



DualCrypt Encryption Mode Support

The Dualcrypt Encryption feature enables the Session and Resource Manager (SRM) to configure the PowerKey and DVB CAS sessions on the same line card (LC) of the Cisco cBR-8 Converged Broadband Router.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

- [Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1](#)
- [Information about DualCrypt Encryption Mode, on page 2](#)
- [How to Configure Dualcrypt Encryption Mode, on page 4](#)
- [Configuration Examples, on page 9](#)
- [Feature Information for DualCrypt Encryption Mode, on page 12](#)

Hardware Compatibility Matrix for the Cisco cBR Series Routers



Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	<p>Cisco IOS-XE Release 16.5.1 and Later Releases</p> <p>Cisco cBR-8 Supervisor:</p> <ul style="list-style-type: none"> • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G 	<p>Cisco IOS-XE Release 16.5.1 and Later Releases</p> <p>Cisco cBR-8 CCAP Line Cards:</p> <ul style="list-style-type: none"> • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC <p>Digital PICs:</p> <ul style="list-style-type: none"> • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G <p>Cisco cBR-8 Downstream PHY Module:</p> <ul style="list-style-type: none"> • PID—CBR-D31-DS-MOD <p>Cisco cBR-8 Upstream PHY Modules:</p> <ul style="list-style-type: none"> • PID—CBR-D31-US-MOD

Information about DualCrypt Encryption Mode

You can use this feature when you want the PowerKey and DVB sessions on the same QAM channel. This feature is applicable only to GQI-based sessions, as it uses the Generic QAM Interface (GQI) protocol.

To configure the dualcrypt encryption mode, you should set up connections with Event Information Scheduler (EIS) and Entitlement Control Message Generator (ECMG).

Prerequisites for Dualcrypt Encryption Mode

- Ensure that the following components are available on your system before configuring dualcrypt encryption for sessions.

- Service Distribution Group (SDG)
 - Virtual Carrier Group (VCG) with encrypt
 - Logical Edge Device (LED) with GQI protocol
 - Event Information Scheduler (EIS)
 - Entitlement Control Message Generator (ECMG)
- Ensure that the VCG is bound to SDG
 - Ensure that the VCG is associated to LED
 - Ensure that the Virtual Edge Input is configured only on LED
 - Ensure that the following configurations are available on your system:

- The encryption algorithm of the line card is set to DVB-CSA.

You can set it using the following command:

```
linecard <slot>/<bay> ca-system dualcrypt scrambler dvb-csa
```

- The virtual port group interface is configured and the same is set for the management interface under cable video, because the DVB requires a management IP address for communicating with external servers.

Use the following commands to set the virtual port group interface as management interface for cable video:

```
configure terminal
cable video
mgmt-intf VirtualPortGroup <id>
```

- The CA interface on the line card and the route for reaching the ECMG server are specified for session-based scrambling.

Use the following commands to specify CA interface and the route:

```
ca-interface linecard <slot>/<bay> <IP_Address>
route-ecmg <ECMG_Server_IP_Address> <Netmask> <Interface>
<Forwarding_Router_IP_Address>
```

- The **vrf <vrf_name>** keyword is configured for routes to populate on the respective VRFs, if you are using VRF for traffic or management separately. Configure the CA interface with specific VRF name.

```
ca-interface linecard <slot>/<bay> <IP_Address> vrf <vrf_name>
```

- (Optional) The bind option is used to associate EIS with specific IP address or GQI-based LED

To use a single IP address for GQI (create and delete sessions) and EIS (provision/de-provision SCGs), the operator should bind the EIS with GQI-based LED using the IP option and configure the required IP address. The IP address should be the subnet of the configured virtual port group. By default, the EIS uses the management IP address configured under DVB and the GQI uses the management IP address configured under LED for session control.

The following sample commands show how to bind the EIS:

```
configure terminal
cable video
encryption
```

```

dvb
eis <name of eis>
listening-port <1-65535> bind ip <ip address>
or
listening-port <1-65535> bind led <id | name> <led id | led name>

```

**Note**

- If all configured EIS are bound to a specific IP/LED using the bind option, the configuration of management IP address under DVB is optional.
- The bind option is not available in Cisco RF Gateway 10.

Restrictions for DualCrypt Encryption Mode

The following restrictions are applicable for configuring DualCrypt encryption mode:

- The DualCrypt Encryption feature is applicable only to GQI-based remapped sessions.
- Use this feature only for PowerKey, DVB, and Clear sessions.
- Do not use this feature along with tier-based scrambling mode.

How to Configure Dualcrypt Encryption Mode

Configuring DVB Session for DualCrypt Encryption

This section explains how to configure the session-based scrambling with DualCrypt encryption mode.

Procedure

To configure a DVB session for DualCrypt encryption, use the following commands:

```

enable
configure terminal
cable video
mgmt-intf VirtualPortGroup <group_id>
encryption
linecard <lcslot/subslot> ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg ECMG_Server_IP_Address Netmask Interface Forwarding_Router_IP_Address
mgmt-ip IP_Address
eis EIS_Name id EIS_ID
listening-port port_number [bind {ip <ip address> | led < id <led id >| name <led name>>}]

ca-interface linecard <slot>/<bay> IP_Address
ecmg ECMG_Name id ECMG_ID
mode vod linecard <slot>/<bay>
type <standard/hitachi/irdeto/nagra/pkey>
ca-system-id CA_System_ID CA_Subsystem_ID
ecm-pid-source <sid/auto/ecm-id>
connection id ID priority connection_priority IP_Address Port

```

Verifying DVB Session for DualCrypt Encryption

To verify the configuration of the encryption algorithm on the linecard, use the **show cable video encryption linecard <slot>/<bay>** command as shown in the following example:

```
Router#show cable video encryption linecard 8/0
Line card: 8/0
CA System      Scrambler      DVB-Conformance
=====
dualcrypt      dvb-csa        Enabled
```

To verify the scrambler configuration, use the **show cable video encryption scrambler brief** command as shown in the following example:

```
Router#show cable video encryption scrambler brief
Scrambler information
Chassis wide scrambler: none
-----
Linecard      Current      Configured
              Scrambler    Scrambler
=====
1             Not Ready    None
2             Not Ready    None
3             Not Ready    None
4             Not Ready    None
5             Not Ready    None
6             Not Ready    None
7             dvb-csa      None
8             dvb-csa      dvb-csa
9             des/dvs042   None
```

To verify the ECMG connection, use the **show cable video encryption dvb ecmg id <id> connection** command as shown in the following example:

```
Router#show cable video encryption dvb ecmg id <ID> connection
-----
ECMG Slot  ECMG ID  ECMG Type  CA Sys ID  CA Subsys ID  PID Source  Lower limit  Upper limit  Streams/ECMG  Open Streams/ECMG  Auto Chan ID
-----
1         test  standard  0x950      0x0           sid          0          0            1            1              Enabled
7         1          VOD
```

ECMG Connections for ECMG ID = 1

```
-----
Conn -ID  Conn Priority  IP Address      Port Number  Channel ID  Conn Status  Open Streams
-----
1     1      10.10.1.1      9878         1           Open        1
```

The `Conn Status` field shows the status of the connection with the ECMG server and the `Open Streams` field indicates the number of active ECM streams.

To verify the EIS connection, use the **show cable video encryption dvb eis id <id>** command as shown in the following example:

```
Router#show cable video encryption dvb eis id <ID>
-----
EIS EIS Peer      Management TCP CP      CP      Overwrite Fail-To-Clear Connection
```

ID	Name	IP	IP	Port	Overrule	Duration	SCG	Duration	Status
1	test	10.10.1.1	10.10.1.10	9898	DISABLED	0	DISABLED	0	Connected

Verifying the GQI Configuration

To verify the GQI connection, use the **show cable video gqi connection** command, as shown in the following example:

```
Router>show cable video gqi connection
LED Management Server      Connection Version Event   Reset      Encryption
ID  IP          IP          Status      Pending Indication Discovery
-----
2   10.10.1.1   10.100.1.1 Connected  2         0         ACKED      Sent
```

To verify the statistics of GQI, use the **show cable video logical-edge-device id <ID> statistics** command, as shown in the following example:

```
Router>show cable video logical-edge-device id <ID> statistics

      Create   Delete   Insert   Cancel   Switch   Reset      Encryption   Event
      Session Session Packet Packet Source Indication Discovery Notification
-----
Success 4       0       0       0       0       3         7           0
Error   0       0       0       0       0       0         0           0
Total   4       0       0       0       0       3         7           0
```

Verifying the GQI Sessions for Encryption

To verify whether the sessions are encrypted, use the **show cable video session logical-edge-device id <ID>** command, as shown in the following example, and check the **Encrypt Status** field.

```
Router>show cable video session logical-edge-device id <ID>
Total Sessions = 4

Session Output Streaming Session Session Source      UDP   Output  Input
Output Input   Output Encrypt Encrypt Low   Session
Id      Port   Type  Type  Ucast Dest IP/Mcast IP (S,G) Port  Program State   State
Bitrate Bitrate Type  Status Latency Name
-----
1048580 20     Passthru UDP    10.10.10.11      49152 -      ACTIVE-PSI ON
      1713128 1698122 CLEAR -              N      0x00000000000000000000000000000000
1048581 20     Remap   UDP    10.10.10.11      49153 2      ACTIVE-PSI ON
      1711859 1707422 DVB    Encrypted N      0x00000000000000000000000000000002
1048582 23     Passthru UDP    10.10.10.11      49154 -      ACTIVE-PSI ON
      1711962 1699101 CLEAR -              N      0x00000000000000000000000000000003
1048583 23     Remap   UDP    10.10.10.11      49155 4      ACTIVE-PSI ON
      1712498 1707834 DVB    Encrypted N      0x00000000000000000000000000000004
```

The session's **Encrypt Status** should be **Encrypted**. The **Output State** should be **ON** to show the proper **Encrypt Status** for **DVB** sessions. If the **Output State** is **Pending**, the **Encrypt Status** will be shown as **Pending**.

To get a list of SCGs, use the **show cable video scg allq** command as shown in the following example:

```
Router>show cable video scg allq
SCGs: 4      Carriers with SCGs: 3

-----
SCG      ON   TS   SCG Ref Activation CP Duration SCG   Sess LED/
ID      ID   ID   ID   Time      (msec)   Status Id  EIS
```

```

-----
900      1      20  65535  Immediate  10000      Active N/A  1
  Service IDs : 2
  ES PIDs : NA

9001     1      20  65535  Immediate  10000      Active N/A  1
  Service IDs : 1
  ES PIDs : NA

9006     1      22  65535  Immediate  10000      Active N/A  1
  Service IDs : 1
  ES PIDs : NA

9002     1      23  65535  Immediate  10000      Active N/A  1
  Service IDs : 4
  ES PIDs : NA

Number of SCGs = 4

```

Verifying ONID and TSID of the QAMs Configured for Specific LED

To get the details of ONID and TSID configured for QAMs configured under LED, use the **show cable video logical-edge-device id 1**, as shown in the following example, and verify the ONID and TSID details:

```

Logical Edge Device: led1
Id: 1
Protocol: GQI
Service State: Active
Discovery State: Disable
Management IP: 10.10.10.11
MAC Address:
Number of Servers: 1
  Server 1: 10.10.10.11
Reset Interval: 5
Keepalive Interval: 5   Retry Count:3
Number of Virtual Carrier Groups: 1
Number of Share Virtual Edge Input: 1
Number of Physical Qams: 39
Number of Sessions: 4
No Reserve PID Range

Virtual Edge Input:
Input Port   VEI           Slot/Bay   Bundle   Gateway
ID           IP
-----
1            10.10.10.11   7/0       -        -

Virtual Carrier Group:
ID Name Total Total   Service-Distribution-Group Service-Distribution-Group
VEI   RF-channel Name                               ID
-----
1   vcg1 0    39    sdg1                               1

QAM          Port   Physical Admin Operational TSID ONID Output VCG SDG Encryption
Controller Type   QAM ID  State  State           1   1   Port  ID  ID  Capable
-----
7/0/0:0     RF Port 0      ON    UP           1   1   1    1   1  dualcrypt
7/0/0:1     RF Port 1      ON    UP           2   1   2    1   1  dualcrypt
7/0/0:2     RF Port 2      ON    UP           3   1   3    1   1  dualcrypt
7/0/0:3     RF Port 3      ON    UP           4   1   4    1   1  dualcrypt
7/0/0:4     RF Port 4      ON    UP           5   1   5    1   1  dualcrypt

```

7/0/0:5	RF Port 5	ON	UP	6	1	6	1	1	dualcrypt
7/0/0:6	RF Port 6	ON	UP	7	1	7	1	1	dualcrypt
7/0/0:7	RF Port 7	ON	UP	8	1	8	1	1	dualcrypt
7/0/0:8	RF Port 8	ON	UP	9	1	9	1	1	dualcrypt
7/0/0:9	RF Port 9	ON	UP	10	1	10	1	1	dualcrypt
7/0/0:10	RF Port 10	ON	UP	11	1	11	1	1	dualcrypt
7/0/0:20	RF Port 20	ON	UP	20	1	20	1	1	dualcrypt
7/0/0:21	RF Port 21	ON	UP	21	1	21	1	1	dualcrypt
7/0/0:22	RF Port 22	ON	UP	22	1	22	1	1	dualcrypt
7/0/0:23	RF Port 23	ON	UP	23	1	23	1	1	dualcrypt
7/0/0:24	RF Port 24	ON	UP	24	1	24	1	1	dualcrypt
7/0/0:25	RF Port 25	ON	UP	25	1	25	1	1	dualcrypt
7/0/0:26	RF Port 26	ON	UP	26	1	26	1	1	dualcrypt
7/0/0:27	RF Port 27	ON	UP	27	1	27	1	1	dualcrypt
7/0/0:28	RF Port 28	ON	UP	28	1	28	1	1	dualcrypt
7/0/0:29	RF Port 29	ON	UP	29	1	29	1	1	dualcrypt
7/0/0:30	RF Port 30	ON	UP	30	1	30	1	1	dualcrypt
7/0/0:31	RF Port 31	ON	UP	31	1	31	1	1	dualcrypt
7/0/0:32	RF Port 32	ON	UP	32	1	32	1	1	dualcrypt
7/0/0:33	RF Port 33	ON	UP	33	1	33	1	1	dualcrypt
7/0/0:34	RF Port 34	ON	UP	34	1	34	1	1	dualcrypt
7/0/0:35	RF Port 35	ON	UP	35	1	35	1	1	dualcrypt
7/0/0:36	RF Port 36	ON	UP	36	1	36	1	1	dualcrypt
7/0/0:37	RF Port 37	ON	UP	37	1	37	1	1	dualcrypt
7/0/0:38	RF Port 38	ON	UP	38	1	38	1	1	dualcrypt
7/0/0:39	RF Port 39	ON	UP	39	1	39	1	1	dualcrypt
7/0/0:40	RF Port 40	ON	UP	40	1	40	1	1	dualcrypt
7/0/0:41	RF Port 41	ON	UP	41	1	41	1	1	dualcrypt
7/0/0:42	RF Port 42	ON	UP	42	1	42	1	1	dualcrypt
7/0/0:43	RF Port 43	ON	UP	43	1	43	1	1	dualcrypt
7/0/0:44	RF Port 44	ON	UP	44	1	44	1	1	dualcrypt
7/0/0:45	RF Port 45	ON	UP	45	1	45	1	1	dualcrypt
7/0/0:46	RF Port 46	ON	UP	46	1	46	1	1	dualcrypt
7/0/0:47	RF Port 47	ON	UP	47	1	47	1	1	dualcrypt

Troubleshooting Tips

If some configuration errors occur, see the following troubleshooting tips:

- The Management IP must be unique and in the subnet of virtual port group.
- Ensure that the ECMG Server is pingable with source interface as the virtual port group from the Cisco cBR-8 console. This indicates that the ECMG Server is reachable and route is valid.
- Ensure that the TCP port number configured for the ECMG Server in the Cisco cBR-8 is the same as that of the ECMG Server listening port.
- Ensure that the management IP is pingable from the EIS Server. Otherwise, check the routing between the cBR-8 chassis and the EIS server.
- Ensure that the listening port that is configured for the EIS is used for establishing the connection from the EIS Server.
- Ensure that the Virtual Port Group interface is active.
- Ensure that the TenGigabitEthernet interface using which the management traffic reaches the Cisco cBR-8 and the interface through which the CA interface route is configured are active.
- Ensure that the GQI connection is active and sessions are available to be set up.
- Ensure that the EIS connection is active and SCG is available in the Cisco cBR-8.

- Ensure that the CAS configured for ECMG matches the ECM group in SCG.
- Ensure that the ONID, TSID, and Program Number are synchronized with the configured sessions and SCG.

Configuration Examples

This section provides examples for configuring DualCrypt Encryption Mode:

Example: Basic Session-based Scrambling Configuration

```

cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 2.26.1.2
mgmt-ip 10.10.10.11
eis test id 1
    listening-port 9898
ca-interface linecard 8/0 10.10.10.12
ecmg test id 1
mode vod linecard 8/0
type standard
ca-system-id 950 0
auto-channel-id
ecm-pid-source sid
connection id 1 priority 1 10.10.10.13 9878
service-distribution-group sdg1 id 1
    rf-port integrated-cable 8/0/0
virtual-carrier-group vcg1 id 1
encrypt
service-type narrowcast
rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
protocol gqi
mgmt-ip 10.10.10.10
server 10.100.10.11
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcg1
active

```

Example: Session-based Configuration with EIS Binding to LED using LED ID

```

cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 10.10.10.10
mgmt-ip 10.10.10.13
eis test id 1
    listening-port 9898 bind led id 1
ca-interface linecard 8/0 10.10.10.14
ecmg test id 1

```

Example: Configuration with EIS Binding to LED using LED Name

```

mode vod linecard 8/0
type standard
ca-system-id 950 0
auto-channel-id
ecm-pid-source sid
connection id 1 priority 1 10.10.10.11 9878
service-distribution-group sdgl id 1
onid 1
rf-port integrated-cable 8/0/0
virtual-carrier-group vcgl id 1
encrypt
service-type narrowcast
rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
vcg vcgl sdg sdgl
logical-edge-device led1 id 1
protocol gqi
mgmt-ip 10.10.10.11
server 10.10.10.112
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcgl
active

```

Example: Configuration with EIS Binding to LED using LED Name

```

cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 10.10.10.11
mgmt-ip 10.10.10.11
eis test id 1
    listening-port 9898 bind led name led1
ca-interface linecard 8/0 10.10.10.11
ecmg test id 1
mode vod linecard 8/0
type standard
ca-system-id 950 0
auto-channel-id
ecm-pid-source sid
connection id 1 priority 1 10.10.10.11 9878
service-distribution-group sdgl id 1
onid 1
rf-port integrated-cable 8/0/0
virtual-carrier-group vcgl id 1
encrypt
service-type narrowcast
rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
    vcg vcgl sdg sdgl
logical-edge-device led1 id 1
protocol gqi
mgmt-ip 10.10.10.11
server 10.10.10.112
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcgl
active

```

Example: EIS Binding to IP Address Other than Default DVB Management IP Address

```

cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 10.10.10.11
mgmt-ip 10.10.10.11
eis test id 1
  listening-port 9898 bind ip 10.10.10.11
ca-interface linecard 8/0 10.10.10.11
ecmg test id 1
  mode vod linecard 8/0
  type standard
  ca-system-id 950 0
  auto-channel-id
  ecm-pid-source sid
  connection id 1 priority 1 10.10.10.11 9878
service-distribution-group sdg1 id 1
onid 1
rf-port integrated-cable 8/0/0
virtual-carrier-group vcg1 id 1
encrypt
service-type narrowcast
rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
  vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
protocol gqi
mgmt-ip 10.10.10.11
server 10.10.10.11
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcg1
active

```

Example: Session-based Configuration with VRF

```

cable video
multicast-uplink Loopback410 access-list all-multicast vrf vrf_script_red_1 next-hop
10.10.10.11
mgmt-intf VirtualPortGroup 0
encryption
linecard 1/0 ca-system dvb scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel21 10.10.10.1
route-ecmg 10.10.10.16 255.255.255.224 Port-channel21 10.10.10.1
mgmt-ip 10.10.10.10
eis pytool1 id 1
  listening-port 2500
  cp-overrule 6
  overwrite-scg
ca-interface linecard 1/0 10.10.10.0 vrf vrf_script_red_1
ecmg emcg1 id 1
  mode vod linecard 1/0
  type standard
  ca-system-id 952 0
  auto-channel-id
  ecm-pid-source sid
  connection id 1 priority 1 10.10.10.11 5678

```

```

        connection id 2 priority 1 10.10.10.16 8765
    ecmg emcg2 id 2
        mode vod linecard 1/0
        type standard
        ca-system-id 951 0
        auto-channel-id
        ecm-pid-source sid
        connection id 1 priority 1 10.10.10.14 8765
    ecmg emcg3 id 3
        mode vod linecard 1/0
        type standard
        ca-system-id 950 0
        auto-channel-id
        ecm-pid-source sid
        connection id 1 priority 1 10.10.10.11 5678

interface VirtualPortGroup0
    vrf forwarding vrf_script_red_1
    ip address 10.10.10.11 255.255.224.0
    no mop enabled
    no mop sysid

```

Feature Information for DualCrypt Encryption Mode

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the cfng.cisco.com link. An account on the Cisco.com page is not required.



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 2: Feature Information for DualCrypt Encryption Mode

Feature Name	Releases	Feature Information
DualCrypt Encryption Mode	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.