



Explorer Controller System Release 8.0 Release Note

Overview

Introduction

System Release 8.0 (SR 8.0) is a release of the Cisco DBDS (Digital Broadband Delivery System) Explorer Controller (EC) software. This release note contains the following information:

- New feature descriptions
- Media and software versions for this release
- Site requirements
- Procedures on how to view implemented, enhancement, and open BRs (Bug Reports)
- General information on contacting Cisco Services

Purpose

The purpose of this release note is to inform system administrators contemplating an upgrade of the new features, known issues, related documents, and upgrade notes for SR 8.0.

Scope

This release note provides an executive overview of SR 8.0. If you have questions about this release or require more detailed information, contact Cisco Services.

Audience

This release note is for system operators, customer verification labs personnel, and sales and program managers.

Highlights

Document Version

This is the first formal release of this document. This document covers the Explorer Controller System Release 8.0.

Highlights

New features and product improvements for SR 8.0 are described in this section.

ECMG Device Support

SR 7.0 includes support for ECMG devices, including provisioning, session management, and source definition management.

The PowerKEY CAS Gateway (PCG) is an ECMG device.

SAM File Delivery Options

Beginning in SR 7.0, you can now choose to send SAM files (for example, channel map files) to set-tops using BFS on an in-band (IB) carousel, on an out-of-band (OOB) carousel, on both carousels, or you can choose to not deliver SAM files over BFS.

Browser Recommendations

The EC has been tested and verified against the Mozilla Firefox Extended Support Release (ESR) version 24 browser and Firefox desktop version 50 or later. Due to unpredictable results with other browsers, we highly recommend that you only use these browsers on your system when you work with the EC.

Important:

- To prevent automatic updates to the Firefox ESR browser, you must change your update preferences. See *Turn Off Firefox ESR Automatic Updates* (next in this document) for instructions.
- You must enable Java in the browser to be able to view the Performance Monitoring graph.

Turn Off Firefox ESR Automatic Updates

- 1 Open the Firefox ESR 24 browser.
- 2 Click **Tools > Options** to open the Options window.
- 3 Click **Advanced**.
- 4 Click the **Update** tab.
- 5 Under the Firefox updates section, click either the **Check for updates, but let me choose whether to install them** or the **Never check for updates** option.
- 6 Click **OK**.

Known Issues

At the time of this release, there are no known issues.

Network Element Dependencies

The following network elements must be at the listed minimum versions prior to the upgrade to SR 8.0:

- GQAM: 4.2.2
- MQAM: 2.6.19
- Netcrypt: 1.2.12
- QAM (UniQAM): 2.5.3
- QPSK: G09
- GoQAM: 1.1.3

Site Requirements

This section provides information to help you prepare for the upgrade to SR 8.0. Please read this entire section before you upgrade.

For more information, please visit the Bug Toolkit to view a list of pertinent change requests. This list is updated regularly. For more information, see *Bug Search Tool* (on page 12).

Notes:

- The Bug Search Tool website is under password control. If necessary, contact the representative who handles your account for instructions.
- You may also need to upgrade your Solaris operating system and install VMware. See the installation document for this system release for more information.

If you have questions or would like to order our products, please contact Cisco Services.

Upgrade Logistics

Introduction

This section contains information that can help system operators plan an upgrade to SR 8.0.

Time to Complete

The entire upgrade to SR 8.0 must be completed within a single maintenance window that usually starts around midnight. A few pre-upgrade procedures, consisting mainly of system checks, backups, and various operations upon the metadevices of the DNCS, can be completed *before* the maintenance window begins.

Cisco engineers have determined that a typical site can be upgraded within one maintenance window. See *Scheduling Requirements* (on page 10) for additional details.

Supported Upgrade Path

Note these important upgrade requirements:

- To perform the software upgrade, the EC must currently be operating at one of the following releases:
 - DNCS SR 4.2.0.x SP4
 - DNCS SR 4.3.x.x
 - DNCS SR 5.0.x.x
 - DNCS SR 5.1.x.x

Site Requirements

- EC SR 6.0
- EC SR 7.0
- For upgrade instructions, refer to the *Installation and Upgrade Guide for System Release 7.0* (part number OL-31614). Rollback procedures and software are also provided in the event that the upgrade is unsuccessful.

System Performance Impact

Interactive services will not be available during portions of the maintenance window.

EC and Application Server Hardware Platforms

Introduction

This section describes the hardware configurations that are supported by SR 8.0.

Running the Doctor Report

- 1 If necessary, open an xterm window on the EC and log in as dncs user.
- 2 Type `cd /dvs/dncs/Utilities/doctor` and then press **Enter**. The `/dvs/dncs/Utilities/doctor` directory becomes the working directory.
- 3 Type `doctor` and press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report. Each parameter causes the Doctor Report to generate output with specific configuration information.



```
Kdncs:dncs > cd /dvs/dncs/Utilities/doctor/
Kdncs:doctor > doctor

= Doctor package version =
./doctor -agestobindhcn: I ud l on
./doctor [-c<number>]

a - (almost) All options (except q and x)
g - General Info: INCS info, installed software info, INCS and
  App Server disk utilization, INCS and App Server swap space,
  database utilizations, database extents, load averages, INCS
  and App Server debug flags, tracing levels, INCS and App
  Server processes, INCS and App Server corefiles, DNS, check
  force time for valid service, dncs license check, large log file check
  INCS install options
e - Element Info: DHCT state summary, DHCT type summary, active
  elements, mod slot tolerance, source, source definitions,
  sessions, subscription packages, EMIc expiring soon.
s - SI Info: SI_INSERT_RATE, system time message, distinguished
  SI QRM, SI out of band interval.
t - Time Info: INCS and App Server time sync, timezone, BST.
p - PPV Info: PPV services and events, PPV and SMI service
  discrepancies, event use services, PPV files, phoneactivetime,
  EUT, GBRMs.
b - BFS Info: BFS carousels, BFS sessions, BFS source definitions.
i - IPC Info: IPC collector, IPC data files.
n - Ping Elements: QPSK Ethernet, QPSK RF, QRM, NETCRYPT, BIG, TED.
q - Check for quarantined qans and ping elements.
  This option is NOT included in all (-a).
x - Check one-to-one correspondence of DHCTs and serial numbers.
  This option is NOT included in all (-a).
v - Verbose mode: Detailed output, even if OK.
d - Suppress screen output. Write to output file only.
h - Generate this help text.
u - Clean up (delete) all but the last <number> doctor reports.
  Use this switch independently of all others. Report NOT GENERATED.

n = and one of the following options:
hubcmList - list what hub are associated to which QMls
smgInfo - list SMG (Stream/M Dajitter Group) and respective QGM
sdbgInfo - list SDB Service Group Mini Carousel Info
genericQmInfo - display generic QMls and IPs
dialbeqcmInfo - display generic QMls and IPs
sdbInfo - display SDB server info and status
pegInfo - display PCDs info and status

One or more of the a, g, e, s, t, p, b, i, n, c, x or q options is required.
d and v are optional but should be used with a required option.
Option order is irrelevant.

Note the q option must be explicitly chosen. It can be time consuming.
The q option automatically sets the v (verbose) option and pings and checks rpc bind for qans.
Kdncs:doctor > █
```

- 4 Type `doctor -g` and press **Enter** to view the version of EC software installed and the EC and Application Server platform, CPU, and disk information.

What to Verify Using the Doctor Report

Using the results of the Doctor Report, verify that your system meets the following requirements.

For detailed information on reading the data in the Doctor Report, see the *DBDS Utilities Version 6.6 Installation Instructions and User Guide* (part number OL-32256).

System Release Required

In the Doctor Report, look for one of the following entries under the **All SAI Installed Package Information** section.

- For SR 7.0 and earlier, look for **SAIdncs**
- For SR 8.0 and later, look for **CSCOec**

Make sure the **SAIdncs** version is at one of the following releases:

- DNCS SR 4.2.0.x SP4
- DNCS SR 4.3.x.x
- DNCS SR 5.0.x.x
- DNCS SR 5.1.x.x
- EC SR 6.0
- EC SR 7.0

If you have installed Service Packs for your system release, your version may include additional characters.

Hardware Configurations

Ensure your site meets the following hardware requirements before upgrading to SR 8.0. The following table lists the minimum requirements for the EC hardware platform that is supported by SR 8.0.

EC Server Platform	Hard Drive Configuration	Memory	Processor	Ports
Cisco UCS C240 M3	16 x 300 GB	128 GB RAM	2 x 2.90 GHz	12 x 1 GB

Important: The minimum number of servers for an EC installation is one; however, Cisco strongly recommends that you install two servers for all production installations (for failover and database replication purposes).

Scheduling Requirements


With the live upgrade, your site only needs to be down for 2 to 3 hours during the entire upgrade process. Most of the upgrade procedures have no system impact. The pre-install and pre-upgrade steps can be performed at any time of day. However, the actual upgrade process normally takes place during a maintenance window beginning at midnight. The following table provides a breakdown of each upgrade process.

Process	Length of Time	Activity	Impact
Pre-install	1-3 hours	Activities are performed by Cisco Services, including checking the overall health of the system.	These activities do not impact the system.
Pre-upgrade	3-4 hours	Backing up the system: <ul style="list-style-type: none"> ■ Configure the EC components ■ Back up the DNCS and Application Server files ■ Complete system checks 	These activities do not impact the system.
Upgrade	8-10 hours total; 2-3 of these hours require system outage Note: Actual time may vary based on the number of devices being upgraded.	Upgrade the DBDS network: <ul style="list-style-type: none"> ■ Back up the DNCS database ■ Install the EC software ■ Enable additional features (licensed or unlicensed) needed as a result of this upgrade Note: Sites planning to use an RFGW to carry GigE BFS will need to enable GQI QAM support. ■ Install and download the component software (QAM, MQAM, GQAM, GQI-based QAM, and QPSK modulator) ■ Complete functional checks 	QPSK modulator upgrades and some QAM, MQAM, and GQAM upgrades can be completed with little or no subscriber impact. For 2 to 3 hours during the database migration portion of the upgrade, the DNCS and EC will be down. Broadcast video services will remain active but set-tops will not be able to boot or receive BFS and other data from the DNCS/EC until the migration is completed and the system is activated.
Post-Upgrade	3-4 hours	Back up the system: <ul style="list-style-type: none"> ■ Back up the file system ■ Back up the EC database 	These activities do not impact the system.
Secondary EC Configuration	3-4 hours 2-4 hours	Configure the secondary EC <ul style="list-style-type: none"> ■ Configure RepDb between the primary and secondary ECs ■ Allow the primary and secondary ECs to synchronize 	These activities do not impact the system.

Software Configuration

View Installed Software Versions

To view the versions of software installed with SR 8.0:

- 1 Click the navigation menu () . The EC main menu opens.
- 2 Click **Utilities > Installed Software Versions**. A table opens that lists all the software packages and their versions installed as part of this release.

Bug Search Tool

The Bug Search Tool is an online tool that allows registered users to search for bugs by release or by a bug number.

To log on to the Bug Search Tool, go to <https://tools.cisco.com/bugsearch> and log on with your user name and password. The Bug Search Tool page opens.

Note: If you have not set up an account on www.cisco.com, click **Register Now** and follow the on-screen instructions to register.

Search for Bugs in This Release

- 1 In the product type-in field (to the right of the product drop-down list), type **DNCS System Release 6.0**. Then choose **DNCS System Release 6.0** from the list that appears. (Do *not* press **Enter**.)
- 2 In the Releases field, type **8.0** and press **Enter**. The Bug Search Tool displays the list of bugs for this release. You can use the filters to restrict the bugs that you want to view.
- 3 If you want to view a specific bug, enter the ID of the bug that you want to view in the **Search For** field and press **Enter**.

For Information

If You Have Questions

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



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

678 277-1120
800 553-6387
www.cisco.com

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.

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)

Product and service availability are subject to change without notice.

© 2017 Cisco and/or its affiliates. All rights reserved.

January 2017

Part Number TP-00141-01