Enabling Session-Based Encryption for VOD Services

System Release 2.5/3.5/4.0 and Later

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. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.
- CableCARD, M-Card, and OpenCable are trademarks of Cable Television Laboratories, Inc.
- 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. (1009R)

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 v

Chapter 1 Before You Activate SBE 1

Verify that the DIS Flag is Enabled 2
Check Available Database Space 7
Verify the SBE License Option is Enabled 9

Chapter 2 Activate SBE and Verify Activation 11

Activating SBE 12
Verifying SBE License Activation 13

Chapter 3 Customer Information 17

About This Guide

Introduction

Video-On-Demand (VOD) is an interactive, session-based application that provides video services to subscribers. Session-Based Encryption (SBE) provides an added degree of security for VOD content and prevents QAM tuner-equipped televisions from viewing unpurchased VOD content.

Note: Contact the representative who handles your account for information about purchasing the optional SBE software product for your system.

Purpose

This document provides instructions for setting up SBE on systems using System Release (SR) 2.5/3.5/4.0 and later.

Audience

These instructions are written for DBDS system operators, system administrators of the DNCS, and field technicians responsible for setting up the SBE option.

Document Version

This is the second release of this document.

1

Before You Activate SBE

Introduction

This chapter details the procedures that must be completed before you set up SBE on your system.

In This Chapter

- Verify that the DIS Flag is Enabled 2
- Check Available Database Space 7
- Verify the SBE License Option is Enabled 9

Verify that the DIS Flag is Enabled

Overview

Your system DHCTs must receive the DIS enable flag on each transaction from the billing system in order for SBE to be activated. The two tests in this section will verify whether the Billing department is enabling the DIS flag on transactions sent to the DNCS.

CAUTION:

If you have a Separable Security CableCARD (SSC) set-top box, once the SSC set-top is licensed, you will:

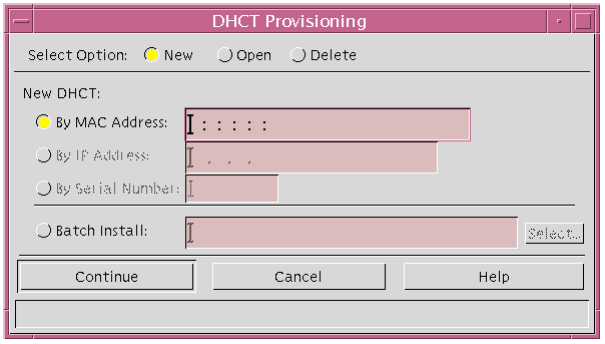
- Stage it normally **without** the DIS flag enabled.
- After the set-top box is staged and bound, have billing enable DIS by sending a hit to the set-top box.

Check Test Group DHCTs

Before you contact your billing provider, we recommend that you select three DHCTs for a test group. If the DIS flag is set, disable the DIS enable flag for each DHCT in that test group. After disabling the DHCT DIS flag from the DNCS, you must contact your billing provider and ask them to set the DIS flag to Enable.

Complete the following steps to perform Test One on three DHCTs.

1. Select three DHCTs for your test group.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click one of the following tabs:
   - If you are using SR 4.2 and later, click **Home Element Provisioning**.
   - If you are using SR 4.0 and earlier, click **Element Provisioning**.
4. Click **DHCT.** The DHCT Provisioning window appears.



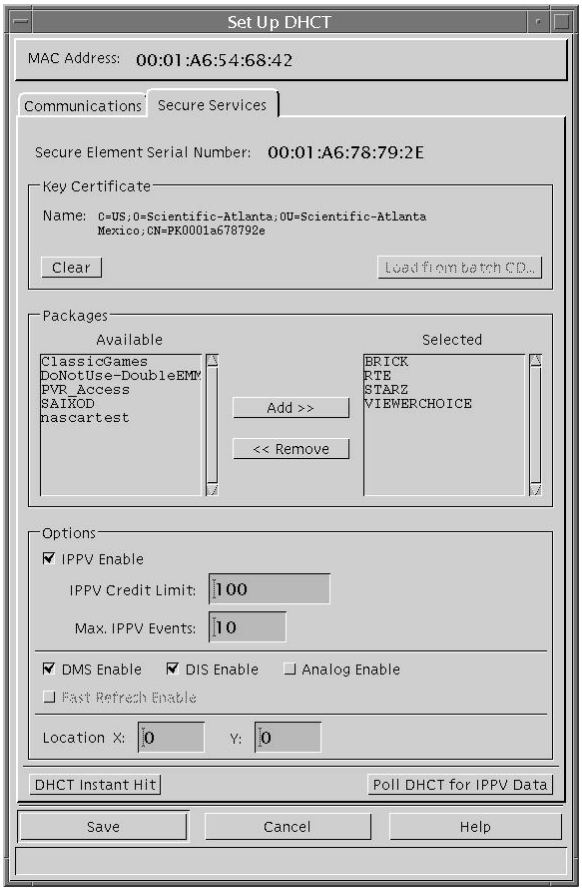
5 In the Select Option area, click the **Open** option if it is not already selected.

6 Do you know the MAC address for the DHCT you want to check?

- If **yes,** click the **By MAC Address** option, then click in the corresponding field, and type the MAC address for the DHCT you want to check. Go to step 7.
- If **no,** click the **By Serial Number** option, then click in the corresponding field, and type the serial number for the DHCT you want to check. Go to step 7.

7 Click **Continue.** The Set Up DHCT window opens for the DHCT you want to check.

8 Click the **Secure Services** tab.



9 Does a check mark appear in the DIS Enable field?

- If **yes,** click the **DIS Enable** option to turn the DIS enable flag off, then click **Save.** Go to step 10.
- If **no,** then the DIS Enable option is already off. Click **Cancel** to exit the Secure Services tab, then go to step 10.

10 Repeat steps 4 through 9 on the other two DHCTs in your test group to ensure that the DIS Enable flag is turned off.

11 Contact your billing provider and ask them to enable the DIS flag on billing transactions being sent to the DNCS.

12 After billing enables the DIS flag on transactions, repeat steps 2 through 8 on a test group DHCT to verify that billing has enabled the DIS flag.

13 Does a check mark appear in the DIS Enable field?

- If **yes**, then the billing system is setting the DIS enable flag.
- If **no**, you *must* contact your billing provider to have them enable the DIS flag on billing transactions being sent to the DNCS.

14 Repeat steps 12 and 13 on the other two DHCTs in your test group to verify that the DIS Enable flag is being set.

15 Click **Cancel** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16 Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

Check Recently-Staged DHCTs

After you verify that your billing provider is enabling the DIS flag on billing transactions to the DNCS, test a few recently-staged DHCTs to ensure that the DIS Enable flag is being received.

Special Case: SSC CableCARD Set-Top Boxes

Setting the DIS flag to **enabled** when loading SSC set-top boxes will cause binding and staging problems. Instead, stage them without special flags enabled, enable DIS after staging is complete, and send a Hit in order to obtain Type 8 EMMs.

WARNING:

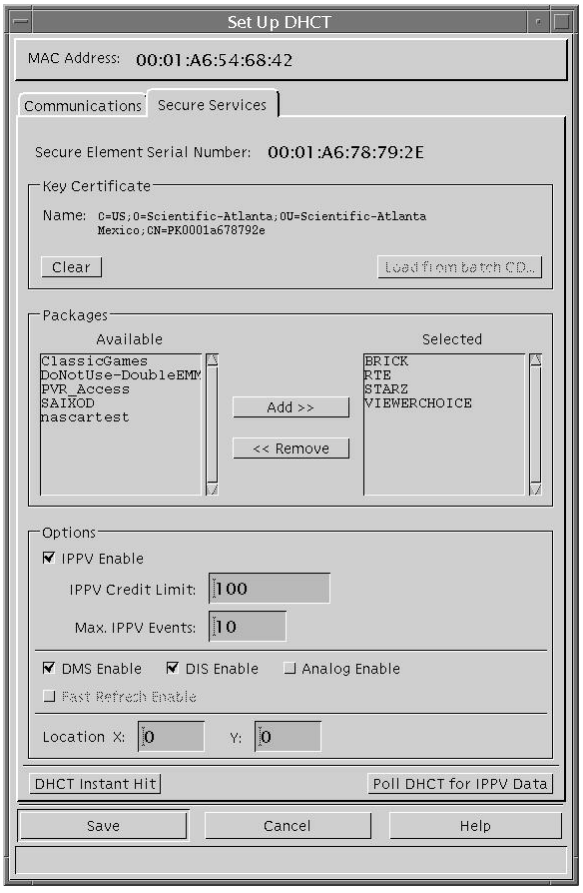
- Do not enable DIS in billing on SSC CableCARD set-top boxes.
- Do not use CableCARD set-top boxes for DIS flag testing purposes.

Ensure the DIS Flag is Enabled

Complete the following steps to perform Test Two on a few recently-staged DHCTs.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click one of the following tabs:
   - If you are using SR 4.2 and later, click **Home Element Provisioning**.
   - If you are using SR 4.0 and earlier, click **Element Provisioning**.
3. Click **DHCT**. The DHCT Provisioning window appears.
4. In the Select Option area, click the **Open** option, if it is not already selected.

5. Do you know the MAC address for the DHCT you want to check?
   - If **yes**, click the **By MAC Address** option, then click in the corresponding field, and type the MAC address for the DHCT you want to check. Go to step 6.
   - If **no,** click the **By Serial Number** option, then click in the corresponding field, and type the serial number for the DHCT you want to check. Go to step 6.
6. Click **Continue.** The Set Up DHCT window opens for the DHCT you want to check.
7. Click the **Secure Services** tab.



8. Does a check mark appear in the DIS Enable field?
   - If **yes**, then the billing system is setting the DIS enable flag.
   - If **no**, you *must* contact your billing provider to have them enable the DIS flag on billing transactions being sent to the DNCS.

9. Repeat steps 4 through 8 on a few recently-staged DHCTs to verify that the DIS enable flag is being set.
10. Click **Cancel** to close the Set Up DHCT window and return to the DHCT Provisioning window.
11. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.
12. If you determine the DIS flag is currently being set to **enabled** by your billing system then it will not be necessary for you to proceed to the next section, ***Check Available Database Space*** (on page 7). Instead, you will skip ahead to ***Verify the SBE License Option is Enabled*** (on page 9).

Check Available Database Space

Overview

Before you enable SBE, run a Doctor Report to ensure you have enough database space for additional type 8 EMMs.

Important: If your system does not have enough database space available for additional type 8 EMMs, you *cannot* proceed with the SBE setup.

Checking Your Available Database Space

Complete the following steps to check the available database space using the Doctor Report.

1. Open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and press **Enter.** The system accesses the doctor directory and displays a prompt.

   Note: You may want to expand the xterm window to be able to see more of the report without having to scroll as much.
3. Type **doctor -av** and press **Enter.** The system generates the doctor report. When finished, the system displays the directory where the report is stored.

   Example: Output report file is **/export/home/dncs/doctor/report.040227_1058.doc**
4. Type **more <doctor report file path>** and press **Enter.** The system displays the Doctor Report one page at a time.

   Example: more /export/home/dncs/doctor/report.040227_1058.doc

5 Press **Enter** to scroll through the report until you see the DNCS Database Check section as shown in the following example:

DNCS Database Check

Total tempspace = 20520 pages (40.0 M)

Free tempspace = 20083 pages (39.2 M)

Database tempspace is at 2.2% used capacity.

Total dataspace = 2097150 pages (4095.9 M)

Free dataspace = 1919078 pages (3748.1 M)

OK: Database dataspace is at 8.5% used capacity.

Notes:

- In the preceding example, the last line of data indicates that the database is at 8.5 percent used capacity. The Doctor Report displays an error condition once the database reaches 75 percent used capacity.
- For each 100,000 DHCTs you will need an additional 461 MB of data space for type 8 EMMs.

6 Does your Doctor Report show a dataspace used capacity of 75% or more?

- If **yes,** contact the representative who handles your account for assistance on this issue.
  Important: If your site does not have enough database space, you *cannot* proceed.
- If **no**, continue to step 7.

7 Press **Ctrl-C** to exit the utility.

8 Type **exit** and press **Enter.** The xterm window closes.

9 Go to ***Verify the SBE License Option is Enabled*** (on page 9).

Verify the SBE License Option is Enabled

Overview

After you verify that billing is enabling the DIS flag on billing transactions being sent to the DNCS and you have checked the available database space, you must ensure that VOD session encryption is licensed.

Verifying your SBE License Option

Complete the following steps to verify that VOD session encryption is licensed using the Doctor Report.

1. Open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and press **Enter.** The system accesses the doctor directory and displays a prompt.

   Note: You may want to expand the xterm window to be able to see more of the report without having to scroll as much.
3. Type **doctor -av** and press **Enter.** The system generates the doctor report. When finished, the system displays the directory where the report is stored.

   Example: Output report file is **/export/home/dncs/doctor/report.040227_1058.doc**
4. Type **more <doctor report file path>** and press **Enter.** The system displays the Doctor Report one page at a time.

   Example: more /export/home/dncs/doctor/report.040227_1058.doc
5. Press **Enter** to scroll through the report until you see the DNCS License Check section as shown in the following example.

   DNCS License Check

EAS FIPS Code Filtering	licensed
DOCSIS DHCT Support	not_licensed
Enhanced VOD Session Throughput	licensed
VOD Session Encryption	licensed

   - If VOD Session Encryption is licensed, contact the representative who handles your account to schedule SBE activation.
   - If VOD Session Encryption is not licensed, contact the representative who handles your account to schedule SBE activation and have VOD session encryption licensed.
6. Press **Ctrl-C** to exit the utility.
7. Type **exit** and press **Enter.** The xterm window closes.

2

Activate SBE and Verify Activation

Introduction

This chapter details the procedures that must be completed to activate SBE and to verify that it is active on your system.

In This Chapter

- Activating SBE..... 12
- Verifying SBE License Activation..... 13

Activating SBE

In preparation for activating SBE, we completed the following steps:

1. We enabled licensing
2. We turned on the DIS flag

The rest of the SBE activation process is automatic; within 72 hours of your enabling licensing and the DIS flag, billing will send type 8 EMMs to your set-top box and SBE will then be active.

The next step is to wait 72 hours and then proceed with the following section, ***Verifying SBE License Activation*** (on page 13), to ensure SBE has successfully been activated.

Verifying SBE License Activation

Overview

To verify SBE activation you must run the checkDIS.ksh program and check database counts.

Run checkDIS.ksh

1. Are you logged into the DNCS as **dncs user**?
   - If **yes**, go to step 4.
   - If **no,** go to step 2.
2. Log on as the **dncs user**. The password prompt appears.
3. Type the dncs user password and press **Enter**.
4. Type **cd /dvs/dncs/bin** and press **Enter**.
5. Run the **checkDIS.ksh** command to see if any DHCTs have DIS disabled:

   Important: All DHCTs in your system should have DIS enabled. If you see any DHCTs with DIS disabled, then your billing system could be sending DIS disabled flags and you *must* contact Cisco Services.
6. Run the **checkDIS.ksh -c** command to obtain two counts from the database.

   Note: It may take several minutes to receive count results. Record the database count results on a sheet of paper.

   Sample checkDIS.ksh Output

```
[Lab Sys1 40.107] $ checkDIS.ksh
# Report of DHCT-count with DIS enabled/disabled...
#  Tue Nov 27 16:39:29 EST 2007
   1786 DHCTs have DIS enabled.
      5 DHCTs have DIS disabled.
      2 DHCTs have DIS disabled with DMS enabled.
0 percent of boxes do NOT have DIS enabled.
 - Would you like to generate a list of 5 MAC addresses
 - for boxes with DIS disabled? (y/n) y (I answered yes)
Building a list of MACs with DIS=disabled.
List is in file: /tmp/noDIS.out
 - Would you like to generate a list of 2 MAC addresses
 - for boxes with DIS disabled, but DMS enabled? (y/n) y (I answered yes)
Building a list of MACs with DIS=disabled AND DMS=enabled.
List is in file: /tmp/noDISwDMS.out
# Done: Tue Nov 27 16:39:49 EST 2007
```

7 The sample data in step 6 clearly shows the following database count:

1786 DHCTs have DIS enabled, 5 DHCTs have DIS disabled, 2 DHCTs have DIS disabled with DMS enabled, and 0 percent of boxes do NOT have DIS enabled.

Important: The desired result of the database counts is for two database counts to match or for the first number to be larger than the second number. You *must* contact Cisco Services if you do not notice progress from one count to the next.

Check Database Counts

Use the VOD Information diagnostic screen to verify that a DHCT has received type 8 EMMs. This step cannot be performed on DHCTs that do not support the SA Resident Application (SARA).

Important: If your DHCTs are supported by a resident application other than SARA, contact your vendor to see if there is a similar verification procedure to determine that the DHCTs have received type 8 EMMs.

1 Check the DNCS for missing QAM key certificates using the *Correcting QAM, MQAM, GQAM, and GoQAM Modulators With Missing Key Certificates* (part number 745235) document. This document contains procedures to determine whether or not QAM key certificates are stored on the DNCS, including instructions to correct this condition.

Important: A QAM with a missing key certificate will cause encrypted VOD purchases on that QAM to fail.

2 For any DHCTs, use the VOD Information diagnostic screen to check the VOD cells field to verify that the DHCT has received type 8 EMMs.

Notes:

- This step cannot be performed on DHCTs that do not support the SARA.
- If your DHCTs are supported by a resident application other than SARA, contact your vendor to see if there is a similar verification procedure to determine that the DHCTs have received type 8 EMMs.
- For more information, refer to *Understanding Diagnostic Screens for the Explorer Digital Home Communications Terminals Application Guide* (part number 749244).

Results:

The VOD cells field shows the bit map representation of the number of non-volatile storage cells available for VOD events, as follows:

- If the VOD cells field shows **FC000000,** then the DHCT has received the type 8 EMMs needed for encryption.
- If the VOD cells field shows **00000000,** then the DHCT has not received the type 8 EMMs needed for encryption. Contact Cisco Services for assistance.

The following image illustrates the VOD Information diagnostic screen; as shown, your VOD cells field will show **FC000000** if the DHCT has received the type 8 EMMs needed for encryption.

3

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.

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

April 2012 Printed in USA

Part Number 740029 Rev B