PowerKEY Server for Encrypted VOD in an IBDS Network
Installation and Upgrade Guide
Please Read

Important

Please 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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of cisco trademarks, go to this URL: www.cisco.com/go/trademarks.

DVB is a registered trademark of the DVB project.

Other third party trademarks mentioned are the property of their respective owners.
The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2009-2011, 2012 Cisco and/or its affiliates. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.
# Contents

**Safety Precautions**

**About This Guide**

**Chapter 1 PKES Hardware Installation**
Overview of the PowerKEY Encryption Server ........................................ 2
The PKES Hardware .................................................................................. 3
PKES Front Panel Description .................................................................. 4
PKES Back Panel Description ................................................................. 5
Rack Mounting ......................................................................................... 6

**Chapter 2 PKES Platform Installation**
Install the PKES Platform ..................................................................... 12

**Chapter 3 VOD MSK Management**
Create and Configure the VOD MSK .................................................... 20

**Chapter 4 PKES Software Installation and Configuration**
Overview of the PKES Application ....................................................... 24
Install the PKES Software ..................................................................... 25
Configure the PKES Application .......................................................... 27
Configure SNMP on the PKES ............................................................ 38
Configure NTP on the PKES ................................................................. 39
Enable Support for Clear DRM VOD Assets (Optional) ....................... 41
Restart the PKES Application ............................................................... 42

**Chapter 5 PKES Upgrade Procedures**
Upgrade the PKES Software ................................................................. 44

**Chapter 6 Customer Information**

---

4026603 Rev H
Appendix A Troubleshooting the PKES 65

Verify CAS Manager Delegates Online ................................................................. 66
Low Disk Space ........................................................................................................ 67
Manage PKES Log File ............................................................................................ 68
Assets Processing Slowly ....................................................................................... 69
Safety Precautions

Read, Retain, and Follow These Instructions
Carefully read all safety and operating instructions before operating this product. Follow all operating instructions that accompany this product. Retain the instructions for future use. Give particular attention to all safety precautions.

Warning and Caution Icons

![WARNING:]

Avoid personal injury and product damage! Do not proceed beyond any icon until you fully understand the indicated conditions.

The following icons alert you to important information about the safe operation of this product:

- You will find this icon in the literature that accompanies this product. This icon indicates important operating or maintenance instructions.
- You may find this icon affixed to this product and in this document to alert you of electrical safety hazards. On this product, this icon indicates a live terminal; the arrowhead points to the terminal device.
- You may find this icon affixed to this product. This icon indicates a protective earth terminal.
- You may find this icon affixed to this product. This icon indicates excessive or dangerous heat.
- You may find this symbol affixed to this product and in this document. This symbol indicates an infrared laser that transmits intensity-modulated light and emits invisible laser radiation and an LED that transmits intensity-modulated light.

Heed All Warnings
Adhere to all warnings on the product and in the operating instructions.

Avoid Electric Shock
Follow the instructions in this warning.
WARNING: To reduce risk of electric shock, perform only the instructions that are included in the operating instructions. Refer all servicing to qualified service personnel.

Servicing

WARNING: Avoid electric shock! Opening or removing the cover may expose you to dangerous voltages.

Do not open the cover of this product and attempt service unless instructed to do so in the operating instructions. Refer all servicing to qualified personnel only.

Cleaning, Water, Moisture, Open Flame

To protect this product against damage from moisture and open flames, do the following:

- Before cleaning, unplug this product from the AC outlet. Do not use liquid or aerosol cleaners. Use a dry cloth for cleaning.
- Do not expose this product to moisture.
- Do not place this product on a wet surface or spill liquids on or near this product.
- Do not place or use candles or other open flames near or on this product.

Ventilation

To protect this product against damage from overheating, do the following:

- This product has openings for ventilation to protect it from overheating. To ensure product reliability, do not block or cover these openings.
- Do not open this product unless otherwise instructed to do so.
- Do not push objects through openings in the product or enclosure.

Placement

To protect this product against damage from breakage, do the following:

- Place this product close enough to a mains AC outlet to accommodate the length of the product power cord.
- Route all power supply cords so that people cannot walk on, or place objects on, or lean objects against them. This can pinch or damage the cords. Pay particular attention to cords at plugs, outlets, and the points where the cords exit the product.
- Make sure the mounting surface or rack is stable and can support the size and weight of this product.

**WARNING:**

Avoid personal injury and damage to this product! An unstable surface may cause this product to fall.
Safety Precautions

When moving a cart that contains this product, check for any of the following possible hazards:

- Move the cart slowly and carefully. If the cart does not move easily, this condition may indicate obstructions or cables that you may need to disconnect before moving this cart to another location.
- Avoid quick stops and starts when moving the cart.
- Check for uneven floor surfaces such as cracks or cables and cords.

**WARNING:**

Avoid personal injury and damage to this product! Move any appliance and cart combination with care. Quick stops, excessive force, and uneven surfaces may cause the appliance and cart to overturn.

### Fuse

When replacing a fuse, heed the following warnings.

**WARNING:**

Avoid electric shock! Always disconnect all power cables before you change a fuse.

**WARNING:**

Avoid product damage! Always use a fuse that has the correct type and rating. The correct type and rating are indicated on this product.

### Grounding This Product (U.S.A. and Canada Only)

#### Safety Plugs

If this product is equipped with either a three-prong (grounding pin) safety plug or a two-prong (polarized) safety plug, do not defeat the safety purpose of the polarized or grounding-type plug. Follow these safety guidelines to properly ground this product:

- For a 3-prong plug (consists of two blades and a third grounding prong), insert the plug into a grounded mains, 3-prong outlet.
  
  *Note:* This plug fits only one way. The grounding prong is provided for your safety. If you are unable to insert this plug fully into the outlet, contact your electrician to replace your obsolete outlet.

- For a 2-prong plug (consists of one wide blade and one narrow blade), insert the plug into a polarized mains, 2-prong outlet in which one socket is wider than the other.

  *Note:* If you are unable to insert this plug fully into the outlet, try reversing the plug. The wide blade is provided for your safety. If the plug still fails to fit, contact an electrician to
replace your obsolete outlet.
Grounding Terminal
If this product is equipped with an external grounding terminal, attach one end of an 18-gauge wire (or larger) to the grounding terminal; then, attach the other end of the wire to an earth ground, such as an equipment rack that is grounded.
About This Guide

Introduction

This guide describes the PowerKEY™ Encryption Server (PKES). Refer to this guide for installing, upgrading, and troubleshooting your PKES.

Audience

This document is written for system operators of the IPTV Broadband Delivery System (IBDS). Headend operators and support engineers may also find the contents of this document to be useful.

Document Version

This is the seventh formal release of this document. In addition to minor text and graphic changes, the following table provides the technical changes to this document.

<table>
<thead>
<tr>
<th>Description</th>
<th>See Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages displayed by the system when creating the VOD MSK on the TED were updated.</td>
<td>See VOD MSK Management (on page 19).</td>
</tr>
<tr>
<td>Minor edits were made to the Upgrading the PKES Application Software procedure that better describe the flow of events.</td>
<td>See Upgrading the PKES Application Software (on page 48).</td>
</tr>
<tr>
<td>Added a troubleshooting appendix.</td>
<td>See Troubleshooting the PKES (on page 65).</td>
</tr>
</tbody>
</table>
Introduction

This chapter describes the PowerKEY Encryption Server (PKES) and outlines the procedures required for installing the PKES hardware.

If you are installing PKES software for the first time, complete the procedures in Chapters 1 through 4. If you are upgrading the PKES, complete the procedures in Chapter 5.

In This Chapter

- Overview of the PowerKEY Encryption Server ......................... 2
- The PKES Hardware........................................................................ 3
- PKES Front Panel Description ..................................................... 4
- PKES Back Panel Description....................................................... 5
- Rack Mounting.............................................................................. 6
Overview of the PowerKEY Encryption Server

The PowerKEY Encryption Server (PKES) is a computer server that "pre-encrypts" video-on-demand (VOD) content in a format that is compatible with the PowerKEY Conditional Access System (CAS).

**Note:** Pre-encryption refers to the fact that the VOD "asset" is encrypted before it is stored on a VOD server. Previous solutions stored the asset in the clear and did not encrypt the VOD asset until ordered by a subscriber.

The PKES connects to an asset manager. When VOD content is ready to be processed, the asset manager sends a notification to the PKES which results in the initiation of an FTP transfer from the asset manager. The notification includes a setting that directs the PKES to either encrypt the content or leave it in the clear but apply copy protection. In both cases, the PKES inserts appropriate PowerKEY Entitlement Control Messages (ECMs) into the file. When the encryption setting is enabled, the PKES encrypts packets that have been previously marked for encryption. Once the processing of the file is complete, the PKES FTPs the file back to the asset manager for storage. Both the PKES and ISDS must be provisioned with a key generated by the Transaction Encryption Device (TED) before encryption can occur.
The PKES Hardware

We occasionally update the PKES hardware to take advantage of newer technologies as they become available. This guide presents examples based on a typical server configuration.

Refer to the hardware install guide provided with your PKES server for specifics on how to physically install the server and for safety recommendations regarding server placement and cooling requirements.

Before beginning your installation, read the Safety Precautions (on page v) at the beginning of this document. Pay particular attention to the Placement topic in the Safety Precautions section.

Site Requirements

Your site must meet the following requirements before you proceed with the installation:

- The hardware must be installed in a standard four-post rack. See Rack Mounting (on page 6) in the next section for the rack requirements.
- Approved power sources: 90 to 120 V AC (continuous)
- Racking and environment temperature: Inside rack temperature must be maintained at between 0° and +50°C (32° and 122°F)
PKES Front Panel Description

The PKES is a rack-mounted server designed to work seamlessly within a number of different architectures.

Front Panel Connectors and Controls

The PKES front panel connectors and controls are shown below (image may vary from actual product and specification).

The following table describes the front panel connectors and controls from left to right.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. DVD-ROM drive</td>
<td></td>
</tr>
<tr>
<td>2. Three Hard Drives</td>
<td>146 GB Hard Drives</td>
</tr>
<tr>
<td>3. Power Button</td>
<td>On/Off button</td>
</tr>
<tr>
<td>4. Reset Switch</td>
<td>System restart</td>
</tr>
<tr>
<td>5. ID Switch/NMI Switch</td>
<td>On/Off button for the shelf identification LED</td>
</tr>
<tr>
<td>6. LED Indicators</td>
<td>Critical alarm LED, Major alarm LED, Minor alarm LED, Power alarm LED,</td>
</tr>
<tr>
<td></td>
<td>System ID LED, NIC activity LED, Main power LED, HDD activity LED</td>
</tr>
<tr>
<td>7. Serial Com Port</td>
<td>RJ45 serial port</td>
</tr>
<tr>
<td>8. USB 2.0 Connector</td>
<td>Peripheral equipment connections</td>
</tr>
</tbody>
</table>

*For details about the hardware, refer to the data sheet for this product.
PKES Back Panel Description

Back Panel Connectors

The back panel connectors are shown below (image may vary from actual product and specification).

The following table describes the back panel connectors from left to right.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. PS/2 Connector</td>
<td>Mouse Connector</td>
</tr>
<tr>
<td>2. PS/2 Connector</td>
<td>Keyboard Connector</td>
</tr>
<tr>
<td>3. DB-15 Serial Port Connector</td>
<td>Alarms Connector</td>
</tr>
<tr>
<td>4. Serial Com Port Connector</td>
<td>RJ45 Serial Port</td>
</tr>
<tr>
<td>5. Gigabit Ethernet Connectors</td>
<td>Network connections:</td>
</tr>
<tr>
<td></td>
<td>1 = eth0</td>
</tr>
<tr>
<td></td>
<td>2 = eth1</td>
</tr>
<tr>
<td>6. Six expansion slots</td>
<td>Expansion Slots</td>
</tr>
<tr>
<td>7. Video Connector</td>
<td>Monitor connection</td>
</tr>
<tr>
<td>8. USB 2.0 Connector</td>
<td>Peripheral device connection</td>
</tr>
<tr>
<td>9. RMM2 Ethernet Interface</td>
<td>Ethernet interface for the remote management module</td>
</tr>
<tr>
<td>10. Power Connector</td>
<td>AC power cord connection</td>
</tr>
<tr>
<td>11. Power Supply Indicator LED</td>
<td>Status indicator lights for the power supply units</td>
</tr>
</tbody>
</table>
Rack Mounting

Installing the PKES in the Rack

Follow these steps to install the PKES in the rack using the angle support brackets.

**CAUTION:**
Avoid personal injury and damage to this product! Be sure to support the server from underneath until it is securely positioned in the rack. Failure to do so could result in the server falling to the floor. The server could be damaged and you could be injured as a result.

1. Make sure that the site requirements are met as outlined in the previous section.
2. Determine the approximate position in the equipment rack where you want the bottom of the PKES to be located. Then, position the angle support brackets in the rack. The cut-outs in the brackets must face toward the back of the rack as shown in the following illustration.
3  Attach the angle support brackets to the equipment rack using rack screws or other mounting hardware that came with your rack.

4  Slide the PKES into the equipment rack and onto the angle support brackets from the front of the rack until the front panel mounting flanges on the PKES are flush with the front mounting rails of the rack.

5  While holding the PKES in this position, make sure that the bottom of the unit is supported by the angle support brackets on both sides along the entire depth of the PKES chassis.

6  Check that the PKES front panel thumbscrews on both sides align with the proper mounting holes on the equipment rack.

<table>
<thead>
<tr>
<th>If the thumbscrews...</th>
<th>THEN...</th>
</tr>
</thead>
<tbody>
<tr>
<td>align with holes in the rack</td>
<td>carefully remove the PKES from the rack and go to step 7.</td>
</tr>
</tbody>
</table>
do not align with holes in the rack carefully remove the PKES from the rack and repeat steps 4 and 5 until the thumbscrews align correctly, and the weight of the PKES is fully supported by the angle support brackets along both sides of the PKES.

7 Securely tighten the rack screws (or other mounting hardware) that hold the angle support brackets in the rack.

8 Re-insert the PKES into the equipment rack and onto the angle support brackets from the front of the rack until the front panel mounting flanges of the PKES are flush with the front mounting rails of the rack.

9 Tighten the two thumbscrews to secure the server in the rack.

**Important:** Verify that the weight of the server is still supported by the angle support brackets on both sides. If not, go back to step 5.

10 If you plan to use the keyboard, mouse, and monitor, attach them to their respective rear panel connectors.

11 Connect the input power cord to the rear panel.

12 Attach the front panel bezel if it is available and if you plan to use it.
Additional PKES Requirements

To install and configure the PKES software, the PKES must have a standard keyboard and monitor connected to it.

Removing the PKES from the Rack

Follow these steps to remove the PKES from the rack.

⚠️ CAUTION:
Avoid personal injury and damage to this product! Be sure to support the server from underneath while removing it from the rack. Failure to do so could result in the server falling to the floor. The server could be damaged and you could be injured as a result.

Note: You do not need to remove the optional front bezel to install or remove the system from the rack.

1. Turn off the system and attached peripherals.
2. Disconnect the system from the electrical power.
3. Disengage both thumbscrews from the front panel of the chassis.
4. Carefully pull the system forward and out of the rack.
2

PKES Platform Installation

Introduction

The instructions in this chapter describe how to install the PKES platform software for the first time.

If you are upgrading the PKES, skip this chapter and complete the procedures in Chapter 5.

In This Chapter

- Install the PKES Platform ................................................................. 12
Install the PKES Platform

Follow these instructions to install the PKES platform.

Important: A keyboard and a monitor need to be connected to the PKES before installing the platform software.

1. If the server is not powered on, press the power button on the front of the server. The server powers on.
2. Insert the PKES platform CD into the CD drive of the PKES. After a few minutes, the Cisco screen appears.
3. Type `platform` and press Enter. The system runs an automated installation script.
   Notes:
   - The installation script should complete within 15 minutes and the system automatically reboots and ejects the CD.
   - The operator will be unable to log in until the system has rebooted.
4. Remove the CD from the CD drive of the PKES.
5. After the system has rebooted, log on to the PKES as root user.

Configuring the Management Network Interfaces

Follow these instructions to configure the management network interface for the PKES. This is the interface that is used to communicate with the ISDS and other management devices within the network.

1. On the PKES, type the following command and then press Enter. The `/etc/sysconfig/network-scripts` becomes the working directory.
   ```bash
   cd /etc/sysconfig/network-scripts
   ```
2. Type the following command and then press Enter. The `ifcfg-eth1` file opens for editing using the `vi` text editor.
   ```bash
   vi ifcfg-eth1
   ```
3. Add the following information to the `ifcfg-eth1` file:
   ```bash
   # Intel Corporation 80003ES2LAN Gigabit Ethernet Controller (Copper)
   DEVICE=eth1
   BOOTPROTO=static
   DHCPCLASS=
   HWADDR=00:0E:0C:E5:F1:20
   IPADDR=172.105.1.173
   NETMASK=255.255.255.240
   ONBOOT=yes
   ```
Important: The values used for HWADDR, IPADDR, and NETMASK in the preceding example are for illustration, only. Use the actual MAC address, IP address, and netmask of the PKES in use on your system.

4 Save and close the ifcfg-eth1 file.

Configuring the CAS Network Interface

Follow these instructions to configure the CAS network interface for the PKES. The CAS network interface is the interface that is used to communicate with video-on-demand (VOD) equipment, such as the AMS and NAS devices within the network.

1 On the PKES, type the following command and then press Enter. The /etc/sysconfig/network-scripts becomes the working directory.

   cd /etc/sysconfig/network-scripts

2 Type the following command and then press Enter. The ifcfg-eth0 file opens for editing using the vi text editor.

   vi ifcfg-eth0

3 Add the following data to the ifcfg-eth0 file:

   # Intel Corporation 80003ES2LAN Gigabit Ethernet Controller (Copper)
   DEVICE=eth0
   BOOTPROTO=static
   DHCPCLASS=
   HWADDR=00:0E:0C:E5:F1:21
   IPADDR=192.168.1.173
   NETMASK=255.255.255.240
   ONBOOT=yes

Important: The values used for HWADDR, IPADDR, and NETMASK in the preceding example are for illustration, only. Use the actual MAC address, IP address, and netmask of the PKES in use on your system.

4 Save and close the ifcfg-eth0 file.

Configuring the Routing Information

Follow these instructions to configure the routing information for the PKES.

1 At the PKES, type the following command and then press Enter. The /etc/sysconfig/network-scripts directory becomes the working directory.
cd /etc/sysconfig/network-scripts

2 Type the following command and then press Enter. The route-eth0 file opens for editing in the vi text editor.

vi route-eth0
3 Add the following lines to the route-eth0 file:

GATEWAY0=[the IP address of the Headend Control router]
NETMASK0=0.0.0.0
ADDRESS0=0.0.0.0

Example: When you are finished, the route-eth0 file should look similar to the following example:

GATEWAY0=172.105.1.174
NETMASK0=0.0.0.0
ADDRESS0=0.0.0.0

4 Save the route-eth0 file and close the vi editor.

5 Type the following command and then press Enter. The route-eth1 file opens for editing in the vi text editor.

vi route-eth1

6 Add the following lines to the route-eth1 file:

GATEWAY0=[The IP address of the Asset Ingest router]
NETMASK0=255.255.255.255
ADDRESS0=[The IP address of the Ericsson AMS-PKES]

GATEWAY1=[The IP address of the Asset Ingest router]
NETMASK1=255.255.255.255
ADDRESS1=[The IP address of the Ericsson NAS]

Example: When you are finished, the route-eth1 file should look similar to the following example:

GATEWAY0=192.106.1.174
NETMASK0=255.255.255.255
ADDRESS0=192.106.2.177

GATEWAY1=192.106.1.174
NETMASK1=255.255.255.255
ADDRESS1=192.106.2.178

7 Save and close the route-eth1 file.

**Configuring the PKES Hostname**

Follow these instructions to configure the hostname on the PKES.

1 At the PKES, type the following command and then press Enter. The /etc/sysconfig directory becomes the working directory.

```
4026603 Rev H
```
2 Type the following command and then press Enter. The network file opens for editing in the vi text editor.

```bash
vi network
```
3. Add the following lines to the network file:

```plaintext
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=[PKES Hostname]
```

**Example:** When you are finished, the network file should look similar to the following example:

```plaintext
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=PKES1
```

4. Save and close the network file.

**Activate the PKES Platform Configuration**

After installing the PKES platform software and editing the network interface and route files, follow these instructions to activate those changes, and to test the connection between the ISDS and the PKES.

1. Ensure that the network cables are connected to the PKES.

2. While logged into the PKES, type the following command and then press Enter to reboot the PKES server and activate the PKES platform configuration.

   ```plaintext
   shutdown -y -g0 -i6
   ```

3. After the PKES has rebooted, from an xterm window on the ISDS, type the following command and press Enter to verify connectivity.

   ```plaintext
   ping [PKES MGMT IP address]
   ```
3

VOD MSK Management

Introduction
After setting up the PKES platform, your next task is to create and configure the video-on-demand multi-session key (VOD MSK) for the PKES. The instructions in this chapter guide you through the necessary steps.

If you are upgrading the PKES, skip this chapter and complete the procedures in Chapter 5.

In This Chapter
- Create and Configure the VOD MSK......................................................... 20
Create and Configure the VOD MSK

Creating the VOD MSK on the TED

Follow these instructions to set up the VOD MSK on the TED.

1. If necessary, open an xterm window on the ISDS.
2. Complete the following steps to log on to the xterm window as root user.
   a. Type `su -` and press Enter. The password prompt appears.
   b. Type the root password and press Enter.
3. Type the following command and then press Enter to remotely log on to the TED.
   `ssh root@dncsted`
4. When presented with the password prompt, enter the password for the root user on the TED.
5. Type the following command and then press Enter. The `/home/teduser/bin` directory on the TED becomes the working directory.
   `cd /home/teduser/bin`
6. Type the following command and then press Enter. The GenMsk script runs and a menu appears.
   `./GenMsk`
7. Select menu option 1, Generate MSK with VOD passphrase. A message appears, prompting you to enter a new pass phrase.
8. Type a VOD pass phrase that ranges from 10 to 64 characters long. A prompt to re-enter the pass phrase appears.
   **Important:** If you do not know the pass phrase, contact your System Administrator. Your System Administrator creates the pass phrase and stores it in a secured location.
9. Type your VOD pass phrase again. A message appears that prompts you to enter the location of where you want to store the encrypted MSKs.
10. Type the following location and press Enter. The vodMskPkes file is written to the specified directory.
    `/home/teduser/bin/`
11. Select menu option 2, Generate MSK with EA Passphrase. The system prompts you to enter the VOD pass phrase.
12. Type the VOD pass phrase that you created in step 8. The system prompts you to enter the location where the encrypted MSKs are stored.
Create and Configure the VOD MSK
13 Type the following location and press Enter.
/home/teduser/bin/
Result: The system prompts you to enter the location where you want to store
the encrypted MSKs.
14 Type the following location and press Enter. The file, which is titled vodMskIsds,
is written to the specified directory.
/home/teduser/bin/
15 Select menu option 3 to exit from the menu.
16 Type exit and then press Enter to close the remote login to the TED.

Configuring the VOD MSK on the ISDS

Follow these instructions to set up the VOD MSK on the ISDS.
1 If necessary, open an xterm window on the ISDS.
2 Type the following command and then press Enter to log on as the dncs role.
su - dncs
3 Type the following command and press Enter.
mkdir /export/home/dncs/vodMsk
4 Type the following command and press Enter.
cd /export/home/dncs/vodMsk
5 Type the following command and press Enter to copy the VOD MSK files from
the TED to the ISDS.
scp root@dncsted:/home/teduser/bin/vodMsk* /export/home/dncs/vodMsk
Note: When prompted for the password, enter the password for the root user on
the TED.
6 Type the following command and then press Enter. A camDncsTedInit menu
appears.
camDncsTedInit
7 Select option 5. A message appears that prompts you to enter the complete path
and file name of where VOD MSK files are stored on the ISDS.
8 Type the following command and press Enter.
/export/home/dncs/vodMsk/vodMskIsds
9 Select option 2 to upload the TED with the updated MSK. Follow the prompts to
enter both the EA and CAA pass phrases.
10 Select option 6 to exit from the camDncsTedInit menu.
PKES Software Installation and Configuration

Introduction

Use the procedures in this chapter to help you install and configure the PKES software.

If you are upgrading the PKES, skip this chapter and complete the procedures in Chapter 5.

In This Chapter

- Overview of the PKES Application .................................................... 24
- Install the PKES Software ............................................................... 25
- Configure the PKES Application ...................................................... 27
- Configure SNMP on the PKES ......................................................... 38
- Configure NTP on the PKES ............................................................ 39
- Enable Support for Clear DRM VOD Assets (Optional) .......... 41
- Restart the PKES Application .......................................................... 42
Overview of the PKES Application

Anyone who configures the PKES application is likely to benefit from understanding the structure of the PKES package. The following table describes the directories that comprise the PKES package.

**Note:** In the table that follows, `<PKES pkg>` represents a placeholder for the full path of the PKES software (for example, `/usr/local/pkses`).

<table>
<thead>
<tr>
<th>Package Directories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;PKES pkg&gt;/bin</code></td>
<td>This directory holds the executable files for the PKES application.</td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/config</code></td>
<td>This directory contains configuration files used by the PKES application.</td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/content</code></td>
<td>These directories hold the in-process VOD content, as well as VOD files that are retained for debugging purposes when an error occurs.</td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/content/current</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/content/current/clear</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/content/current/encrypted</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/content/error</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/content/error/clear</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/content/error/encrypted</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/logs</code></td>
<td>This directory contains the PKES log file and asset status tables recorded by the PKES applications for use by SNMP.</td>
</tr>
<tr>
<td><code>&lt;PKES pkg&gt;/config/</code></td>
<td>These directories contain the PKES SNMP configuration and MIB files.</td>
</tr>
<tr>
<td><code>/usr/share/snmp/</code></td>
<td></td>
</tr>
<tr>
<td><code>/usr/share/snmp/mibs/</code></td>
<td></td>
</tr>
</tbody>
</table>
Install the PKES Software

1. If necessary, open an xterm window on the ISDS.
2. Type the following command and press Enter to log on to the PKES from the ISDS.
   ```
   ssh root@[PKES MGMT IP address]
   ```
3. Type the root password and then press Enter when prompted to do so.
4. Type the following command and then press Enter to create a directory for mounting the CD.
   ```
   mkdir -p /media/cdrom
   ```
5. Insert the PKES application CD into the CD drive of the PKES.
6. Type the following command and then press Enter to mount the CD. The /dev/cdrom is write-protected; mounting read-only message appears.
   ```
   mount /dev/cdrom /media/cdrom
   ```
7. Type the following command and then press Enter.
   ```
   cd /media/cdrom
   ```
8. Type the following command and then press Enter. The system installs the application software and reboots.
   ```
   ./install
   ```
9. Log in as root using the default password. A message prompts you to change the password.
10. Type a new password and press Enter. A message prompts you to confirm the new password.
11. Type the new password and press Enter to confirm the new password.
12 Type the following command and then press **Enter** to obtain the current version of the PKES application software.

`rpm -qi SAIpkes`

**Example:** The following example illustrates Version 1.2.0.11 of the PKES application software:

```
Name        : SAIpkes              Relocations: (not relocatable)
Version     : 1.2.0.11             Vendor: Cisco Systems, Inc.
Release     : 1       Build Date: Thu 21 Jul 2011 01:48:20 PM EDT
Install Date: Wed 27 Apr 2011 03:28:27 AM EDT   Build Host: happy
Group       : System Environment/Base Source RPM: SAIpkes-1.2.0.11-1.src.rpm
Size        : 919423                        License: Proprietary
Signature   : (none)
Packager    : SPVTG
Summary     : SAI PKES Application
Description :
The PKES is responsible for taking clear VOD content in the form of an MPEG file and producing an encrypted version of the file. The PKES is controlled through a web services interface that triggers the transfer of the asset to the PKES, the encryption of the asset, and the transfer back to the source machine.
```

13 Did the output display the expected PKES application version?

- If **yes**, continue with the next procedure in this chapter.
- If **no**, contact Cisco Services TAC for assistance.
Configure the PKES Application

Configuring the PKES Software

Follow these instructions to configure the PKES application.

1. At the ISDS directory used in steps 2 and 3 of Configuring the VOD MSK on the ISDS (on page 22), type the following command and press Enter.
   `scp vodMskPkes root@[PKES MGMT IP address]:/usr/local/pkes/bin/vodMskPkes`
   *Note:* The vodMskPkes file pertains to the file specified in step 10 of Creating the VOD MSK on the TED (on page 20).

2. At the password prompt, type the root password.

3. Type the following command and then press Enter. The password prompt appears.
   `ssh root@[PKES MGMT IP address]`

4. Type the root password and then press Enter.

5. Type the following command and then press Enter. The /usr/local/pkes/bin directory becomes the working directory.
   `cd /usr/local/pkes/bin`

6. Type the following command and then press Enter. The system prompts for the path to the vodMskPkes file.
   `./provisionMsk`

7. Type the following command and then press Enter. The system prompts for the pass phrase you created in step 8 of Creating the VOD MSK on the TED (on page 20).
   `/usr/local/pkes/bin/vodMskPkes`
   *Note:* The vodMskPkes file pertains to the file specified in step 10 of Creating the VOD MSK on the TED (on page 20).

8. Type the VOD pass phrase and then press Enter.

Editing the pkesConfiguration File

1. Type the following command and press Enter. The /usr/local/pkes/config directory becomes the working directory.
   `cd /usr/local/pkes/config`

2. Type the following command and then press Enter to open the pkesConfiguration file for editing.
vi pkesConfiguration
Configure the PKES Application

3 Edit the pkesConfiguration file to set the following values.

Example: Refer to Sample pkesConfiguration File (on page 29) for an example of what the file might look like.

- PKES IP address
- AMS IP address
- Encryption mode to be applied to VOD content
- Crypto period hint delay (in seconds)
- Crypto period ECM construction delay (in seconds)
- Crypto period control word activation delay (in seconds)
- AMS FTP user name to enable file transfers
- AMS FTP password to enable file transfers
- Encryption interrupt rate (determines the number of packets the PKES processes between checking for a query or a cancel command from the AMS)
- Assumed transfer rate in bytes per second (this number is used to estimate the time remaining for the current encryption)
- MSK parity (odd or even)
- Retain error file setting (determines whether or not VOD content should be retained following an error for debugging purposes)
- DRM override mode (enable or disable)
- DRM override setting
- PKES timeout value (determines the time that the PKES waits to timeout an incoming query or cancel command before generating an error)

4 Save the file and close the vi editor.

5 Type the following command and then press Enter.

```
service pkesd restart
```

Sample pkesConfiguration File

An example of a pkesConfiguration file follows:

```
#

# PKES Configuration File
# IP Address of the PKES
PKES_IP_ADDRESS = 10.90.46.1
# IP Address of the AMS
```
AMS_IP_ADDRESS = 10.90.46.2

# Core Encryption Mode
# Encryption mode specified by the following index values:
#       0 - PowerKEY native
#       1 - DVB CSA
#       6 - AES NSA 2
#       7 - ATIS_IIF_DSA
#
ENCRIPTION_MODE = 1
# Crypto period - length of delay in seconds after setting hint bit
# Default value: 2
# Minimum value: 1
CRYPTO_PERIOD_HINT_DELAY = 2
# Crypto period - length of delay in seconds after constructing the ECM
# Default value: 1
# Minimum value: 1
CRYPTO_PERIOD_CONSTRUCT_ECM_DELAY = 1
# Crypto period - length of delay in seconds after activating control word
# Default value: 5
# Minimum value: 2
CRYPTO_PERIOD_ACTIVATE_CW_DELAY = 5
# FTP account user name
FTP_ACCOUNT_NAME = ftpUser
# FTP account password
FTP_ACCOUNT_PASSWORD = ftpPass
# Encryption interrupt rate
# This is the number of packets at which the encryption process is interrupted
# to check for a query or cancel command from the AMS
# Default value: 30000
INTERRUPT_RATE = 30000
# Encrypted packet threshold
# This is the threshold percentage of encrypted packets for an encryption to
# be successful. In other words, if the encryption of an asset is requested
# and the resulting file has less than the specified percentage of encrypted
# packets, the encryption will be considered a failure
#
# Default value: 50
ENCRYPTION_PERCENTAGE_THRESHOLD = 50

# DRM Override value
# This value is applied to every asset regardless of the AMS setting as
# long as the override is enabled
# The following values are valid:
#   0 - copying is permitted
#   1 - no further copying is permitted
#   2 - one generation copy is permitted
#   3 - copying is prohibited
#
DRM_OVERRIDE_VALUE = 3

# DRV Override switch
# This switch enables/disables the DRM override setting. When the override
# is enabled, the setting specified by DRM_OVERRIDE_VALUE will replace
# the DRM setting for each asset received from the AMS
#
# Options include:
#   Yes
#   No
# Default value: No
ENABLE_DRM_OVERRIDE = No
# Assumed encryption rate

#
# This is the assumed number of packets processed in one second. This rate
# is used to estimate the remaining number of seconds to encrypt the
# current asset
#
ESTIMATED_ENCRYPTION_RATE = 80000
#
# Assumed file transfer rate
#
# This is the assumed rate at which files are transferred via FTP in bytes
# per second. This value is used to estimate the remaining time required
# to process an asset
#
ESTIMATED_TRANSFER_RATE = 3500000
#
# MSK switch
# This setting switches between the even/odd MSK
# Options include:
#   Even
#   Odd
# Default value: Even
MSK_PARITY = Even
#
# Retain content file setting
# This setting enables/disables the saving of a content file when an
# error occurs during the encryption process. The file is saved
# to a directory labeled with the eventSeqNum in the content/error area
# Options include:
#   Yes
#   No
#
RETAIN_ERROR_FILE = Yes
Configure the PKES Application

# PKES timeout value
#
# This setting determines the number of seconds the PKES waits before
# timing out a query or cancel command from the AMS. The timeout value
# is an integer that must be greater than zero.
#
PKES_TIMEOUT_VALUE = 300

Editing the syslog.conf File

Complete these instructions to edit the syslog.conf file.
1. At the PKES, type the following command and then press Enter. The /etc
directory becomes the working directory.
   cd /etc
2. Type the following command and then press Enter. The syslog.conf file opens for
   editing using the vi text editor.
   vi syslog.conf
3. Append the following lines, as shown, to the end of the syslog.conf file:
   # Saves pkes messages to pkes.log
   *.debug;kern.none;mail.none;authpriv.none;cron.none
   /var/log/pkes.log
4. Save the file and close the vi text editor.
5. Type the following command and then press Enter to restart the syslog process.
   service syslog restart
Configure SNMP on the PKES

Refer to *IBDS SNMP Administration Guide* (part number 4028434) for general SNMP information for PKES servers, as well as for instructions to configure the PKES servers for SNMP queries and notifications (traps).
Configure NTP on the PKES

Complete these instructions to configure NTP on the PKES.

1. At the PKES, type the following command and then press **Enter**. The /etc directory becomes the working directory.
   ```
   cd /etc
   ```

2. Open the ntp.conf file with a text editor.

3. Within the ntp.conf file, comment out the following lines by placing a `#` at the beginning of each line:
   ```
   #server 0.rhel.pool.ntp.org
   #server 1.rhel.pool.ntp.org
   #server 2.rhel.pool.ntp.org
   ```

4. After the last server entry, create a new entry containing the IP address for the NTP server to be used as the time source for the PKES.
   ```
   Example: `server 172.40.90.1`
   ```
   **Note:** The ISDS can be used as the time source for the PKES. If this is desired, use the ISDS dncsatm IP Address.

5. Save and close the file.

6. Type the following command and then press **Enter** to stop the NTP process.
   ```
   service ntpd stop
   ```

7. Type the following command and then press **Enter** to synchronize the time on the PKES to the time from the NTP server.
   ```
   ntpdate [NTP Server IP]
   Example: `ntpdate 172.40.90.1`
   ```

8. Repeat step 7 three times.

9. Type the following command and then press **Enter** to start the NTP process.
   ```
   service ntpd start
   ```
   **Note:** Allow up to 10 minutes for the NTP to fully synchronize its time with the NTP server.
10 Type the following command and then press **Enter** to check the synchronization status between the PKES NTP process and the NTP server.

```
ntpq -p
```

**Example:** Output should be similar to the following example:

```
remote     refid   st  t  when  poll  reach  delay  offset  jitter
*172.40.90.1  192.133.225.100  5  u  177  1024  377  0.420  9.695  4.578
LOCAL (0) .LOCL.  10  1  11   64  377  0.000  0.000  0.001
```

**Note:** When the PKES has synchronized with the NTP server, the NTP server will contain an asterisk at the beginning of the line, as displayed in the previous example.
Enable Support for Clear DRM VOD Assets (Optional)

Complete these instructions to implement support for clear DRM VOD assets.

1. On the PKES, type the following command and then press Enter. The pkesd file opens for editing in the vi text editor.
   `vi /etc/init.d/pkesd`

2. Add the following entry below the line that reads `PKES=pkes`.
   `export PKES_ENABLE_TSC_CLEAR=1`
   **Note:** The top portion of the pkesd file should look similar to the following example when you are finished:
   ```
   RETVAL=0
   prog="pkes"
   PKES_DIR=/usr/local/pkes/bin
   PKES=pkes
   export PKES_ENABLE_TSC_CLEAR=1
   ```

3. Save and close the pkesd file.
Restart the PKES Application

To restart the PKES application, as root user, type the following command and then press Enter:

```
service pkesd restart
```
Introduction

Use the procedures in this chapter to upgrade and configure the PKES platform and/or application software.

Important: If you are installing and configuring the PKES software for the first time, do not complete the procedures in this chapter. Complete the procedures in Chapters 1 through 4, instead.

In This Chapter

- Upgrade the PKES Software.......................................................... 44
Upgrade the PKES Software

Complete the procedures in this section for each PKES server to be upgraded.

**Important:** Note these important points:

- A keyboard and monitor must be connected to the PKES server before beginning the upgrade of the PKES platform software.
- The PKES MSK file is required to complete the upgrade of the PKES platform software. This file should be onsite prior to beginning these upgrade procedures.

Determining the PKES Platform Software Version

Before you begin, obtain the expected platform version of the PKES from your Cisco account manager. Then, complete the following steps to determine the current PKES platform software version.

1. From an xterm window on the ISDS, type the following command and then press Enter.
   ```
   ssh root@[PKES MGMT IP address]
   ```
   **Note:** Substitute the MGMT IP address of the PKES server for [PKES MGMT IP address].
   **Important:** The root password is not included in these procedures. If you need the root password, contact Cisco Services.

2. Type the following command and then press Enter to obtain the current version of the PKES platform software.

```
rpm -qi SAIlxplat
```

**Example:** The following example illustrates Version 1.0.4 of the PKES platform software.

<table>
<thead>
<tr>
<th>Name</th>
<th>SAIlxplat</th>
<th>Relocations: not relocatable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0.4</td>
<td>Vendor: Cisco Systems, Inc.</td>
</tr>
<tr>
<td>Release</td>
<td>1</td>
<td>Build Date: Tue 12 May 2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10:32:21 AM EDT</td>
</tr>
<tr>
<td>Install Date</td>
<td>Tue 16 Jun 2009</td>
<td></td>
</tr>
<tr>
<td></td>
<td>04:30:53 AM EDT</td>
<td></td>
</tr>
<tr>
<td>Build Host</td>
<td>sausat1pcg01.dvsg.sciatl.com</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>System</td>
<td>Source RPM: SAIlxplat-1.0.4-1.src.rpm</td>
</tr>
<tr>
<td></td>
<td>Environment/Base</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>0</td>
<td>License: Proprietary</td>
</tr>
<tr>
<td>Signature</td>
<td>(none)</td>
<td>Packager: SPVTG</td>
</tr>
</tbody>
</table>
Summary
SAI Linux Platform Package (RHEL 5.1)

Description
The base platform for Linux based products. This rpm is used to track the platform release version.

Backing Up the PKES Configuration

1. From an xterm window on the ISDS, type `su - dncs` and then press Enter to log on as the dncs role.

2. When prompted, type the password for the dncs role and then press Enter.

3. Type the following command and then press Enter to create a directory which will be used to back up the current PKES server configuration.
   ```bash
   mkdir /export/home/dncs/pkes-[PKES-Name or IP]-backup-[YYYYMMDD]
   ```
   Note: Substitute the current date for [YYYYMMDD].
   Example: `mkdir /export/home/dncs/pkes-172.105.1.173-backup-20090819`

4. Type the following command and then press Enter.
   ```bash
   cd /export/home/dncs/pkes-backup-[YYYYMMDD]
   ```

5. Type the following commands to back up the current PKES server configuration.

   Important:
   - In each of the following commands, a space precedes a period at the end of the command.
   - For each of the following commands, when presented with the password prompt, type the password for the root user on the PKES.
   
   ```bash
   a scp root@[PKES MGMT IP address]:/etc/hosts . and then press Enter.
   b scp root@[PKES MGMT IP address]:/etc/syslog.conf . and then press Enter.
   c scp root@[PKES MGMT IP address]:/etc/sysconfig/network . and then press Enter.
   d scp root@[PKES MGMT IP address]:/etc/sysconfig/network-scripts/ifcfg-eth0 . and then press Enter.
   e scp root@[PKES MGMT IP address]:/etc/sysconfig/network-scripts/ifcfg-eth1 . and then press Enter.
   f scp root@[PKES MGMT IP address]:/etc/sysconfig/network-scripts/route-eth0 . and then press Enter.
   g scp root@[PKES MGMT IP address]:/etc/sysconfig/network-scripts/route-eth1 . and then press Enter.
   ```
scripts/route-eth1 . and then press Enter.

h scp root@[PKES MGMT IP address]:/usr/local/pkes/config/pkesConfiguration . and then press Enter.

i scp root@[PKES MGMT IP address]:/usr/local/pkes/config/trapDestinationTable . and then press Enter.
Upgrade the PKES Software

**j**  scp root@[PKES MGMT IP address]:/usr/share/snmp/snmpd.conf . and then press Enter.

**k**  scp root@[PKES MGMT IP address]:/etc/ntp.conf . and then press Enter to back up the NTP configuration file.

6  Record the following information for later use:

- PKES MGMT IP address:  ____________________
- PKES MGMT Subnet Mask:  ____________________
- PKES Default Gateway:  ____________________

7  Did the PKES server have the desired platform software version, as determined in *Determining the PKES Platform Software Version* (on page 44)?

- If **yes**, skip to *Upgrading the PKES Application Software* (on page 48).
- If **no**, continue with *Upgrading the PKES Platform Software* (on page 47).

---

**Upgrading the PKES Platform Software**

1  From the attached keyboard and monitor, log on to the PKES server as **root** user.

2  Type the following command and then press Enter to reboot the PKES server.

```
shutdown  -y  -g0  -i6
```

3  Once the server has begun the reboot process, press the CD/DVD eject button to the drive on the server.

4  Insert the PKES platform CD into the drive tray and close the tray. After a few minutes, the Cisco screen appears. Type **platform** and then press Enter. The PKES runs an automated installation script and the following warning message may appear:

```
The partition table on the device sda was unreadable ... Would you like to initialize this drive, erasing ALL DATA?
```

5  Type **y** and then press Enter. The installation script continues.

**Notes:** Note these important points about the installation process.

- The installation script should complete within 15 minutes.
- The system automatically ejects the CD upon completion.
- The system automatically reboots.

6  From the attached keyboard and monitor, log on to the PKES server as **root** user.
Chapter 5  PKES Upgrade Procedures

7 Type the following command and then press **Enter** to obtain the current version of the PKES platform software.

```
rpm -qi SAIxlxplat
```

**Example:** The following example illustrates Version 1.0.4 of the PKES platform software.

<table>
<thead>
<tr>
<th>Name</th>
<th>SAIxlxplat</th>
<th>Relocations: not relocatable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0.4</td>
<td>Vendor: Cisco Systems, Inc.</td>
</tr>
<tr>
<td>Release</td>
<td>1</td>
<td>Build Date: Tue 12 May 2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10:32:21 AM EDT</td>
</tr>
<tr>
<td>Install Date</td>
<td>Tue 16 Jun 2009</td>
<td>Build Host: sausatlpcg01.dvsg.sciatl.com</td>
</tr>
<tr>
<td>Group</td>
<td>System</td>
<td>Source RPM: SAIxlxplat-1.0.4-1.src.rpm</td>
</tr>
<tr>
<td></td>
<td>Environment/Base</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>0</td>
<td>License: Proprietary</td>
</tr>
<tr>
<td>Signature</td>
<td>(none)</td>
<td></td>
</tr>
<tr>
<td>Packager</td>
<td>SPVTG</td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>SAI Linux Platform Package (RHEL 5.1)</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>The base platform for Linux based products. This rpm is used to track the platform release version.</td>
<td></td>
</tr>
</tbody>
</table>

8 Go to *Upgrading the PKES Application Software* (on page 48).

---

**Upgrading the PKES Application Software**

1 Did you just complete an upgrade of the PKES platform software?

- If **yes**, continue with step 2.
- If **no**, skip to step 4.

2 From the attached keyboard and monitor, login to the PKES server as **root** user.

3 Follow these directions to create a directory for mounting the PKES application CD.

   a Type the following command and then press **Enter**.

   ```
   mkdir -p /media/cdrom
   ```

   b Skip to step 7.
4 Is the SSH connection to the PKES still established from step 1 of *Determining the PKES Platform Software Version* (on page 44)?

- If **yes**, continue with step 5.
- If **no**, from an xterm window on the ISDS, type the following command and then press *Enter*.
  
  ```
  ssh root@[PKES MGMT IP]
  ```

Notes:

- Substitute the MGMT IP address of the PKES server for [PKES MGMT IP].
- When presented with the **password** prompt, type the password for the *root* user of the PKES server.

5 Type the following command and then press *Enter* to stop the PKES application.

   ```
   service pkesd stop
   ```

6 Type the following command and press *Enter* to stop SNMP.

   ```
   service snmpd stop
   ```

7 Insert the PKES application CD into the CD drive of the PKES server.

8 Type the following command and then press *Enter* to mount the CD.

   ```
   mount /dev/cdrom /media/cdrom
   ```

9 Type the following command and then press *Enter*.

   ```
   cd /media/cdrom
   ```

10 Type the following command and then press *Enter* to upgrade the PKES application software.

   ```
   ./install -U
   ```

11 When the PKES application software has finished installing, the PKES will automatically reboot and eject the CD. When the CD ejects, remove it from the drive and close the drive.

12 When the PKES reboots, the SSH connection is lost. A few minutes after the automatic reboot, the PKES will again be accessible. From an xterm window on the ISDS, type the following command and then press *Enter*.

   ```
   ssh root@[PKES MGMT IP]
   ```

Notes:

- Substitute the MGMT IP address of the PKES server for [PKES MGMT IP].
- When presented with the password prompt, type the password for the *root* user of the PKES server and press *Enter*.

13 Check the log file for errors. The log file is

   ```
   /var/sadm/system/logs/INST_R_SAIpkes.log
   ```
14 Type the following command and then press Enter to obtain the current version of the PKES application software.

    rpm -qi SAIpktes

Example: The following example illustrates Version 1.2.0.11 of the PKES application software:

    Name        : SAIpktes                      Relocations: (not relocatable)
    Version     : 1.2.0.11                     Vendor: Cisco Systems, Inc.
    Release     : 1                            Build Date: Thu 21 Jul 2011 01:48:20 PM EDT
    Install Date: Wed 27 Apr 2011 03:28:27 AM EDT      Build Host: happy
    Group       : System Environment/Base       Source RPM: SAIpktes-1.2.0.11-1.src.rpm
    Size        : 919423                           License: Proprietary
    Signature   : (none)
    Packager    : SPVTG
    Summary     : SAI PKES Application
    Description :
    The PKES is responsible for taking clear VOD content in the form of an MPEG file and producing an encrypted version of the file. The PKES is controlled through a web services interface that triggers the transfer of the asset to the PKES, the encryption of the asset, and the transfer back to the source machine.

15 Did the output display the expected PKES application version?
   - If yes, continue with step 16.
   - If no, call Cisco Services for assistance.

16 Did you previously upgrade the PKES platform software (in Upgrading the PKES Platform Software (on page 47))?  
   - If yes, continue with Restoring the PKES Platform Configuration Files (on page 51).
   - If no, skip to Restoring the PKES Application Configuration Files (on page 55).

Restoring the PKES Platform Configuration Files

1 Reference the information from step 6 of Backing Up the PKES Configuration (on page 45), to temporarily configure the PKES MGMT network interface to allow the PKES platform configuration files to be restored.

   Note: You will temporarily configure the PKES MGMT network interface in the next few steps.

2 On the PKES, type the following command and then press Enter. The
/etc/sysconfig/network-scripts becomes the working directory.

cd  /etc/sysconfig/network-scripts
3 Type the following command and then press Enter. The ifcfg-eth1 file opens for editing using the vi text editor.
   vi  ifcfg-eth1

4 Update the ifcfg-eth1 file with the following information:
   - IPADDR=[PKES MGMT IP address]
   - NETMASK=[PKES MGMT Subnet Mask]
   Note: For both of these values, reference the PKES MGMT IP address and the PKES MGMT Subnet Mask you recorded in step 6 of Backing Up the PKES Configuration (on page 45).

5 Save and close the ifcfg-eth1 file.

6 Type the following command and then press Enter. The route-eth1 file opens for editing using the vi text editor.
   vi  route-eth1

7 Update the route-eth1 file with the following information:
   - GATEWAY0=[PKES Default Gateway]
   - NETMASK0=0.0.0.0
   - ADDRESS0=0.0.0.0
   Note: For the GATEWAY0 value, reference the PKES Default Gateway you recorded in step 6 of Backing Up the PKES Configuration (on page 45).

8 Save and close the route-eth1 file.

9 Type the following command and then press Enter.
   service network restart

10 From the PKES, type the following command and then press Enter to verify network communications.
   ping  [ISDS_IP]

11 Was the response from the ping command successful?
   - If yes, continue with step 12.
   - If no, contact Cisco Services for assistance.

12 From an xterm window on the ISDS, type the following command and then press Enter to log on in the dncs role.
   su - dncs

13 Type the following command and then press Enter to navigate to the directory in which you backed up the PKES configuration.
   cd  /export/home/dncs/pkes-[PKES-Name or IP]-backup-[YYYYMMDD]
   Note: This is the directory created in step 3 of Backing Up the PKES Configuration (on page 45).
14 Type the following commands to restore the platform configuration files. **Important:** For each of the following commands, when presented with the **password** prompt, enter the password for the root user on the PKES.

a. `scp hosts root@[PKES MGMT IP]:/etc/hosts` and then press **Enter**.

b. `scp syslog.conf root@[PKES MGMT IP]:/etc/syslog.conf` and then press **Enter**.

c. `scp network root@[PKES MGMT IP]:/etc/sysconfig/network` and then press **Enter**.

d. `scp ifcfg-eth0 root@[PKES MGMT IP]:/etc/sysconfig/network-scripts/ifcfg-eth0` and then press **Enter**.

e. `scp ifcfg-eth1 root@[PKES MGMT IP]:/etc/sysconfig/network-scripts/ifcfg-eth1` and then press **Enter**.

f. `scp route-eth0 root@[PKES MGMT IP]:/etc/sysconfig/network-scripts/route-eth0` and then press **Enter**.

g. `scp route-eth1 root@[PKES MGMT IP]:/etc/sysconfig/network-scripts/route-eth1` and then press **Enter**.

h. `scp ntp.conf root@[PKES MGMT IP]:/etc/ntp.conf` and then press **Enter** to restore the NTP configuration file.

15 Go to *Restoring the PKES Application Configuration Files* (on page 55).

**Restoring the PKES Application Configuration Files**

1 From an xterm window on the ISDS, type the following command and press **Enter** to log on as the dncs role.

   `su - dncs`

2 Type the following command and press **Enter** to navigate to the directory in which you backed up the PKES configuration.

   `cd /export/home/dncs/pkes-[PKES-Name or IP]-backup-[YYYYMMDD]`

   **Note:** This is the directory created in step 3 of *Backing Up the PKES Configuration* (on page 45).

3 Type the following commands and then press **Enter** to restore the PKES application configuration files. **Important:** For each of the following commands, when presented with the **password** prompt, enter the password for the root user on the PKES.

a. `scp pkesConfiguration root@[PKES MGMT IP]:/usr/local/pkes/config/pkesConfiguration`

b. `scp snmpd.conf root@[PKES MGMT IP]:/etc/snmpd.conf`
IP]/usr/share/snmp/snmpd.conf.orig
Restoring the PKES SNMP Configuration

Complete these procedures to restore the PKES SNMP Configuration.

Checking the PKES Trap Destinations
1. From an xterm window on the ISDS, type the following command and press Enter. The password prompt appears.
   
   ```
   ssh root@[PKES MGMT IP]
   ```

   **Note:** Substitute the MGMT IP address of the PKES for [PKES MGMT IP].

2. Type the root password and press Enter.

3. Type the following command and press Enter.
   
   ```
   cd /usr/share/snmp
   ```

4. Type the following command and press Enter. The system displays the original platform trap destination entries.
   
   ```
   grep trapsess snmpd.conf.orig
   ```

   **Example:**
   
   ```
   trapsess -v 2c -c trapcomm 172.40.90.1:162
   trapsess -e 0x80001f88800ed913fddbb5774800000000 -v 3 -u myuser -a MD5-A mypassword -l authNoPriv 172.40.90.1:162
   ```

5. Were any trap destinations displayed in the output from step 4?
   - If yes, go to step 6.
   - If no, you are finished with this procedure; go to the next procedure in this section.

6. Type the following command and press Enter.
   
   ```
   vi snmpd.conf
   ```

7. Add all of the original trap destinations to the end of the snmpd.conf file.

8. Did any of the original trap destinations include `-v 3` which indicates the trap destination is SNMPv3?
   - If yes, follow these instructions to verify the engine ID.
     a. As root user in another xterm window on the PKES, type the following command and press Enter. SNMP configuration data, including the hexadecimal engine ID, appears.

     ```
     grep usmUser /var/net-snmp/snmpd.conf
     ```

     **Note:** The first hexadecimal number after usmUser in the second entry returned in the results from step a is the SNMPv3 engine ID.

     **Example:**
     
     ```
     0x80001f88800ed913fddbb5774800000000
     ```

     b. Does the engine ID displayed in step 8a match the engine ID of the
original SNMPv3 trap destination?
  ▪ If yes, go to step 8c.
  ▪ If no, then update the SNMPv3 trap destination engine ID with the engine ID found in step 8a.
  c Save and close the snmpd.conf file.

Checking the SNMP Communities
1 From the SSH session connected to the PKES, as root user, type the following command and press Enter. The system displays all of the original SNMPv2 communities configured on the PKES.
  
  grep rocommunity  snmpd.conf.orig
2 Did the system display any un-commented values other than the following:
  rocommunity  public localhost
  rocommunity  public 192.168.44.60
  ▪ If yes, go to step 3.
  ▪ If no, go to Restarting the SNMP Daemon (on page 58).
3 Complete the following steps to restore the SNMPv2 communities on the PKES.
  a Type the following command and press Enter.
    vi snmpd.conf
  b Add all of the original SNMPv2 community entries to the end of the snmpd.conf file.
    Important: Do not add the following entries:
    rocommunity  public localhost
    rocommunity  public 192.168.44.60
  c Save and close the snmpd.conf file.

Restarting the SNMP Daemon
1 Did you make any changes to either the snmpd.conf file or the trapDestinationTable file?
  ▪ If yes, follow these steps to restart the Net-SNMP daemon.
    a Type the following command and press Enter.
      service snmpd stop
    b Type and press Enter.
      service snmpd start
    c Type the following command and press Enter to verify that the Net-SNMP daemon started.
      service snmpd status
    Example: Output should look similar to the following:
snmpd (pid 6895) is running...

- If no, go to *Enable Support for Clear DRM VOD Assets (Optional)* (on page 48).

2 Type **exit** and then press **Enter** to log out of the PKES as root user.
Enable Support for Clear DRM VOD Assets (Optional)

Complete these instructions only if you require support for clear DRM VOD assets.

1. On the PKES, type the following command and then press Enter. The pkesd file opens for editing in the vi text editor.
   
   ```
   vi /etc/init.d/pkesd
   ```

2. Add the following entry below the line that reads PKES=pkes
   ```
   export PKES_ENABLE_TSC_CLEAR=1
   ```
   Note: The top portion of the pkesd file should look similar to the following example when you are finished:
   ```
   RETVAL=0
   prog="pkes"
   PKES_DIR=/usr/local/pkes/bin
   PKES=pkes
   export PKES_ENABLE_TSC_CLEAR=1
   ```

3. Save and close the pkesd file.

Restarting the PKES Application

To restart the PKES application, as root user, type the following command and then press Enter.
```
service pkesd restart
```
path to the vodMskPkes file.

)./provisionMsK
Chapter 5 PKES Upgrade Procedures

8 Type the following command and then press **Enter**. The system prompts for the pass phrase you created in step 8 of *Creating the VOD MSK on the TED* (on page 20).

```
/usr/local/pkes/bin/vodMskPkes
```

**Note:** The vodMskPkes file pertains to the file specified in step 10 of *Creating the VOD MSK on the TED* (on page 20).

9 Type the VOD pass phrase and then press **Enter**.

10 Type the following command and then press **Enter** to restart the PKES and to activate these changes.

```
service pkesd restart
```

11 Complete the *Configure SNMP on the PKES* (on page 38) procedure.

12 Continue with *Verifying the PKES Upgrade* (on page 62).

**Verifying the PKES Upgrade**

1 From an xterm window on the ISDS, type the following command and press **Enter**. The password prompt appears.

```
ssh root@[PKES MGMT IP]
```

2 Type the root password and press **Enter**.

3 Type the following command and press **Enter** to verify communications between the AMS and the PKES.

```
ping [AMS_IP]
```

4 Was the response to the ping command successful?

- If **yes**, continue with step 5.
- If **no**, call Cisco Services.

5 From the AMS-PKES, navigate to the list of encryption delegates and verify that the upgraded PKES is in an online state. If not, set it to online.

6 Take note of the total number of online PKES devices.

7 From the OpenETF Pre-Processor, export a series of packages to the AMS-PKES, one package for each online PKES.

8 Monitor the package ingest on the AMS-PKES.

9 Verify that the ingested packages display a state of **encrypting** while the PKES servers are encrypting the assets and a state of **encrypted** once the PKES servers have completed encrypting the assets.
Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.
Troubleshooting the PKES

In This Appendix

- Verify CAS Manager Delegates Online ............................................. 68
- Low Disk Space ................................................................................. 67
- Manage PKES Log File..................................................................... 70
- Assets Processing Slowly................................................................. 71

Introduction

Refer to this appendix for assistance in troubleshooting the PKES.
Verify CAS Manager Delegates Online

Assets will fail to process if a required AMS CAS Manager delegate is offline. Follow these steps to check the status of delegates and, if necessary, change the state.

**Note:** Complete these steps on the Ericsson AMS.

1. From a web browser, log on to the Ericsson AMF that interacts with the PKES.
2. Click the **AMS** module on the Admin page.
3. Click the **CAS Manager** menu option and select **CAS managers** from the pull-down list.
4. Click the name link of the CAS Manager you wish to verify.

**Result:** The **Delegate Id** and **State** for the encryption delegates are displayed.

5. Is a delegate offline that should be online?
   - If **yes**, follow these instructions.
     a. Click the checkbox next to the delegate that is offline.
     b. Click **Active**. The state changes to **Available**.
     c. Go to step 6.
   - If **no**, continue with step 6.

6. Repeat this procedure for other delegates and CAS Managers.
Low Disk Space

After an ftp download error, the PKES clears directories of stale assets. Should the assets fail to clear properly, the disk space on the server could eventually be consumed, depending upon the size of the assets being downloaded when the ftp download error occurred.

Complete these steps to check the file system space on the PKES.

1. Use the SSH (secure shell) protocol to log on to the PKES.
2. Type the following command and press Enter.
   
   
   ```
   df -k
   ```
   
   Sample output:
   ```
   [root@JK-PKES1 ~]# df -k
   Filesystem  1K-blocks  Used  Available  Use% Mounted on
   /dev/sda1  135566544  5236436  123332600    5%  /
   tmpfs  4081248  0  4081248    0%  /dev/shm
   ```

3. Is the Use% value greater than 30 percent for the `/dev/sda1` filesystem?
   - If yes, follow these instructions.
     a. Type the following command and press Enter to stop the PKES.
      ```
      service pkesd stop
      ```
   
     b. Type the following command and press Enter.
      ```
      cd /usr/local/pkes/content/current/clear
      ```
   
     c. Type the following command and press Enter to remove the files.
      ```
      rm *
      ```
   
     d. Type the following command and press Enter.
      ```
      cd /usr/local/pkes/content/current/error
      ```
   
     e. Type the following command and press Enter to remove the files.
      ```
      rm *
      ```
   
     f. Type the following command and press Enter to restart the PKES.
      ```
      service pkesd start
      ```
   
     g. Verify that the AMS CAS delegates are online. Go to Verify CAS Manager Delegates Online (on page 66) to perform this verification.
      
      **Important:** Whenever the PKES process is restarted, it is good practice to verify that the AMS CAS delegates remain online.
   - If no, you do not have low disk space. Log out of the PKES.
Manage PKES Log File

Log files can sometimes grow too large for easy reference. If you think your PKES log file has grown too large, you can archive it and start a new log file. Use these instructions to start a new log file.

1. Type the following command and press Enter to stop the PKES.
   ```
   service pkesd stop
   ```
2. Type the following command and press Enter to change to the directory containing the log file.
   ```
   cd /var/log
   ```
3. Type the following command and press Enter to archive and compress the existing PKES log file.
   ```
   tar -czvf pkeslog<date>.tar.gz pkes.log
   ```
4. Type the following command and press Enter to delete the existing PKES log file.
   ```
   rm pkes.log
   ```
5. Type the following command and press Enter to stop and restart the syslog process, which initiates the creation of a new PKES log file.
   ```
   service syslog restart
   ```
6. Type the following command and press Enter to restart the PKES.
   ```
   service pkesd start
   ```
7. Verify that the AMS CAS delegates are online. Go to Verify CAS Manager Delegates Online (on page 66) to perform this verification.

**Important:** Whenever the PKES process is restarted, it is good practice to verify that the AMS CAS delegates remain online.
**Assets Processing Slowly**

If the PKES appears to be processing assets too slowly, verify the activity in the `/var/log/pkes.log` file. A typical high-definition asset is approximately 10 GB and should take about 5 minutes or less to download to the PKES via FTP, assuming that network traffic is running at 1,000 Mb/s.

Examine the sample log file that follows. This sample shows the processing time of the PKES. Pertinent information in this example has been made bold to help clarify what is occurring. An actual log file would contain additional lines that have been removed here to simplify the example.

This example depicts a 10 GB asset, 5 minutes download time, 29 minutes encrypting time, and 4 minutes upload time.

download

May 18 21:13:11 PKES52 pkes: FTP download thread received command to download file from AMS

### Start of download ###

May 18 21:13:11 PKES52 pkes: - Event seq number: 277819
May 18 21:13:11 PKES52 pkes: - Provider ID: TVN.com
May 18 21:13:11 PKES52 pkes: - Asset ID: TVNX0008654301064012
May 18 21:13:11 PKES52 pkes: - Asset Title: Titan_A_E___HD_A1OXF_movie
May 18 21:13:11 PKES52 pkes: - Action verb: 2, Encrypt


### Completion of download ###
encrypt

May 18 21:18:17 PKES52 pkes: _initFileAccess - Initializing input file
../content/current/clear/Titan_AE_HD_05242011_CAN_movie_0E9C2F32

May 18 21:18:17 PKES52 pkes: _initFileAccess - Initializing output file
../content/current/encrypted/Titan_AE_HD_05242011_CAN_movie_0E9C2F32_pkes

May 18 21:18:17 PKES52 pkes: Input file size: 10708191232 and packet number: 56958464
### Convert bytes to GB. 10708191232 bytes = 9.97GB ###


upload

May 18 21:46:54 PKES52 pkes: FTP upload thread received command to upload file
### Start of upload ###

May 18 21:46:54 PKES52 pkes: Preparing to upload file
../content/current/encrypted/Titan_AE_HD_05242011_CAN_movie_0E9C2F32_pkes

### Completion of upload ###