your system environment meets the hardware and software requirements defined in this chapter.

In This Chapter

Hardware Requirements

- Cisco UCS C220 M3 or C220 M4 servers with the latest ESXi software installed.

  Important: If you are using a new UCS C220 server, refer to ***Hardware Configuration Procedures for the Cisco UCS C220 Server*** (on page 35) for details about configuring the server. This must be completed prior to deploying the OVA.

- Supported PCG Server Platform:

Platform	Hard Drive (GB)	Memory (GB minimum)
Cisco UCS C220 M3	3 x 300	16
Cisco UCS C220 M4	3 x 300	64

- Cisco UCS hardware should have adequate CPU, memory and hard disk capacities:

CPU	Memory (GB)	Hard Disk (GB)	Network Interfaces
2	2	1 x 32 (root)	1 x Public

- **Network Mapping**:
  - NET0 — vSwitch0 — Controller Network
  - NET1 — vSwitch1 — Simulcrypt Synchronizer (SCS) Network

Software Requirements

The following software is required for the PCG 4.1 installation.

- Requires a vCenter Web UI login or a vSphere client to connect and perform management tasks.
  - A vCenter login must have admin privileges to deploy VMs.
- Reserve two static IP addresses:
  - One for the network interface to the client (EC/DTACS server).
  - One for the Simulcrypt Synchronizer (SCS).
- Obtain the associated domain name server, default gateway and network mask values from your system administrator.
- Download the following software from your customer-specific forum on Cisco's File Exchange Server and save it to a local directory that is accessible to the vSphere application.
  - PCG Linux VMware OVA (for example, PCG-4.1.0-4.ova)
  - PCG Application Package (for example, CSCOec-pcg-4.1.0-4.x86_64.rpm)

2

Install the Software on the EC/DTACS Server

This chapter provides the procedure to install or upgrade the PCG package to your EC/DTACS system.

Notes:

- Make sure the RPM version you plan to install matches the OVA version that will be deployed to build the PCG VM.
- If you did not yet download the PCG RPM package to your local system, refer to ***Software Requirements*** (on page 3) to do so now.

In This Chapter

Installing the PCG Package on the EC or DTACS Server

Complete the following steps to install the PCG package on an EC 9.0/8.0 or a DTACS 5.2/5.0 server.

1. Copy the **CSCOec-pcg** package (for example, CSCOec-pcg-4.1.0-4.x86_64.rpm) to the **/var/tmp/** directory on your EC/DTACS server.
2. As **admin** user, log into the EC/DTACS server.
3. Enter the following command to install the **CSCOec-pcg** package on the EC/DTACS server. An **Is this ok [y/d/N]** prompt appears.

   Command Syntax:

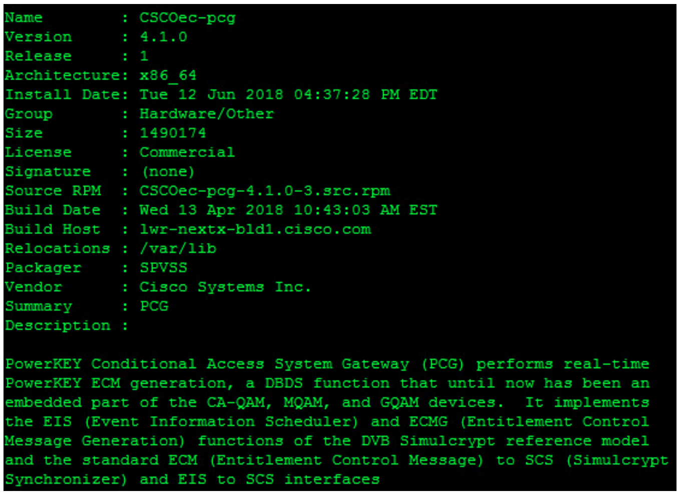
   ```
   sudo yum install CSCOec-pcg-[VERSION].x86_64.rpm
   ```

   Example:

   ```
   [admin@EC/DTACS ~]$ sudo yum install
   CSCOec-pcg-4.1.0-4.x86_64.rpm
   ```

4. When prompted to confirm the installation, type **y** and press **Enter**. The package is downloaded and installed and a **Complete** message is displayed.
5. Enter the following command to verify the PCG package installation.

   ```
   [admin@EC/DTACS ~]$ rpm -qi CSCOec-pcg
   ```



```
Name        : CSCOec-pcg
Version     : 4.1.0
Release     : 1
Architecture: x86_64
Install Date: Tue 12 Jun 2018 04:37:28 PM EDT
Group       : Hardware/Other
Size        : 1490174
License     : Commercial
Signature   : (none)
Source RPM  : CSCOec-pcg-4.1.0-3.src.rpm
Build Date  : Wed 13 Apr 2018 10:43:03 AM EST
Build Host  : lwr-nextx-bld1.cisco.com
Relocations : /var/lib
Packager    : SPVSS
Vendor      : Cisco Systems Inc.
Summary     : PCG
Description :

PowerKEY Conditional Access System Gateway (PCG) performs real-time
PowerKEY ECM generation, a DBDS function that until now has been an
embedded part of the CA-QAM, MQAM, and GQAM devices.  It implements
the EIS (Event Information Scheduler) and ECMG (Entitlement Control
Message Generation) functions of the DVB Simulcrypt reference model
and the standard ECM (Entitlement Control Message) to SCS (Simulcrypt
Synchronizer) and EIS to SCS interfaces
```

3

Deploy the PCG Virtual Machine

This chapter describes how to deploy the PCG virtual machine using the PCG Linux platform OVA that you downloaded to your local PC.

Note: If you did not yet downloaded the PCG OVA to your local system, refer to ***Software Requirements*** (on page 3) to do so now.

In This Chapter

Deploying the PCG Virtual Machine from the vSphere Web UI

Complete the following procedure to deploy the PCG VM using the PCG OVA (for example, PCG-4.1.0-4.ova).

Note: This procedure is written using vSphere vCenter Web Client 6.0.

1 Via a Web browser, login to the vCenter Web UI.

2 Go to the **Hosts and Clusters** view.

3 Right-click the ESXi host or cluster where you will deploy the PCG VM instance.

4 Select **Deploy OVF Template**. The Deploy OVF Template > Select source window opens.

5 Click **Local file** and then click **Browse**.

6 Navigate to the directory where you saved the **PCG** OVA file. Select the OVA and click **Open**. The absolute path of the PCG OVA is displayed next to the Browse button.

7 Click **Next**. The Review details window opens.

8 Review the OVF template details and click **Next**. The Accept License Agreements window opens.

9 Review the End User License Agreement and click **Accept**. Then click **Next**. The Select name and folder window appears.

10 In the **Name** text box, enter a name that describes the PCG VM.

11 From the **Select a folder or datacenter** area, select the datacenter where the VM is to be located and click **Next**. The Select storage window opens.

12 From the **Select virtual disk format** dropdown menu, select **Thick Provision Lazy Zeroed**.

13 Select the appropriate datastore to store the configuration files and all of the virtual disks for the VM.

14 Click **Next**. The Setup networks window displays.

15 Select the appropriate **Destination Network** for each Source network. Then click **Next**. The Ready to Complete window displays.

16 Review the details and click **Finish**.

17 Monitor the deployment of the VM from the **Recent Tasks** area to verify that the VM successfully deployed.

Reconfiguring the PCG Virtual Hardware

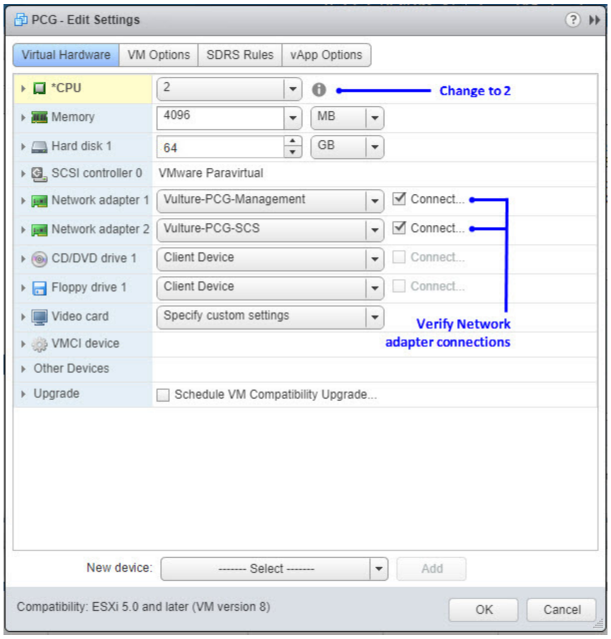
Complete the following procedure to reconfigure the virtual hardware for the PCG VM.

1 Right-click the VM and select **Edit Settings**. The Virtual Machine Properties window displays.

2 From the **CPU** dropdown menu, select **2**.

3 Verify that **Network adapter 1** is connected to the management/controller interface.

4 Verify that **Network adapter 2** is connected to the SCS interface for your network.



*CPU	2		
Memory	4096	MB	
Hard disk 1	64	GB	
SCSI controller 0	VMware Paravirtual		
Network adapter 1	Vulture-PCG-Management	☑ Connect...	
Network adapter 2	Vulture-PCG-SCS	☑ Connect...	
CD/DVD drive 1	Client Device	□ Connect...	
Floppy drive 1	Client Device	□ Connect...	
Video card	Specify custom settings		
VMCI device			
Other Devices			
Upgrade	□ Schedule VM Compatibility Upgrade...		

Change to 2

Verify Network adapter connections

Compatibility: ESXi 5.0 and later (VM version 8)

5 Click **OK** to reconfigure the VM.

6 Monitor the **Recent Tasks** area to confirm that the VM virtual hardware is successfully reconfigured.

Power On and Login to the New PCG Virtual Machine

Complete the following steps to power on and login to the new PCG VM.

1 Select and right-click the PCG VM and select **Power On**.

2 Right-click the VM again and select **Open Console**.

3 Log into the VMware console with the following credentials:

   User Name: admin

   Password: password

   Important: The admin user has full root privileges via the sudo command. Direct root access is not permitted.

4 Press **Enter**. You are prompted to change the password. Please change it to something appropriate for your environment.

5 At the **(current) UNIX password** prompt, re-enter the default password which is **password**.

6 At the **New password** prompt, enter a new password.

7 At the **Retype new password** prompt, re-enter the new password. The admin prompt displays.

8 Enter the following command to verify that the PCG package is installed.

```
[admin@pcg ~]$ rpm -qa | grep -i pcg
```

   Example Output:

```
CSCOec-pcg-4.1.0-4.x86_64
```

9 Go to the next section.

Configuring the PCG Network

Complete the following steps to manually configure the PCG network.

Note: You should be logged into the PCG VM from a Console window.

1 Enter the following command to define a hostname for the PCG server.

Note: Substitute the hostname you want to define for [pcghostname]. Do not include the brackets.

Command Syntax:

```
sudo hostnamectl set-hostname [pcghostname]
```

Example:

```
[admin@pcg ~]$ sudo hostnamectl set-hostname pcgtest
```

2 Enter the following command to reboot the system.

```
[admin@pcg ~]$ sudo reboot now
```

3 Log back into the system as **admin** user. The prompt should now include the hostname you defined in Step 1.

4 Enter the following command to configure the management (**ens192**) network interface.

```
[admin@pcgtest ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

5 Change the **BOOTPROTO** value to **none**.

BOOTPROTO=none

6 Go to the end of the file and add the following lines.

Syntax:

Note: Substitute the appropriate values for terms shown in brackets.

```
IPADDR=[IP_address_PCG_Management_interface]
PREFIX=[[Subnet_PCG_Management_interface]
GATEWAY=[Gateway_PCG_Management_interface]
DEFROUTE=yes
NM_CONTROLLED=no
```

Example:

```
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=none
DEVICE=ens192
HWADDR=00:50:56:b8:15:79
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
IPADDR=204.1.61.100
PREFIX=29
GATEWAY=204.1.61.102
DEFROUTE=yes
NM_CONTROLLED=no
```

7 Save and close the file.

8 Type the following command to determine the MAC address defined for the **ens224** interface.

```
[admin@pcgtest network-scripts]$ ifconfig ens224
```

9 Record the MAC address from the output of Step 9. It will be included in the ifcfg-ens224 configuration file.

MAC address for ens224: ____________________________

10 Type the following command to create the **ifcfg-ens224** network interface file.

```
[admin@pcg network-scripts]$ sudo cp ifcfg-ens192 ifcfg-ens224
```

11 Open the **ifcfg-ens224** file in a text editor.

```
[admin@pcgtest network-scripts]$ sudo vi ifcfg-ens224
```

12 Delete the **GATEWAY** entry.

13 Update the following entries:

Note: Substitute the appropriate values for fields shown in brackets.

```
DEVICE=ens224
HWADDR=[MAC_address_from_Step_10]
IPADDR=[IP_address_SCS/PKE_interface]
DEFROUTE=no
```

Example:

```
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=none
DEVICE=ens224
HWADDR=00:50:56:b8:57:ca
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
IPADDR=140.1.61.100
PREFIX=29
NM_CONTROLLED=no
```

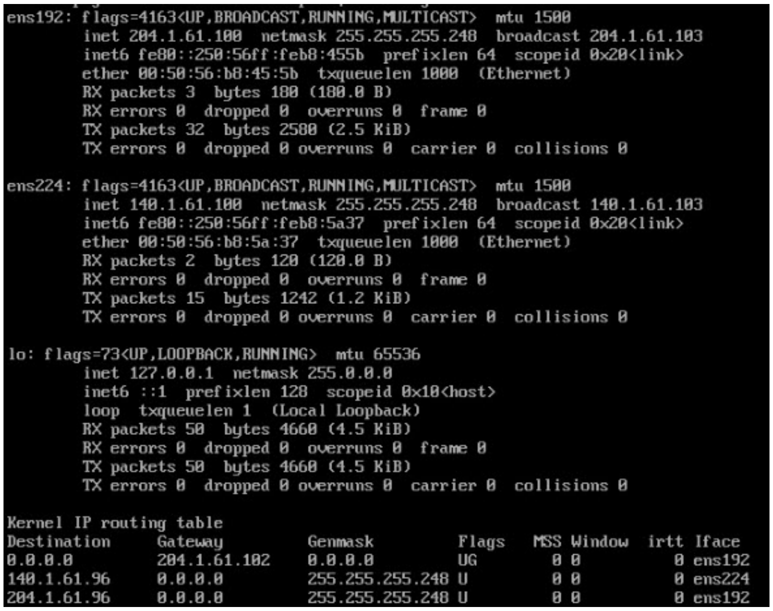
14 Save and close the file.

15 Enter the following command to restart the network service.

```
[admin@pcgtest network-scripts]$ sudo systemctl restart
network
```

16 Enter the following commands, on one line, to verify that the network interfaces and the routing are set up correctly.

```
[admin@pcgtest network-scripts]$ ifconfig -a ; netstat -nrv
```



```
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 204.1.61.100  netmask 255.255.255.248  broadcast 204.1.61.103
        inet6 fe80::250:56ff:feb8:455b  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b8:45:5b  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 180 (180.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 2580 (2.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 140.1.61.100  netmask 255.255.255.248  broadcast 140.1.61.103
        inet6 fe80::250:56ff:feb8:5a37  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b8:5a:37  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 120 (120.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 1242 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 50  bytes 4660 (4.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50  bytes 4660 (4.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         204.1.61.102    0.0.0.0         UG        0 0          0 ens192
140.1.61.96     0.0.0.0         255.255.255.248 U         0 0          0 ens224
204.1.61.96     0.0.0.0         255.255.255.248 U         0 0          0 ens192
```

17 Is the network set up correctly?

- If **no**, review the configuration files you set up or contact Cisco Services.
- If **yes**, close the Console window and go to the next step.

18 From a terminal window, log into the EC/DTACS associated with the PCG server as **admin** user.

19 From the EC/DTACS, SSH into the PCG server as **admin** user.

Command Syntax:

```
ssh admin@[IP address of PCG server]
```

Example:

```
[admin@ec/dtacs ~]$ ssh admin@204.1.61.100
```

20 Enter the following command to display the mapping of the network interfaces to MAC addresses.

Important: The MAC addresses shown in this output are examples. The output for your system will be different.

```
[admin@pcgtest ~]$ ip -o link show | awk '{print $2, $15}'
```

Example Output:

```
lo: 00:00:00:00:00:00
ens192: 00:50:56:b8:45:5b
ens224: 00:50:56:b8:5a:37
```

21 Record the **ens192** MAC address from your output as it is required to configure the PCG via the EC/DTACS Web interface in a later procedure.

ens192: ______________________

Updating the Time Zone

If desired, complete the following steps to query and change the system clock and its settings.

Note: You should be logged into the PCG server as admin user via SSH from the EC/DTACS.

1 Enter the following command to view the default date and timezone.

   Note: The default timezone is UTC (Coordinated Universal Time).

   ```
   [admin@pcgtest ~]$ timedatectl
   ```

   Example Output:

   ```
         Local time: Thu 2018-09-20 20:52:47 UTC
     Universal time: Thu 2018-09-20 20:52:47 UTC
           RTC time: Thu 2018-09-20 20:52:47
          Time zone: UTC (UTC, +0000)
        NTP enabled: yes
   NTP synchronized: yes
    RTC in local TZ: no
         DST active: n/a
   ```

2 Do you want to update the timezone?

   - If **yes**, go to Step 3.
   - If **no**, you have completed this procedure.

3 Enter the following command to determine that proper syntax for your timezone.

   ```
   [admin@pcgtest ~]$ timedatectl list-timezones
   ```

4 Scan through the list to find the entry for your timezone (for example, America/New_York).

5 Press **Ctrl+C** to exit the output list.

6 Enter the following command to set the timezone.

   Command Syntax:

   ```
   sudo timedatectl set-timezone [timezone_syntax]
   ```

   Example: using timezone=America/New_York

   ```
   [admin@pcgtest ~]$ sudo timedatectl set-timezone
   America/New_York
   ```

7 Repeat Step 1 to confirm the new timezone.

Example:

```
       Local time:  Thu 2018-09-20 16:53:07 EDT
  Universal time: Thu 2018-09-20 20:53:07 UTC
        RTC time: Thu 2018-09-20 20:53:07
       Time zone: America/New_York (EDT, -0400)
     NTP enabled: yes
NTP synchronized: yes
 RTC in local TZ: no
      DST active: yes
 Last DST change: DST began at
                  Sun 2018-03-11 01:59:59 EST
 Next DST change: DST ends (the clock jumps one hour backwards) at
                  Sun 2018-11-04 01:59:59 EDT
                  Sun 2018-11-04 01:00:00 EST
```

Installing VMware Tools (Optional)

The installation of VMware Tools is optional. If you wish to install VMware Tools on the PCG machine, follow the instructions provided by VMware.

- ***Installing and Configuring VMware Tools*** (***https://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf***)
- ***VMware KB 1018414*** (***http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1018414***)

Abbreviated Procedure

Complete the following steps to install VMware Tools.

1 Click the link in vCenter to make the VMware Tools CD available to the PCG VM.

2 As **admin** user, enter the following command to change to **root** user.

```
[admin@pcgtest ~]$ sudo -i
```

3 Enter the following command to mount the virtual cdrom.

```
[root@pcgtest ~]# mount -o ro /dev/cdrom /mnt
```

4 Enter the following command to change to the **/root** directory.

```
[root@pcgtest ~]# cd /root
```

5 Enter the following command to extract the VMware Tools tar file.

```
[root@pcgtest ~] ~# tar xzpf /mnt/VMwareTools-*.tar.gz
```

6 Enter the following command to install the VMware Tools using the default options.

```
[root@pcgtest ~]# ./vmware-tools-distrib/vmware-install.pl -d
```

4

Provision the PCG on the EC/DTACS Web UI

This chapter includes the procedures to provision the PCG VM on the EC/DTACS Web UI. Once the PCG is configured in the Web UI, the PCG is reset. During the reset, the EC/DTACS server responds by provisioning the PCG according to the new settings.

Note: Ethernet settings can be used to communicate with the SCS, which can provision the PCG with scrambler or SCS device IP addresses and parameters (for example, maximum number of scrambling control groups (SCGs)).

In This Chapter

Provisioning the PCG on the EC Web UI

Complete the following procedure to provision the PCG on the EC Web UI.

1 As **dncs** user on the EC, type the following command to monitor the bootp log.

Note: You will actually monitor this log after provisioning the PCG on the EC Web UI later in this procedure.

```
[dncs@ecnextx root]$ qtail bootp
```

2 Enter the appropriate values in the following table as they are required to provision the PCG on the EC.

Notes:

- The Control IP address, subnet mask and default gateway fields represent the ens192 interface.
- The SCS IP address and subnet mask fields represent the ens224 interface.
- The PCG ens192 MAC address was recorded in ***Configuring the PCG Network*** (on page 11).

Parameter	Value
Control IP Address	
Control Subnet Mask	
Control Default Gateway	
SCS IP Address	
SCS Subnet Mask	
Control MAC Address (ens192)	

3 From a supported web browser, login into the EC Web UI as an administrative user (for example, ecadmin).

4 Click the **Navigation** button (☰) and then select **Network Element Provisioning > PCG**. The Powerkey CAS Gateway List Web UI displays.

Important: The PCG feature must be enabled as a licensed feature. If PCG is not yet enabled, contact Cisco Services.

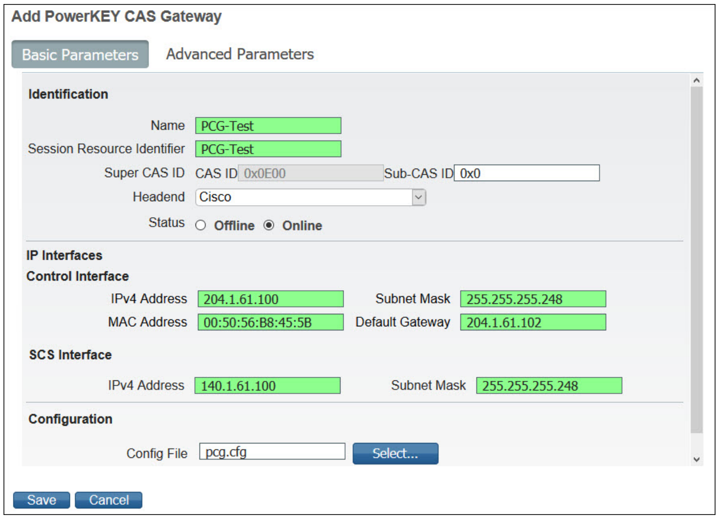
5 Click **Add**. The Add PowerKEY CAS Gateway window displays and the Basic Parameters display by default.

6 Update the fields for your PCG system.

Note: Some of the values are documented in Step 2.

Field	Description
Name	A unique name for the PCG
Session Resource Identifier	A unique identifier for the PCG. **Note**: This can be the same as the entry in the Name field.
Sub-CAS ID	Default is 0x0
Headend	Select the appropriate headend
Status	Set the status to Offline or **Online**
Control Interface IPv4 Address	The IP address of the Control interface (ens192) on the PCG
Control Interface Subnet Mask	The subnet mask of the Control interface (ens192) on the PCG
Control Interface MAC Address	The MAC address of the Control interface (ens192) on the PCG
Control Interface Default Gateway	The default gateway of the Control interface (ens192) on the PCG
SCS Interface IPv4 Address	The IP address of the SCS interface (ens224) on the PCG
SCS Interface Subnet Mask	The subnet mask of the SCS interface (ens224) on the PCG
Config File	The name of the PCG application configuration file. This file is installed, when the PCG application is installed on the EC. The default is pcg.cfg

Example:



Add PowerKEY CAS Gateway

Basic Parameters | Advanced Parameters

Identification

Name: PCG-Test

Session Resource Identifier: PCG-Test

Super CAS ID: CAS ID 0x0E00 Sub-CAS ID 0x0

Headend: Cisco

Status: ○ Offline ● Online

IP Interfaces

Control Interface

IPv4 Address: 204.1.61.100 Subnet Mask: 255.255.255.248

MAC Address: 00:50:56:B8:45:5B Default Gateway: 204.1.61.102

SCS Interface

IPv4 Address: 140.1.61.100 Subnet Mask: 255.255.255.248

Configuration

Config File: pcg.cfg Select...

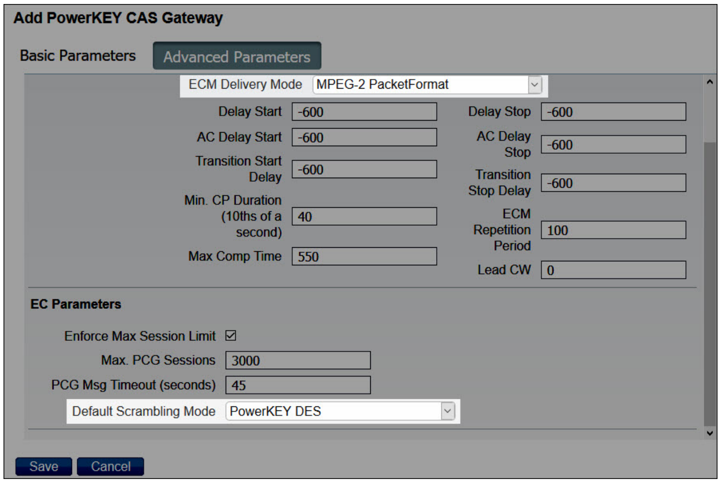
Save Cancel

7 Click the **Advanced Parameters** tab. The Advanced Parameters window displays.

8 Define the following values for the fields shown below.

Field	Description
ECM Delivery Mode	Select MPEG2 PacketFormat
Default Scrambling Mode	Select PowerKEY DES

Example:



Add PowerKEY CAS Gateway

Basic Parameters | Advanced Parameters

ECM Delivery Mode: MPEG-2 PacketFormat

Delay Start: -600 Delay Stop: -600

AC Delay Start: -600 AC Delay Stop: -600

Transition Start Delay: -600 Transition Stop Delay: -600

Min. CP Duration (10ths of a second): 40 ECM Repetition Period: 100

Max Comp Time: 550 Lead CW: 0

EC Parameters

Enforce Max Session Limit: ☑

Max. PCG Sessions: 3000

PCG Msg Timeout (seconds): 45

Default Scrambling Mode: PowerKEY DES

Save Cancel

9 Click **Save**. You are returned to the PowerKEY CAS Gateway List window. The PCG is displayed in the list.

10 In the terminal window where you are monitoring bootp (Step 1), observe the output to verify that the PCG is successfully provisioned.

11 When you have verified the bootp for the PCG device, enter **Ctrl+C** to exit the qtail session.

Note: If boot issues are present, refer to ***Troubleshooting Boot Issues*** (on page 62).

Provisioning the PCG on the DTACS Web UI

Complete the following procedure to provision the PCG on the DTACS Web UI.

1 As **dncs** user on the DTACS, type the following command to monitor the bootp log.

Note: You will actually monitor this log after provisioning the PCG on the DTACS Web UI later in this procedure.

```
[dncs@dtacs root]$ qtail bootp
```

2 Enter the appropriate values in the following table as they are required to provision the PCG on the DTACS.

Important:

- The Control IP address, subnet mask and default gateway fields represent the ens192 interface.
- The SCS IP address and subnet mask fields represent the ens224 interface.
- The PCG ens192 MAC address was recorded in ***Configuring the PCG Network*** (on page 11).

Parameter	Value
Control IP Address	
Control Subnet Mask	
Control Default Gateway	
SCS IP Address	
SCS Subnet Mask	
Control MAC Address (ens192)	

3 Login to the DTACS Web UI as an administrative user (for example, dtacsadmin).

4 Click the **Navigation** button, ☰, and then select **Network Elements > PCG**.

Important: The PCG feature must be enabled as a licensed feature. If PCG is not yet enabled, contact Cisco Services.

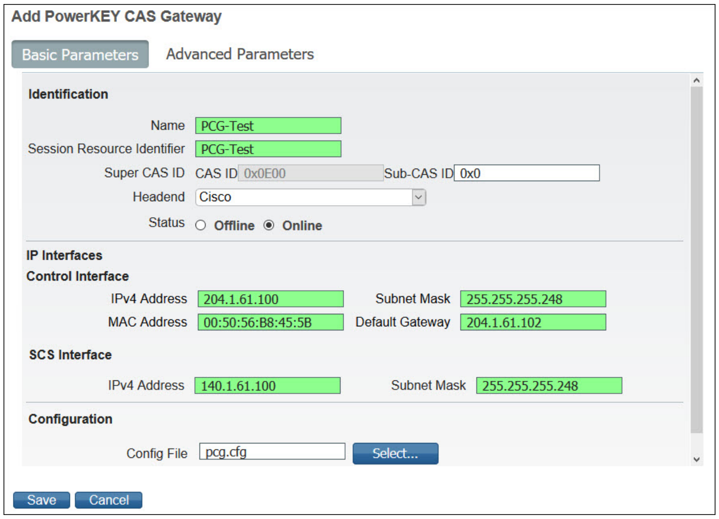
5 Click **Add**. The SCC CAS Gateway List window display and the Basic Parameters display by default.

6 Update the fields for your PCG system.

Note: Some of the values were recorded in Step 2.

Field	Description
Name	A unique name for the PCG
Session Resource Identifier	A unique identifier for the PCG. **Note**: This can be the same as the entry in the Name field.
Sub-CAS ID	Default is 0x0
Headend	Select the appropriate headend
Status	Set the status to Offline or **Online**
Control Interface IPv4 Address	The IP address of the Control interface on the PCG (ens192)
Control Interface Subnet Mask	The subnet mask of the Control interface on the PCG
Control Interface MAC Address	The MAC address of the Control interface (ens192) on the PCG
Control Interface Default Gateway	The default gateway of the Control interface on the PCG (ens192)
SCS Interface IPv4 Address	The IP address of the SCS interface (ens224) on the PCG
SCS Interface Subnet Mask	The subnet mask of the SCS interface (ens224) on the PCG
Config File	The name of the PCG application configuration file. This file is installed, when the PCG application is installed on the DTACS. The default is pcg.cfg

Example:



Add PowerKEY CAS Gateway

Basic Parameters | Advanced Parameters

Identification

Name: PCG-Test

Session Resource Identifier: PCG-Test

Super CAS ID: CAS ID 0x0E00 Sub-CAS ID 0x0

Headend: Cisco

Status: ○ Offline ● Online

IP Interfaces

Control Interface

IPv4 Address: 204.1.61.100 Subnet Mask: 255.255.255.248

MAC Address: 00:50:56:B8:45:5B Default Gateway: 204.1.61.102

SCS Interface

IPv4 Address: 140.1.61.100 Subnet Mask: 255.255.255.248

Configuration

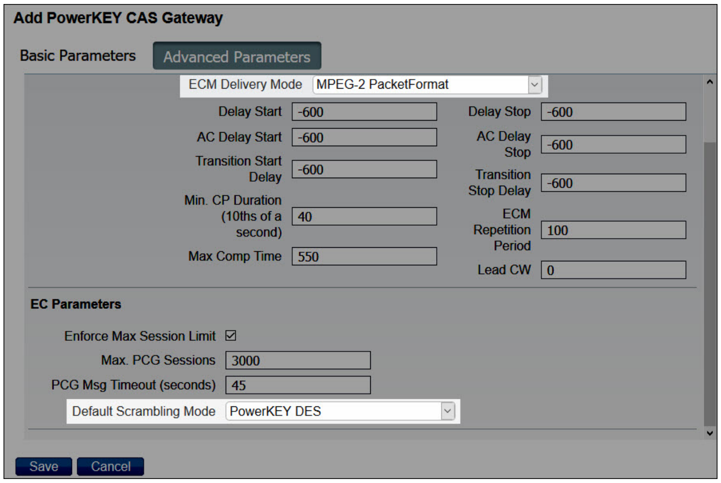
Config File: pcg.cfg

7 Click the **Advanced Parameters** tab. The Advanced Parameters window displays.

8 Define the following values for the fields shown below.

Field	Description
ECM Delivery Mode	Select MPEG2 PacketFormat
Default Scrambling Mode	Select PowerKEY DES

Example:



Add PowerKEY CAS Gateway

Basic Parameters | Advanced Parameters

ECM Delivery Mode: MPEG-2 PacketFormat

Delay Start: -600 Delay Stop: -600

AC Delay Start: -600 AC Delay Stop: -600

Transition Start Delay: -600 Transition Stop Delay: -600

Min. CP Duration (10ths of a second): 40 ECM Repetition Period: 100

Max Comp Time: 550 Lead CW: 0

EC Parameters

Enforce Max Session Limit ☑

Max. PCG Sessions: 3000

PCG Msg Timeout (seconds): 45

Default Scrambling Mode: PowerKEY DES

9 Click **Save**. You are returned to the SCC CAS Gateway List window. The PCG you provisioned and saved appears in the list.

10 In the terminal window where you are monitoring bootp (Step 1), observe the output to verify that the PCG is successfully provisioned.

11 When you have verified the bootp for the PCG device, enter **Ctrl+C** to exit the qtail session.

Note: If boot issues are present, refer to ***Troubleshooting Boot Issues*** (on page 62).

5

Verify PCG Versions

This chapter describes the procedures to verify the PCG version from the EC and the DTACS servers, as well as from the PCG server.

In This Chapter

Verifying PCG Package Versions on the EC/DTACS

Important: The EC/DTACS dictates what PCG version should be loaded on the PCG servers.

Complete the following steps to verify the PCG version installed on the EC/DTACS server.

1. From the EC/DTACS terminal window, enter the following command to verify the version of the PCG package currently installed.

   EC/DTACS:

   ```
   [admin@ec/dtacs ~]$ rpm -qa | grep -i pcg
   ```

   Example Output:

   ```
   CSCOec-pcg-4.1.0-4.x86_64
   ```

2. To determine the PCG version on the PCG server, go to the next section.

Verifying the PCG Version on the PCG Server

Important: Do ***NOT*** use the rpm command to verify the version of the PCG package as the output of the rpm command only reflects the PCG version loaded during initial installation. Therefore, it may not match the actual version of the PCG code that is running.

Complete the following steps to determine the current version of the PCG application installed on the PCG server.

1. From the EC/DTACS, SSH into the PCG server as **admin** user.
2. Enter the following command to access the PCG console application.

   ```
   [admin@pcgtest ~]$ sudo /opt/pcg/console_app/cons
   ```

3. At the **PCG>** prompt, enter the following command to verify the version of the PCG package currently installed.

   ```
   vers
   ```

   Example Output:

   ```
   PCG> PCG version: 4.1.0-4. Build date : 27 August 2018
   ```

   Result: The PCG version on the EC/DTACS and the PCG server should match.
4. Press **Enter** to return to the PCG console application prompt.
5. Type **exit** to return to the PCG prompt.
6. Did the output from Step 2 match the PCG version on the EC/DTACS server?
   - If **yes**, you have completed this procedure.
   - If **no**, go to ***Upgrade the PCG Server*** (on page 49).

6

Configure SNMPv2

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks.

This chapter describe how to configure SNMPv2 and SNMPv3 for the PCG device.

In This Chapter

Configuring SNMPv2

Complete the following procedure to configure SNMPv2 on the PCG.

1 If you are not logged into the PCG, ssh into the PCG server as **admin** user.

2 Enter the following command to edit the **/etc/snmp/snmpd.conf** file.

```
[admin@pcgtest ~]$ sudo vi /etc/snmp/snmpd.conf
```

3 Move to the end of the file and add the following three lines.

Notes:

- Replace [PCG ens192 IP] with the IP address of the ens192 network interface.
- Replace [community_name] with the desired SNMP community name.
- Replace [destination_host]:[port] with the IP address and port of the SNMP trap listener.

Line Syntax:

```
agentaddress [PCG ens192 IP]:161
rocommunity [community_name]
trapsess -v2c -c [community_name][destination_host]:[port]
```

Example:

```
agentaddress 204.1.61.100:161
rocommunity public
trapsess -v2c -c public 204.123.1.33:162
```

4 Save and close the file.

5 Enter the following command to stop the SNMP service.

```
[admin@pcgtest ~]$ sudo systemctl stop snmpd
```

6 Enter the following command to start the SNMP service.

```
[admin@pcgtest ~]$ sudo systemctl start snmpd
```

7 Enter the following command to verify that the SNMP service is running.

```
[admin@pcgtest ~]$ sudo systemctl status snmpd
```

Configuring SNMPv3

Creating the SNMPv3 User

Complete the following steps to create a SNMPv3 user.

Note: Refer to the SNMP RFCs for SNMPv3 username and passphrase constraints.

1 Enter the following command to stop the SNMP service.

```
[admin@pcgtest ~]$ sudo systemctl stop snmpd
```

2 Enter the following command to create the SNMPv3 user.

```
[admin@pcgtest ~]$ sudo /usr/bin/net-snmp-create-v3-user
```

3 When prompted for SNMPv3 user name, enter a user name and press **Enter**.

4 When prompted for an authentication password, enter a password and press **Enter**.

Important: The authentication password must be at least 8 characters and can include alphabetic, numeric, and special characters, but it cannot include control characters.

5 When prompted for an encryption pass-phrase, either type a password and press **Enter** or press **Enter** to use the same password as the authentication password.

Important: If you define a unique password it must be at least 8 characters and can include alphabetic, numeric, and special characters. It cannot include control characters.

Result: The /var/lib/net-snmp/snmpd.conf is updated and the SNMPv3 user is created.

Changing the SNMPv3 User Options

1 Open the **/etc/snmp/snmpd.conf** file and go to the end of the file to the rwuser line.

Note: The SNMPv3 user name you created will be at the end of the rwuser line.

```
[admin@pcgtest ~]$ sudo vi /etc/snmp/snmpd.conf
```

2 Go to the end of the line and add **authPriv** after the new username entry.

rwuser Entry Syntax:

```
rwuser [snmp_username]
```

Example:

```
rwuser snmpuser authPriv
```

3 Next, change rwuser to **rouser**. This allows read-only SNMP operations.

rwuser Entry Syntax:

```
rwuser [snmp_username] authPriv
```

Example:

```
rouser snmpuser authPriv
```

4 Save and close the **snmpd.conf** file.

5 Enter the following command to verify the authPriv entry.

```
[admin@pcgtest ~]$ sudo less /etc/snmp/snmpd.conf | grep -i
priv
```

Example Output:

```
rouser snmpuser authPriv
```

Restart the SNMP Service

1 Enter the following command to start the SNMP service.

```
[admin@pcggtest ~]$ sudo systemctl start snmpd
```

2 Enter the following command to verify that the SNMP service is running.

```
[admin@pcgtest ~]$ sudo systemctl status snmpd
```

Defining the SNMPv3 Trap Destination

Complete the following steps to define the SNMPv3 trap destination.

1 Enter the following command to stop the SNMP service.

```
[admin@pcgtest ~]$ sudo systemctl stop snmpd
```

2 Add the following line to the **/etc/snmpd/snmpd.conf** file.

Notes:

- Replace <username> with the SNMPv3 username.
- Replace <trapDestIP> with the IP address of the SNMP trap receiver.
- Replace <trapDestPort> with the port number of the SNMP trap receiver (typically 162). The -l option can be set to noAuthNoPriv, authNoPriv, or authPriv but is recommended to be authPriv.
- Replace <authProt> with the authentication protocol defined for the SNMPv3 user: MD5 or SHA.
- Replace <privProt> with the encryption (privacy) protocol defined for the SNMPv3 user: DES or AES.

Line Syntax:

```
trapsess -v3 -u [username] -l authPriv -a [authProt] -x
[privProt] [trapDestIP]:[trapDestPort]
```

Example:

```
[admin@pcgtest ~]$ sudo trapsess -v3 -u snmp -l authPriv -a
SHA -x DES 204.123.1.33:162
```

3 Enter the following command to start the SNMP service.

```
[admin@pcgtest ~]$ sudo systemctl start snmpd
```

A

Hardware Configuration Procedures for the Cisco UCS C220 Server

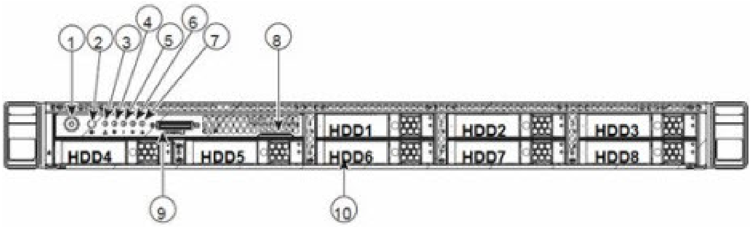
This appendix describes the server hardware and explains how to configure it for initial use with the PCG system.

In This Appendix

Cisco UCS C220 Server Diagram

Chassis Front View

The following diagram displays the chassis front view of the Cisco UCS C220 Server.

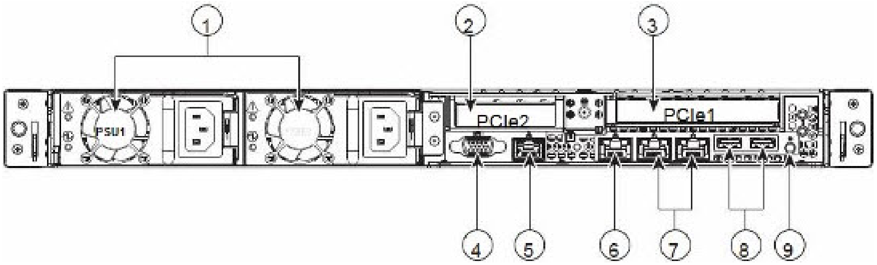


Field	Description
1	Power button or power status LED
2	Identification button or LED
3	System status LED
4	Fan status LED
5	Temperature status LED
6	Power supply status LED
7	Network link activity LED
8	Pull-out asset tag
9	KVM connector (used with KVM cable that provides two USBs, one VGA, and one serial connector)
10	Drives hot-swappable (up to eight 2.5-inch drives)

Chassis Rear View

The following diagram displays the chassis rear view of the Cisco UCS C220 server.

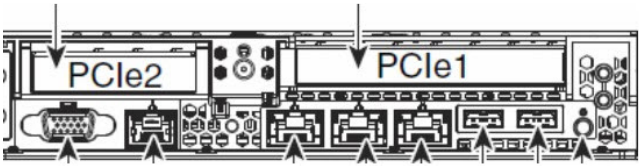
Note: Only the essential features of the rear panel are shown in this image. Also, be certain that the network cards are installed in the slots as shown in this diagram.



Field	Description
1	Power supplies
2	Low-profile PCIe slot 2 on riser (half-height, half-length, x8 lane)
3	Standard-profile PCIe slot on riser (full-height, half-length, x16 lane)
4	VGA video connector
5	Serial port (RJ-45 connector)
6	1-Gb Ethernet dedicated management port
7	Dual 1-Gb Ethernet ports (LAN1 and LAN2)
8	USB ports
9	Rear identification button or LED

Detailed View of PCI Ports

The following diagram shows the detailed view of the PCI Ports.



Note: For the PCIe1 card, the top row contains ports 2, 3, 4, and 5, the bottom row contains ports 0 and 1.

Cisco UCS C220 Server CIMC Configuration

Notes:

- The CIMC firmware and BIOS version should be at or higher than the minimum required version shown in ***Tested Reference Configuration*** section located in the ***Preface*** (on page v). If it does not meet these requirements, contact Cisco Services for assistance in upgrading the firmware and the BIOS.
- You have to perform this procedure only once, that is, when you initially install the UCS C220.
- Be sure that you use configuration data that pertains to the system that you are migrating.

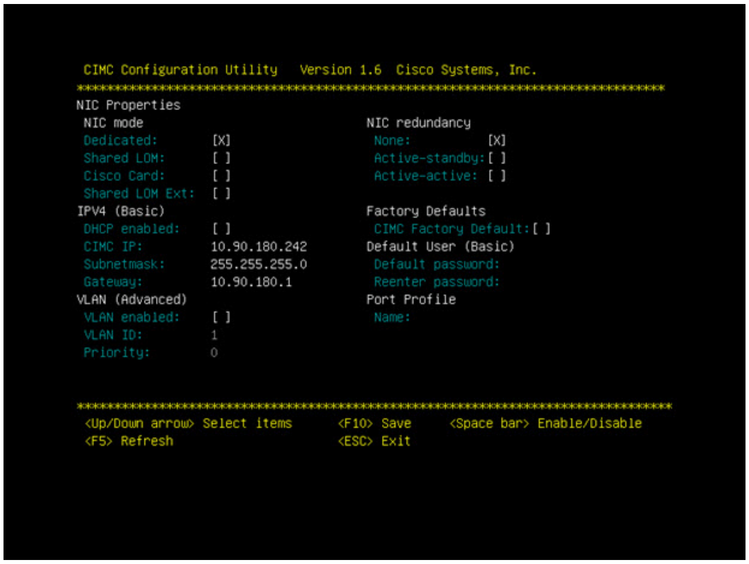
Complete the following steps to configure the Cisco UCS C220 server.

1. Follow the instructions in the ***UCS C220 Server Installation and Service Guide***. This guide is shipped with the server.
2. Press the **Power** button to power on the UCS C220 server.
3. Press **F8** at the Cisco splash screen. The server boots to the CIMC Configuration Utility window.

   Important: Note the BIOS version on the Cisco splash screen as the system is booting.
4. Use the information in the CIMC Configuration Utility window to complete the configuration.

   Note: In addition to the information in the CIMC Configuration Utility window, be sure to obtain the network IP address for the CIMC interface.

   Important: The following image is an example only. Do not use the IP address, netmask, or gateway in the image.



```
 CIMC Configuration Utility   Version 1.6  Cisco Systems, Inc.
*******************************************************************************
NIC Properties
 NIC mode                             NIC redundancy
 Dedicated:       [X]                  None:          [X]
 Shared LOM:      [ ]                  Active-standby:[ ]
 Cisco Card:      [ ]                  Active-active: [ ]
 Shared LOM Ext:  [ ]
IPV4 (Basic)                          Factory Defaults
 DHCP enabled:    [ ]                  CIMC Factory Default:[ ]
 CIMC IP:         10.90.180.242       Default User (Basic)
 Subnetmask:      255.255.255.0        Default password:
 Gateway:         10.90.180.1          Reenter password:
VLAN (Advanced)                       Port Profile
 VLAN enabled:    [ ]                  Name:
 VLAN ID:         1
 Priority:        0


********************************************************************************
 <Up/Down arrow> Select items      <F10> Save     <Space bar> Enable/Disable
 <F5> Refresh                      <ESC> Exit
```

5 Enter a default password and re-enter it at the prompt.

Note: Store this password in a safe place for future use.

6 Press **F10** to save changes.

7 Press **Esc** to exit. The EFI shell prompt may appear.

RAID Configuration

Important: This procedure only needs to be performed once — when you initially install the UCS C220 server.

Go to the appropriate section to configure RAID on your UCS hardware.

- *Configuring RAID for UCS C220 M3 Servers* (on page 40)
- *Configuring RAID for UCS C220 M4 Servers* (on page 42)

Configuring RAID for UCS C220 M3 Servers

The UCS hardware RAID configuration for this system release consists of a RAID 1 for the OS disk and one global hot spare (3x300GB).

Complete the following steps to create these volumes and hot spares.

1. Press **Ctrl-Alt-Del** to reboot the server.
2. Monitor the reboot process closely. After the disks are displayed, observe the boot messages and press **Ctrl-H** when prompted to access the WebBIOS (RAID Configuration Utility). After a few minutes, a **Start** button appears.
3. Click **Start** to configure RAID. The MegaRAID BIOS Config Utility main menu appears.
4. Click the **Configuration Wizard** link in the left area of the utility menu.
5. Click **New Configuration** and then click **Next**. The utility prompts you to clear the existing configuration.
6. Click **Yes**.
7. Click **Manual Configuration** and then click **Next**. The Drive Group Definition screen appears.

   Note: In the drives panel, there is a list of all three hard drives. Create two drive groups, the first consisting of two disks (1 and 2) and the second consisting of one global hot spare drive.
8. Select the **Slot 0** disk and while pressing the **Ctrl** key, click the **Slot 1** disk to highlight both disks.
9. Click **Add to Array** to form Drive Group (0).
10. Click **Accept DG**.
11. Click **Next** and select **Drive Group 0**.
12. Click **Add to SPAN to Drive Group 0** to the span list.
13. Click **Next**. The Virtual Drive Definition window appears.
14. Select **RAID 1** from the **RAID Level** dropdown menu.

15 Click **Update Size**. The maximum allowed size for the selected RAID level populates the Select Size field and records the size.

16 Click **Accept**. The **Write Policy** window appears.

17 Click **Yes** to confirm the default write policy.

18 Click **Back** and then select **Drive Group 0**.

19 Click **Add to SPAN to Drive Group 1** to the span list.

20 Click **Next**. The Virtual Drive Definition window appears.

21 Select **RAID 1** from the RAID Level drop-down menu.

22 Click **Update Size**. The maximum allowed size for the selected RAID level populates the Select Size field and records the size.

23 Click **Accept**. The Write Policy window appears.

24 Click **Yes** to confirm the default write policy. The total list of Vdisks created from Drive Groups 0 to 1 appears.

25 Click **Next**.

26 Examine the configuration preview to verify that the virtual drives match the previous list and select **Accept**. The system prompts to confirm that you want to save the configuration.

27 Click **Yes**. A warning message appears and indicates that you may lose data.

Note: If you cancel the previous screen, you will be prompted to initialize the new virtual drives.

28 Click **Yes** to initialize. The Virtual Drive VD0 is displayed.

29 Click **Home**. The Raid Configuration utility main menu appears.

30 Click the **Physical View** from the left pane if it is not currently displayed.

31 Click **Back** and then repeat Steps 21 through 22 for the drive in Slot 16.

32 Click **Home** and select the **Physical View** (if it is not displayed by default).

33 From the Main Menu, click **Exit** to exit the RAID Configuration Utility.

34 Click **Yes** to confirm that you want to exit the utility.

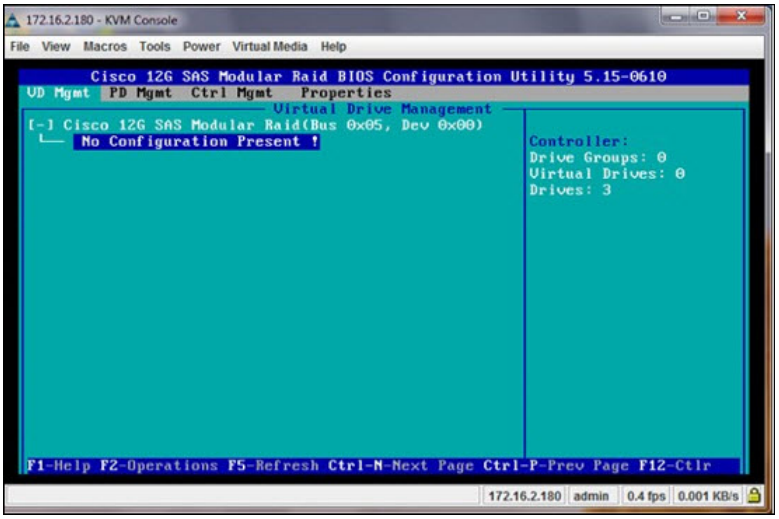
Configuring RAID for UCS C220 M4 Servers

Complete the following steps to configure RAID for a C220 M4 UCS server.

1 Power on the Cisco UCS C220 M4 server.

Note: If the server is already powered on, reboot the server.

2 On boot up, press **CTRL+R** to enter the Cisco 12G SAS Modular Raid Controller BIOS Configuration Utility.



172.16.2.180 - KVM Console
File View Macros Tools Power Virtual Media Help

```
        Cisco 12G SAS Modular Raid BIOS Configuration Utility 5.15-0610
 VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                    Virtual Drive Management
[-] Cisco 12G SAS Modular Raid(Bus 0x05, Dev 0x00)
  └── No Configuration Present !                   Controller:
                                                  Drive Groups: 0
                                                  Virtual Drives: 0
                                                  Drives: 3

F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

172.16.2.180
admin
0.4 fps
0.001 KB/s

3 Press **CTRL+N** and then click the **PD Mgmt** tab.

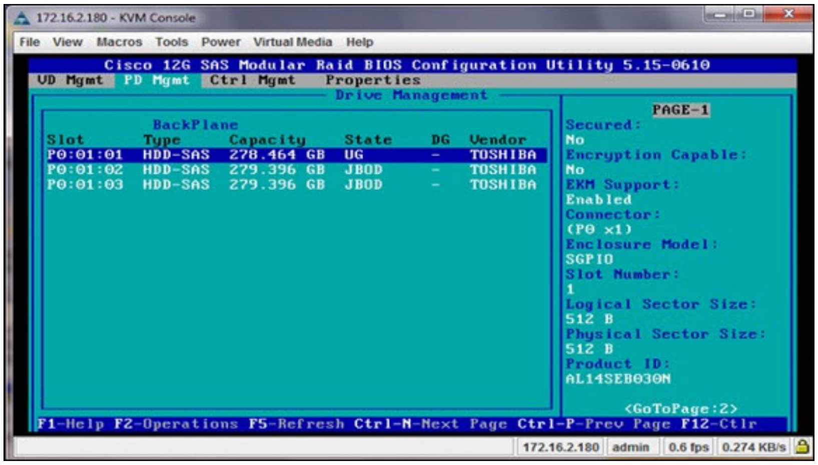
4 Use the **UP** or **DOWN** arrow keys to move between the disks.

5 Complete the following steps to change the disks from Just a Bunch Of Disks (JBOD) to **Unconfigured Good (UG)**.

a Select the first disk and press **F2**.

b Select **Make unconfigured good**.

c When prompted to confirm the change, click **Yes** and press **Enter**. The state of the drive will change from JBOD to UG.



172.16.2.180 - KVM Console
File View Macros Tools Power Virtual Media Help

```
        Cisco 12G SAS Modular Raid BIOS Configuration Utility 5.15-0610
 VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                         Drive Management
                                                          PAGE-1
             BackPlane                                Secured:
 Slot       Type      Capacity    State    DG  Vendor  No
 P0:01:01   HDD-SAS   278.464 GB  UG       -   TOSHIBA Encryption Capable:
 P0:01:02   HDD-SAS   279.396 GB  JBOD     -   TOSHIBA No
 P0:01:03   HDD-SAS   279.396 GB  JBOD     -   TOSHIBA EKM Support:
                                                      Enabled
                                                      Connector:
                                                      (P0 x1)
                                                      Enclosure Model:
                                                      SGPIO
                                                      Slot Number:
                                                      1
                                                      Logical Sector Size:
                                                      512 B
                                                      Physical Sector Size:
                                                      512 B
                                                      Product ID:
                                                      AL14SEB030N

                                                          <GoToPage:2>
F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

- **d** Repeat Steps 4a through 4c for remaining drives.

6 Go back to the **VD Mgmt** tab and press **CTRL+P**.

7 Select **No Configuration Present** and press **Enter**.

8 Configure the following:

- **a** From the RAID Level area, select **RAID-1**.
- **b** From the Secure VD area, select **No**.
- **c** From PD per Span area, enter **2**.
- **d** From the Drives area, use the UP or DOWN arrow to highlight the appropriate drive and press **Enter**. An **X** displays next to the drive to indicate that it is selected.
- **e** Repeat Step 8d to select the next drive that will make up this drive pair.

9 Go to the **Advanced** option and highlight the **Initialize** option.

10 Press **Enter**. An **X** is inserted next to Initialize to indicate that it is selected.

11 Click **Ok**.

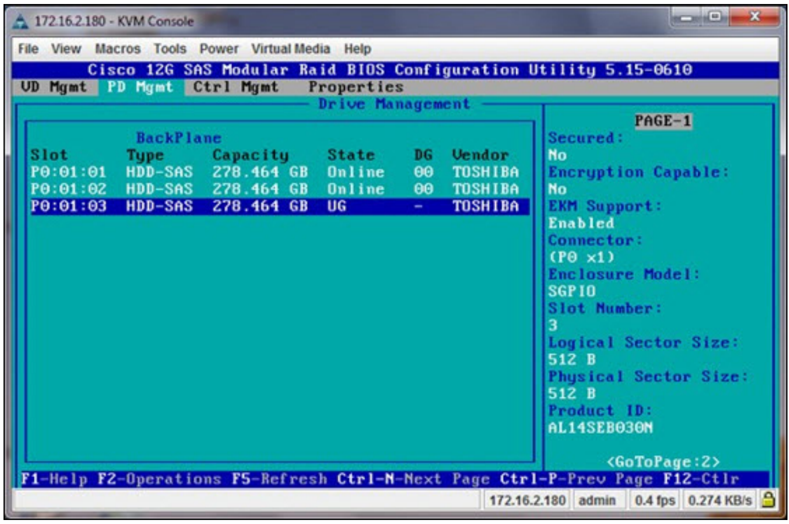
12 Click **Ok** to close the **Advanced** option window. The Configuration window is displayed.

13 Click **Ok** and system will now initialize the RAID-1 array. Wait for the initialization to complete.

14 Click **Ok** after the Confirmation window indicates that the initialization is complete.

15 Click **CTRL+N** to return to the **PD Mgmt** window.

16 From the PD Mgmt window, use the **UP** or **DOWN** arrows to highlight the **UG drive**.


172.16.2.180 - KVM Console
File View Macros Tools Power Virtual Media Help
172.16.2.180
admin
0.4 fps
0.274 KB/s

```
        Cisco 12G SAS Modular Raid BIOS Configuration Utility 5.15-0610
UD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                          Drive Management
                                                              PAGE-1
            BackPlane                                   Secured:
Slot        Type      Capacity     State     DG  Vendor   No
P0:01:01    HDD-SAS   278.464 GB   Online    00  TOSHIBA  Encryption Capable:
P0:01:02    HDD-SAS   278.464 GB   Online    00  TOSHIBA  No
P0:01:03    HDD-SAS   278.464 GB   UG        -   TOSHIBA  EKM Support:
                                                          Enabled
                                                          Connector:
                                                          (P0 x1)
                                                          Enclosure Model:
                                                          SGPIO
                                                          Slot Number:
                                                          3
                                                          Logical Sector Size:
                                                          512 B
                                                          Physical Sector Size:
                                                          512 B
                                                          Product ID:
                                                          AL14SEB030N
                                                             <GoToPage:2>
F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

.

17 Press **F2** and then select **Make Global HS**.

   Note: The state of the drive changes from **UG** to **Hotspare**.

18 Press **ESC** and click **Ok** to exit the utility.

19 Click the **Macros** tab and select **Static Macros > CTRL+ALT+DEL** to reboot the server.

   Note: The server must be rebooted for the changes to go into effect.

B

Backup and Restore Keyfiles

Due to the possibility of a catastrophic event (for example, hardware failure), it is important to create backups of the keyfiles on your PCG server. This will enable you to restore them in the event they are lost, damaged or inaccessible.

This chapter provides the procedures to backup and restore keyfiles. It is recommended that you backup and restore the following files:

- /opt/pcg/mon_app/mon.cfg
- /etc/snmp/snmpd.conf

In This Appendix

Backing Up Keyfiles

Complete the following steps to back up the keyfiles.

1 From the EC/DTACS terminal window. SSH into the PCG server as **admin** user.

2 As **root** user, enter the following command to change to the **/opt** directory.

```
[root@pcgtest ~]# cd /opt
```

3 Enter the following command to create a **pcgbkup-[PCG_IP]** directory.

Command Syntax:

```
mkdir /pcgbkup-[PCG_IP]
```

Example:

```
[root@pcgtest opt]# mkdir /pcgbkup-204.1.61.37
```

4 Copy the following key files to the **pcgbkup-[PCG_IP]** directory.

- /opt/pcg/mon_app/mon.cfg
- /etc/snmp/snmpd.conf

5 Execute the following command to create a tar ball.

Command Syntax:

```
tar cvf pcgbkup-[PCG_IP].tar pcgbkup-[PCG_IP]
```

Example:

```
[root@pcgtest opt]# tar cvf pcgbkup-204.1.61.100.tar
pcgbkup-204.1.61.100
```

6 Using scp, copy the tar file to a different server or NAS device.

Command Syntax:

```
scp pcgbkup-[PCG_IP].tar
admin:[NAS_IP]:[directory_on_EC/DTACS]
```

Example:

```
[root@pcgtest opt]# scp pcgbkup-204.1.61.100.tar
admin:10.90.181.146:/var/tmp
```

Restoring Keyfiles to a Recovered System

Complete the following steps to restore the keyfiles to a recovered PCG system.

1. Refer to the ***Deploy the PCG Virtual Machine*** (on page 7) to deploy a new PCG server.
2. Complete the following steps to restore the keyfiles from the server where you backed the files up to the PCG server.
   a. From the EC/DTACS terminal window, SSH into the newly installed PCG server as **admin** user.
   b. As **root** user, copy the **pcgbkup-[PCG_IP].tar** file from the backup server to the PCG server.

      Command Syntax:

      ```
      scp admin:[NAS_IP]:[directory_on_NAS]/pcgbkup-[PCG_IP].tar
      [directory_on_PCG]
      ```

      Example:

      ```
      [root@pcgtest opt]# scp
      admin:10.90.181.146:/var/tmp/pcgbkup-204.1.61.100.tar
      /var/tmp
      ```

   c. Enter the following command to untar the **/opt/pcgbkup-[PCG_IP].tar** file.

      Command Syntax:

      ```
      tar -xvf /var/tmp/pcgbkup-[PCG_IP].tar
      ```

      Example:

      ```
      [root@pcgtest ~]# tar -xvf
      /var/tmp/pcgbkup-204.1.61.100.tar
      ```

   d. Type **ls -ltr /var/tmp** to view the list of keyfiles.
   e. Copy the keyfiles to the appropriate locations.

      Command Syntax:

      ```
      cp [directory_location]/mon.cfg /opt/pcg/mon_app
      cp [directory_location]/snmpd.conf /etc/snmp
      ```

      Example:

      ```
      [root@pcgtest ~]# cp /var/tmp/mon.cfg /opt/pcg/mon_app
      [root@pcgtest ~]# cp /var/tmp/snmpd.conf /etc/snmp
      ```

3 Login to the EC/DTACS Web UI and access the PCG Web UI by executing the appropriate action. The PCG List window displays.

- **EC**: Network Element Provisioning > PCG
- **DTACS**: Network Elements > PCG

4 From the PCG List Web UI, select the appropriate **PCG** and click **Edit**.

5 Update the **Control MAC Address** and then click **Save**.

6 Return to the PCG List window and select the **PCG** again; then click **Reset**.

7 Verify the PCG version on the EC/DTACS server, as well as on the PCG server. Refer to ***Verifying PCG Package Versions on the EC/DTACS*** (on page 28) for details.

C

Upgrade the PCG Server

This appendix describes the procedures to upgrade the PCG application. The PCG package *is only* upgraded on the EC/DTACS server by updating the CSCOec-pcg rpm.

Important: The PCG application ***cannot*** be upgraded from the PCG server. You must upgrade the EC/DTACS server and then reboot the PCG to obtain the current PCG code.

In This Appendix

Upgrading the PCG Package on the EC/DTACS System

Complete the following steps to upgrade the PCG package (CSCOec-pcg) on an EC 9.0/8.0 or DTACS 5.2/5.0 system.

1 Refer to **Appendix D** in the ***Admin Node 2.0 User's Guide*** for procedures to upgrade the software repo with the PCG RPM package.

  Important: The software repo must be updated before continuing with the next step.

2 Login to the EC/DTACS server as **admin** user.

3 Enter the following command to upgrade the PCG application.

```
[admin@ec/dtacs ~]$ sudo yum update CSCOec-pcg
```

  Result: The upgrade process starts and after running various checks, displays a "Transaction Summary".

4 When prompted to confirm the upgrade, type **y** and press **Enter**. The PCG package is upgraded and a **Complete!** message displays.

5 Enter the following command to verify that the PCG package was successfully upgraded.

```
[admin@ec/dtacs ~]$ rpm -qa CSCOec-pcg
```

6 Go to the next section.

Upgrading the PCG Package on the PCG Server

Important: Once the PCG server is initially installed, you cannot upgrade the PCG application directly from the PCG. You must upgrade the PCG package on the EC/DTACS and then reboot the PCG server to pull the new code.

Complete the following steps to upgrade the PCG package on the PCG 4.1 server.

1. If you have not yet upgraded the PCG package on the EC/DTACS, go to the previous section to do so now.
2. After upgrading the EC/DTACS server, SSH into the PCG server as **admin** user.
3. Enter the following command to reboot the PCG server. The PCG SSH session closes and you are returned to the EC/DTACS session.

   ```
   [admin@pcgtest ~]$ sudo reboot now
   ```

4. After a few minutes, SSH back into the PCG server as **admin** user from the EC/DTACS.
5. Enter the following command to access the PCG console application.

   ```
   [admin@pcgtest ~]$ sudo /opt/pcg/console_app/cons
   ```

6. At the **PCG>** prompt, enter the following command to verify the version of the PCG package currently installed.

   ```
   PCG> vers
   ```

   Example Output:

   ```
   PCG> PCG version: 4.1.0-4. Build date : 27 August 2018
   ```

   Result: The PCG version on the EC/DTACS and the PCG server should match.

7. Press **Enter** to return to the PCG console application prompt.
8. Type **exit** to return to PCG prompt.

D

Manually Configure the PCG Network

This appendix explains how to manually configure the PCG network.

In This Appendix

Manually Configuring the PCG Network

Complete the following steps to manually configure the PCG network.

1 Depending on the server where the PCG is associated, enter one of the following commands.

EC 9.0/8.0:

```
[admin@ec/dtacs ~]$ less /etc/hosts | grep dncsatm
```

DTACS 5.2/5.0:

```
[admin@ec/dtacs ~]$ less /etc/hosts | grep dtacsatm
```

2 Record the IP addresses from Step 1 below:

dncsatm/dtacsatm: ____________________________

3 Enter the following command on the EC/DTACS to change to the **tftpboot** directory.

```
[admin@ec/dtacs ~]$ cd /var/lib/tftpboot
```

4 Enter the following command to secure copy the **pcg** file to the PCG server.

Command Syntax:

```
scp pcg admin@[PCG_IP]:/opt/pcg/pcg_app/app
```

Example:

```
[admin@ec/dtacs ~]$ scp pcg
admin@204.1.61.100:/opt/pcg/pcg_app/app
```

5 Enter the following command to secure copy the **pcg.cfg** file to the PCG server.

Command Syntax:

```
scp pcg.cfg admin@[PCG_IP]:/opt/pcg/pcg_app/app
```

Example:

```
[admin@ec/dtacs ~]$ scp pcg.cfg
admin@204.1.61.37:/opt/pcg/pcg_app/app
```

6 From the EC/DTACS terminal window, SSH to the PCG server as **admin** user.

7 Enter the following command to change the access rights of the **pcg** and the **pcg.cfg** files to **755**.

```
[admin@pcgtest ~]$ sudo chmod 755 /opt/pcg/pcg_app/app/pcg
/opt/pcg/pcg_app/app/pcg.cfg
```

8 Enter the following command to change the ownership of the **pcg** and the **pcg.cfg** files to **root:root**.

```
[admin@pcgtest ~]$ sudo chown root:root
/opt/pcg/pcg_app/app/pcg /opt/pcg/pcg_app/app/pcg.cfg
```

9 Open the **mon.cfg** file in a text editor.

```
[admin@pcgtest ~]$ sudo vi /opt/pcg/mon_app/mon.cfg
```

10 Go to the **skip-bootp** line and change the value from no to **yes**.

11 Save and close the **mon.cfg** file.

12 Open the **pcg.cfg** file in a text editor.

```
[admin@pcgtest ~]$ sudo vi /opt/pcg/pcg_app/app/pcg.cfg
```

13 Make the following changes in the **pcg.cfg** file.

- **RpcServerIPAddr**: enter the appropriate IP address recorded in Step 2
- **AlarmServerIPAddr**: enter the appropriate IP address recorded in Step 2
- **ForceDownload**: change the value to **no**
- Add the following lines to the end of the file:
  - **PcgScsInterface = ens224**
  - **PcgtoDncsIfIPAddr**: append the IP address for the PCG interface that communicates to the EC/DTACS

14 Save and close the **pcg.cfg** file.

15 Open the **ifcfg-ens192** file in a text editor and edit the following fields.

```
[admin@pcgtest ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

- **BOOTPROTO**: set to **Static**
- **IPADDR**: append the IP address of the PCG interface that communicates with the EC/DTACS
- **NETMASK**: append the subnet mask of the PCG interface that communicates with the EC/DTACS
- **ONBOOT**: set to **yes**

16 Save and close the **ifcfg-ens192** file.

17 Open the **ifcfg-ens224** file in a text editor and edit the following fields.

```
[admin@pcgtest ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens224
```

- **BOOTPROTO**: set to **Static**
- **IPADDR**: append the IP address of the PCG interface that communicates with the SCS on private network
- **NETMASK**: append the subnet mask of the PCG interface that communicates with the SCS on private network
- **ONBOOT**: set to **yes**

18 Save and close the **ifcfg-ens224** file.

19 Enter the following command to edit the **/etc/sysconfig/network-scripts/route-ens192** file.

Note: Substitute the IP address of the gateway that the PCG uses to communicate with the EC/DTACS for [PCG_IP_gw].

Command Syntax:

```
sudo default via [PCG_IP_gw] dev ens192
```

Example:

```
[admin@pcgtest ~]$ sudo default via 204.1.61.37 dev ens192
```

20 Enter the following command to edit the **/etc/sysconfig/network-scripts/route-ens224** file.

Note: Substitute the gateway that the PCG uses to communicate with the SCS on a private network.

Command Syntax:

```
sudo [network/subnet_mask] via [PCG_IP_gw] dev ens224
```

Example:

```
[admin@pcgtest ~]$ sudo 204.1.61.100/30 via 204.1.61.102 dev
ens192
```

21 Enter the following command to restart the network.

```
[admin@pcgtest ~]$ sudo systemctl restart network
```

E

Deliver ECMs to DHCTs

This appendix describes how the PowerKEY ECMs are delivered to the DHCTs. The process begins with system initialization and proceeds to the EC/DTACS server. The SCS or scrambler interactions are outlined below.

- The PCG is fully configured and provisioned.
- The EC/DTACS server creates sessions on the PCG.
- The SCS establishes a TCP connection, channel and valid streams on the PCG.
- The PCG responds with ECM streams for existing sessions/services setup by the EC/DTACS server on the PCG.

In This Appendix

Delivering ECMs

Complete the following steps to deliver ECMs to DHCTs.

1 When the PCG powers up, configure it manually or using BOOTP. The SCS-facing port receives its network address and the PCG application is launched.

   Result: The PCG sends a provision request to the EC/DTACS server. When the EC/DTACS server receives the request, it sends the PCG a provision response. The response contains data that sets the EC-facing network address for communication with the scrambler device(s).

   Optional: The response may inform the PCG about how many devices can communicate with the PCG, provide their IP addresses, and indicate how many programs can be serviced on each device.

   Note: The PCG can support a maximum of 3000 sessions.

2 Create a session from the EC/DTACS Web UI. This provides the access criteria for the PCG service.

   Note: If you are using ROSA for access criteria management, then configure the EIS or Access Criteria Manager Component (ACMC) through the ROSA element manager. Ensure the access criteria specified here match the access criteria explicitly administered on the EC/DTACS source definition Web UI for the associated service or program. Access criteria can be configured through the ACMC.

   - A single channel over a TCP connection serves multiple programs. When a program is scheduled for scrambling, the SCS sets up a stream for the program. The scrambler issues access criteria and control words to the PCG for the session, and the PCG responds with the ECMs.
   - The SCS then sends the ECMs and the scrambled program (with the corresponding control word) to the built-in modulator. From there it goes to the RF and then to the set-top.

   Note: If the PCG communicates with an SCS device that does not have a built-in modulator, then a separate modulator is needed to provide RF.

Notes:

- PCG scrambling modes are changed in the EC/DTACS to support the new modes added for AES-128 scrambling.
- EC and DTACS support configuring PCG scramble mode for the following AES modes:
  - AES-ECB-CTS
  - ATIS-IIF-DSA
  - AES-NSA (or AES-DVB-LSA-CBC-MDI)

F

Troubleshoot PCG Issues

This appendix provides some basic troubleshooting tips for potential issues related to the PCG.

In This Appendix

Troubleshooting Boot Issues

If boot issues are present, refer to the following files to assist you in troubleshooting the issue.

PCG:

- /var/log/mon.log

EC:

- /dvs/dncs/bin/bootpd
- /var/log/dncsLog

DTACS:

- /dvs/dtacs/bin/bootpd
- /var/log/dncsLog

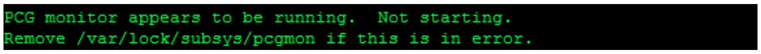
Removing the pcgmon Lock File

A common issue can occur when the PCG server is rebooted without properly shutting down the PCG processes. The issue is that a pcgmon lock file is created and prevents the pcgmon process from starting.

Complete the following steps to remove the PCG application lock file from the PCG.

1 Enter the following command in a PCG terminal window to manually start the **pcgmon** service.

```
[admin@pcgtest ~]$ sudo systemctl start pcgmon
```



```
PCG monitor appears to be running.  Not starting.
Remove /var/lock/subsys/pcgmon if this is in error.
```

2 Enter the following command to remove the **/var/lock/subsys/pcgmon** file.

```
[admin@pcgtest ~]$ sudo rm /var/lock/subsys/pcgmon
```

3 When prompted to remove the file, enter **y**.

4 Repeat Step 1 to start the **pcgmon** service.

5 Enter the following command to verify that the pcgmon service is now running.

```
[admin@pcgtest ~]$ sudo systemctl status pcgmon
```

G

Reset the Password for the admin User

This appendix provides the procedure to change the password for the admin user in the event the password is lost, forgotten or expired.

In This Appendix

Resetting the Password for the admin User

Complete the following procedure to reset the password for the admin user.

Note: This procedure is written using the vSphere 6.0 Web UI. If you are using a different version or if you are using a vSphere client, the steps may differ.

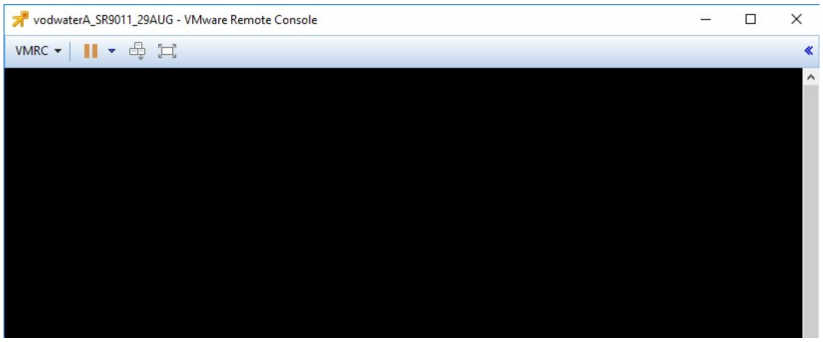
1 From a Web browser, log into the vSphere 6.0 Web UI.

2 Select the VM in which the admin password needs reset.

3 From the right section of the window, click the Summary tab.

4 Click the **Launch Remote Console** link. The VMware Remote Console window opens for the VM opens in a new window.

Important: If you have not yet downloaded the Remote Console, click the **Download Remote Console** link in the Summary window. Follow the prompts to install the remote console. Then click **Launch Remote Console**.



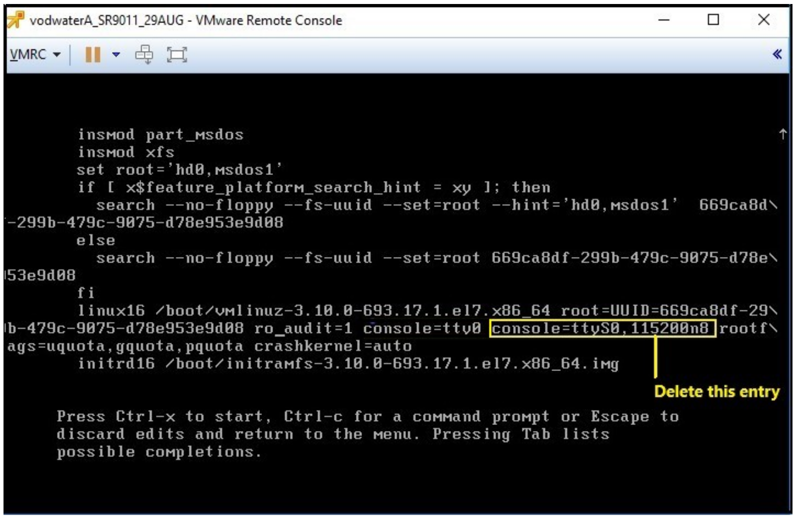
5 Select **VMRC > Ctrl+Alt+Del** to reboot the VM.

6 Use your arrow keys to select the appropriate boot entry from the Grub menu and then press **e** to edit the entry.

Note: In most cases, the first entry is the appropriate entry; therefore, you can simply enter **e** to edit the entry.

7 Use your down arrow key to move to the **linux16** line and delete the following text.

```
console=ttypsS0,115200n8
```

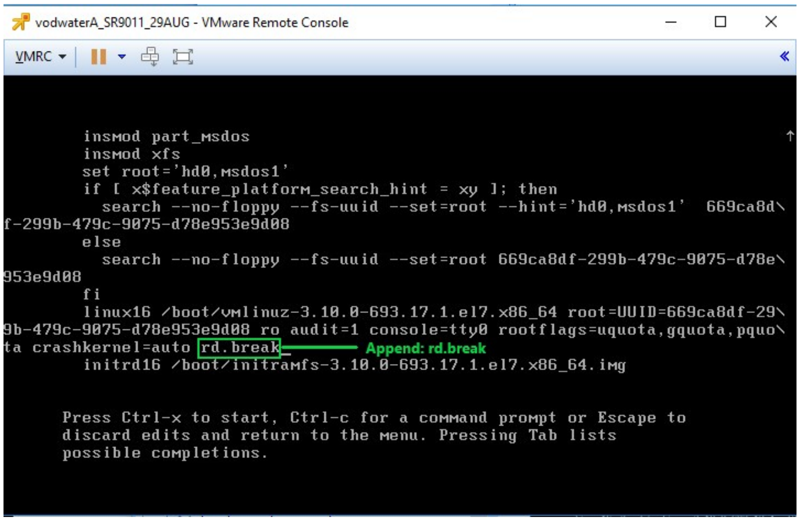


```
        insmod part_msdos
        insmod xfs
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  669ca8d\
-299b-479c-9075-d78e953e9d08
        else
          search --no-floppy --fs-uuid --set=root 669ca8df-299b-479c-9075-d78e\
53e9d08
        fi
        linux16 /boot/vmlinuz-3.10.0-693.17.1.el7.x86_64 root=UUID=669ca8df-29\
b-479c-9075-d78e953e9d08 ro_audit=1 console=tty0 console=ttyS0,115200n8 rootf\
ags=uquota,gquota,pquota crashkernel=auto
        initrd16 /boot/initramfs-3.10.0-693.17.1.el7.x86_64.img

      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

8 Move to the end of this line and add the following text.

```
rd.break
```



```
        insmod part_msdos
        insmod xfs
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  669ca8d\
f-299b-479c-9075-d78e953e9d08
        else
          search --no-floppy --fs-uuid --set=root 669ca8df-299b-479c-9075-d78e\
953e9d08
        fi
        linux16 /boot/vmlinuz-3.10.0-693.17.1.el7.x86_64 root=UUID=669ca8df-29\
9b-479c-9075-d78e953e9d08 ro audit=1 console=tty0 rootflags=uquota,gquota,pquo\
ta crashkernel=auto rd.break_
        initrd16 /boot/initramfs-3.10.0-693.17.1.el7.x86_64.img

      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

9 Press **Ctrl+x** to resume the boot process of the VM. The system boots to the bash prompt.

Note: The modifications that were made are only temporary and will not be saved.

10 At the prompt, type the following command and press **Enter** to mount the root file system with read/write access.

```
switch_root:/# mount -o remount,rw /sysroot
```

11 At the prompt, type the following command and press **Enter**.

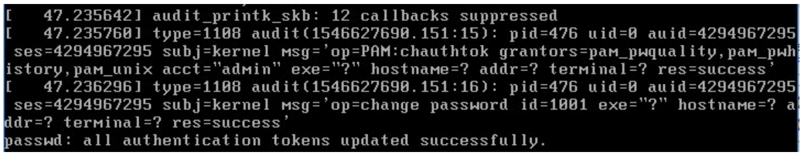
```
switch_root:/# chroot /sysroot
```

12 Enter the following command to change the password for the **admin** user.

```
sh-4.2# passwd admin
```

13 When prompted, enter the new password for the **admin** user and then press **Enter**.

14 When prompted to retype the password, re-enter the new password and then press **Enter**. The output should resemble the following:



```
[   47.235642] audit_printk_skb: 12 callbacks suppressed
[   47.235760] type=1108 audit(1546627690.151:15): pid=476 uid=0 auid=4294967295
 ses=4294967295 subj=kernel msg='op=PAM:chauthtok grantors=pam_pwquality,pam_pwh
istory,pam_unix acct="admin" exe="?" hostname=? addr=? terminal=? res=success'
[   47.236296] type=1108 audit(1546627690.151:16): pid=476 uid=0 auid=4294967295
 ses=4294967295 subj=kernel msg='op=change password id=1001 exe="?" hostname=? a
ddr=? terminal=? res=success'
passwd: all authentication tokens updated successfully.
```

15 At the prompt, enter the following command and press **Enter**.

```
sh-4.2# touch /.autorelabel
```

16 At the prompt, type **exit** and press **Enter**.

```
sh-4.2# exit
```

17 At the prompt, type **exit** again and press **Enter**. The boot process is resumed on the VM.

18 As **admin** user, login with your new password.

Index

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883