Video Encryption

The Cisco cBR-8 supports PowerKey and Privacy Mode Encryption (PME) encryption CA systems for Video On Demand (VOD) sessions to address security concerns. However, only one encryption type can be installed on the line card. There are two levels to the CA system. The lower level encrypts the actual data streams. The upper level specifies the control words that are used to encrypt the data streams.

- Information About Encryption, on page 1
- How to Configure Encryption for the Data Stream, on page 2
- Configuration Examples for Encryption, on page 3
- Configuring Privacy Mode Encryption, on page 3
- Troubleshooting Video Encryption Issues, on page 6
- Feature Information for Encryption, on page 10

Information About Encryption

The encrypted sessions can be created on any QAM carriers on a line card. Only the Single Program Transport Stream (SPTS) VOD session can be encrypted. Encryption is not supported on the Pass-through, and Data-piping sessions.

The VOD session can be encrypted in any of the following types of encryption:

- PowerKey for video session management protocol GQI
- Privacy Mode Encryption (PME) for Table-based session
- Digital Video Broadcasting (DVB)

The scrambler mode varies based on the type of encryption, as given in the following table:

Table 1: Supported Encryption Types and Scrambler Modes

Encryption Type	Scrambler Mode
PowerKey	DES, 3DES
PME	DVS-042
DVB	DVB-CSA

Prerequisites for Encryption

You should configure the Virtual Carrier Group (VCG) to setup an encrypted session. For more details, see the Configuring Virtual Carrier Group, on page 2.

How to Configure Encryption for the Data Stream

This section describes how to configure encryption for the video session on Cisco cBR-8.

- Enforcing Data Stream Encryption Type, on page 2
- Configuring Virtual Carrier Group, on page 2
- Verifying Encryption Configuration, on page 3

Enforcing Data Stream Encryption Type

Note Once the line card and VCG are configured for PowerKey encryption, further configuration of the Cisco cBR-8 is not required.

To configure the encryption type for a VOD session, perform the following steps:

Before You Begin

Configure the Virtual Carrier Group (VCG) to setup an encrypted session. For more details, see .

```
enable
configure terminal
cable video
encryption
linecard slot/bay ca-system [dvb | pme | powerkey] scrambler scrambler-type
exit
```

Configuring Virtual Carrier Group

To configure the Virtual Carrier Group (VCG) for setting up an encrypted session, perform the following steps:

```
enable
configure terminal
cable video
virtual-carrier-group name [id #]
rf-channel start-channel#-end-channel# tsid start-tsid-end-tsid output-port-number
 start-number-end-num
virtual-edge-input ipaddr input-port-number #
encrypt
exit
```

Verifying Encryption Configuration

To verify the encryption configurations, use the following command:

show cable video encryption linecard [*all | slot number*]

Example 1:

```
Router#show cable video encryption linecard 7/0 Line card: 7/0
CA System Scrambler
==============================================
powerkey des
```

Example 2:

```
Router#show cable video encryption linecard all Line card: 7/0
CA System Scrambler
==============================================
powerkey des
```

Configuration Examples for Encryption

This section provides configuration examples for the Encryption feature.

Example: Enforcing Data Stream Encryption Type

The following is a sample in which the line card in slot 7 is configured for powerkey encryption.

```
Router(config)#cable video Router(config-video)#encryption
Router(config-video-encrypt)#linecard 7/0 ca-system powerkey scrambler des
```

Example: Configuring Virtual Carrier Group

The following is a sample in which the QAM channel from 64 to 158 are encryption capable if the virtual channels are successfully bound to a Service Distribution Group. The sessions created on those QAM carriers are encrypted using the scrambler installed on the line card.

```
Router(config)#cable video
Router(config-video)#virtual-carrier-group sdv-grp
Router(config-video-vcg)#rf-channel 64-158 tsid 64-158 output-port-number 64-158
Router(config-video-vcg)virtual-edge-input 14.1.1.1 input-port-number 1
Router(config-video-vcg)encrypt
Router(config-video-vcg)#exit
```

Configuring Privacy Mode Encryption

Only one device from the MSO site can communicate with the Encryption Renewal System (ERS) and obtain the latest ECM templates. The CEM communicates with the ERS and sends the ECM templates to the Cisco Edge QAM devices in the MSO site.

You can configure the following:

- VODS-ID—IDs assigned by CCAD or ARRIS to the MSO site. The configured VODS-ID on the Cisco cBR-8 and the CEM must be same.

- CEM IP—Interface IP of the Windows/Linux system through which the CEM can be reached by Cisco cBR-8.
- CEM Port—Port number on which the CEM listens for connections from the Cisco cBR-8.
- Management Interface—Source IP address of the Cisco cBR-8 virtual interface through which the connection must be established with the CEM server.

Note There can be only one entry for VODS-ID, CEM IP, CEM Port, and Management Interface IP. If you configure any new values for these parameters, the previous configuration is cleared. You can clear the configurations using the 'no' form of the command.

Configuring VODS-ID

To configure the VODS-ID of the CEM, perform the following steps:

```
enable
configure terminal
cable video
encryption
pme vodsid id
exit
```

Configuring CEM IP and Port

To configure the CEM IP and port of the CEM, perform the following steps:

```
enable
configure terminal
cable video
encryption
pme cem ip-address tcp_port
exit
```

Configuring Management IP

To configure the PME management IP address to establish CEM connection, perform the following steps:

Before You Begin

The virtual port group must be configured before configuring the management IP. For more information, see the *Configuring a VirtualPortGroup iIterface* section.

```
enable
configure terminal
cable video
encryption
pme mgmt-ip ip-address
exit
```

Verifying PME Connection Status

To verify the connection status between the Cisco Converged EdgeQAMManager (CEM) application and the Cisco cBR-8,use the following command:

show cable video encryption linecard [*all | slot number*]

This command displays the following information:

- VODS-ID—Specifies the configured VODS-ID on the CEM and Cisco cBR-8.
- CEM IP—Specifies the IP through which CEM can be reached by Cisco cBR-8.
- CEM Port—Specifies the port on which the CEM obtain connections from Cisco cBR-8.
- Local Mgmt IP—Specifies the Cisco cBR-8 interface through which the connection is established with the CEM.
- Local Port—Specifies the Local Port number assigned for the connection with the CEM.
- CEM Connection State—Specifies the status of the connection with the CEM (Connected (or) Not Connected).
- Count of ECMs recd—Specifies the count of ECMs received from the CEM.

Example:

This is a sample output of the show command that displays the connection status of PME.

```
Router#show cable video encryption pme status
PME Connection Status:
VODS-ID : 111
CEM IP : 1.200.1.163
CEM Port : 5000
Local Mgmt IP : 1.24.2.6
Local Port : 50394
CEM Connection State : Connected Count of ECMs recd : 2
```

Verifying PME Version

To verify the version information of the PME module loaded in the chassis, use the following command:

show cablevideo encryption pme version

The version information is read from the IOS PME subsystem. The version information displays in MAJOR.MINOR version format.

Example:

This is a sample output of the show command that displays the version details of PME.

```
Router#show cable video encryption pme version
PME Version: 1.0
```

Verifying PME Sessions on a Line Card

To verify the sessions that use the PME modules that are loaded on a specific line card, use the following command:

show cable video encryption pme linecard [*slot | bay*] **session** {*1-65535 | all | summary*}

Example 1:

This is a sample output of the show command that displays the session details that use PME modules.

```
Router#show cable video encryption pme linecard 7/0 session all Count of ECMG Streams: 4
==================== ECMG Stream DATA ========================
Stream
ID num EcmId CP# CwE CPDur NomCPD EcmRqst EcmRsp
---------- ---------- ---- --- ----- ------ ---------- ----------

0020(0032) 0020(0032) 0002 0 0 40000 7 2
0021(0033) 0021(0033) 0002 0 0 40000 7 2
0040(0064) 0040(0064) 0002 0 0 40000 7 2
0041(0065) 0041(0065) 0002 0 0 40000 7 2
video-LWR-B-A7B#show cable video encryption pme linecard 7/0 session 32 Stream 32, session
 7681 is active

Stream number = 32 Session number = 7681
ECM requests = 8 ECM replies = 2
ECM ID = 32 CryptoPeriod num = 2
CP duration = 0 Nominal duration = 40000
CA transfer mode = 1 Stream status = No Error Blob details

video-LWR-B-A7B#show cable video encryption pme linecard 7/0 session summary Currently
active streams:
Active = 4 ECM req/resp mismatch = 4
ECM req, all streams = 32 ECM resp, all streams = 8

Since last reset:
Sessions created = 4 Sessions deleted = 0
ECMs received = 2 ECMs discarded = 0
```

Troubleshooting Video Encryption Issues

A Video On Demand (VOD) session might fail at the subscriber site due to multiple factors. One of the factors is scrambling.

If scrambling fails during the VOD purchase, the Program Map Table is held back which in turn results in a VOD failure. Though there are alarms already available in the software that indicates the scrambling failure, it gives a high level error and does not provide information about the reason for the failure. These alarms are logged in syslog.

New Events and Alarms for Video Encryption Debugging

Cisco IOS-XE Release 16.12.1y supports New Events and Alarms for Video Scrambling Debugging Log Enhancement. The following new logs provide better debugging of VOD failures. All the new logs are written in btrace log of respective line card.

- Whenever a session under an encrypted VCG gets input to ACTIVE-PSI, the log will be written along with session id, on-id, ts-id and program number.
- Whenever the scrambling starts, the log will be written along with on-id, ts-id and program number.
- After the VoD ends and input goes to off state, a log will be written along with session id, on-id, ts-id and program number.
- If the scrambling fails for any session, then details about the failure will be logged along with the existing alarm in supervisor console.

You can use the **show platform software trace message lc-veman <LC slot number>/0** command to view the logs. See the following example:

```
Router# show platform software trace message lc-veman 8/0
This command is being deprecated. Please use 'show logging process' command.
executing cmd on chassis local ...


2020/02/03 03:34:05.046653 {veman_8-0}{1}: [scs] [7197]:  (warn):  02/03 20:34:04.477 [scs]:
 [7197]: (warning): PERFORMANCE: entering ScsTask too late (65 ms since last tick)

2020/02/03 03:34:05.046624 {veman_8-0}{1}: [scs] [7197]:  (warn):  02/03 20:34:04.179 [scs]:
 [7197]: (warning): PERFORMANCE: entering ScsTask too late (67 ms since last tick)

2020/02/03 03:34:05.046558 {veman_8-0}{1}: [scs] [7197]:  (warn):  02/03 20:34:04.073 [scs]:
 [7197]: (warning): PERFORMANCE: entering ScsTask too late (61 ms since last tick)
```

The following table shows all the new logs and alarms logged in the btrace log.

Table 2: New logs and alarms logged in the btrace log

Alarm/Event	Log Type	Log Message
Input ON	Event	I/p on Ses <session id> qam <on-id>/<ts-id> Sid <program number> qid <qam-id>
Input OFF	Event	I/p off Ses <session id> qam <on-id>/<ts-id> Sid <program number> qid <qam-id>
Scrambling started	Event	Scrambling started. Qam <on-id>/<ts-id> Sid <program number> SCG <SCG id>
Scrambling not started (no Input)	Alarm **Set/Clear**	(117) No i/p=Qam: <on-id>/<ts-id> Sid: <program number>
Scrambling not started (no ECMs)	Alarm **Set/Clear**	(19) No ECMs=CAS:<CAS-id> Qam: <on-id>/<ts-id> Sid: <program number>; SCG=<SCG id>
Scrambling not started (no ECMG)	Alarm **Set/Clear**	(19) Missing Ecmg/Timings; SuperCAS Id=<CAS Id>; ECM Id=1

- **Input ON**

  When a subscriber purchases a VOD session, the VOD asset stream is expected to be hitting the cBR8 input. Once the input stream is detected and the session gets to ACTIVE-PSI state, this information is logged along with the following information:

  - Session ID
  - QAM ID

- Original network ID
- Transport stream ID
- Program number

- **Input OFF**

  When the VoD ends, the input stream stops. The session will move to IDLE state after few milliseconds of input unavailability. After the Off timer, the session will move to OFF state during which this information is logged along with the following.

  - Session ID
  - QAM ID
  - Original network ID
  - Transport stream ID
  - Program number

- **Scrambling started**

  On VOD purchase, after all the required conditions are met for scrambling (Input stream availability, ECM availability, etc.,), the session will get scrambled. That event is logged with following information.

  - Original network ID
  - Transport stream ID
  - Program number
  - SCG ID

- **Scrambling not started (no input)**

  On VoD purchase, if the input VoD asset stream is not hitting the cBR8 for more than 10 seconds, then this alarm is set and logged in the btrace log. After this log is set, if the input starts hitting the cBR8 or if the VoD session is torn down, this alarm will be cleared and also be logged in the btrace log. This log has the following information.

  - Original network ID
  - Transport stream ID
  - Program number

Note This alarm is applicable only for Powerkey and DVB session-based scrambling.

- **Scrambling not started (no ECMs)**

  If the scrambling is not started due to unavailability of ECMs, then this alarm is set and logged in the btrace log. After this log is set, if the ECM is received or if the VoD session is torn down, this alarm will be cleared and also be logged in the btrace log. This log has the following information.

- Original network ID
- Transport stream ID
- Program number
- CAS ID
- SCG ID

- **Scrambling not started (no ECMG)**

  If the scrambling is not started due to unavailability of ECMG server, then this alarm is set and logged in the btrace log. After this log is set, if the ECMG is connected or if the VoD session is torn down, this alarm will be cleared and also be logged in the btrace log. This log has the following information.

  - CAS ID
  - ECM ID

Note This alarm should never happen for Powerkey and PME scrambling.

Example Logs

Following are the example logs for the new events and alarms:

- **Input ON**

```
I/p on Ses 1048578 qam 65535/65041 Sid 65002 qid 9
```

- **Input OFF**

```
I/p off Ses 1048578 qam 65535/65041 Sid 65002 qid 9
```

- **Scrambling started**

```
Scrambling started. Qam 65535/65002 Sid 65041 SCG 1057576
```

- **Scrambling not started (no ECMs) Alarm set**

```
Set: (19) No ECMs=CAS:0x09520000 Qam:65535/65041 Sid:65002,=;SCG=1057576=;
```

- **Scrambling not started (no ECMs) Alarm clear**

```
Clear: (19) No ECMs=CAS:0x09520000 Qam:65535/65041 Sid:65002,=;SCG=1057576=;
```

- **Scrambling not started (no input) Alarm set**

```
Set: (117) No i/p=Qam:65535/65041 Sid:65002,=;
```

- **Scrambling not started (no input) Alarm clear**

```
Clear: (117) No i/p=Qam:65535/65041 Sid:65002,=;
```

- **Scrambling not started (no ECMG) Alarm set**

```
Set: (19) =Missing Ecmg/Timings=;SuperCAS Id=0x01230000=;ECM Id=1=;
```

Feature Information for Encryption

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 3: Feature Information for Encryption

Feature Name	Release	Feature Information
Encryption	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.
Video Encryption Debugging Log Enhancement	16.12.1y	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.