



DTACS 5.2 Release Notes

Overview

Introduction

These release notes describe the Digital Transport Adapter Control System (DTACS) version 5.2 software release. The DTACS controls subscriber DTA boxes that convert digital signals to analog for analog TVs. The DTACS is installed adjacent to the EC (Explorer Controller) and provides provisioning of basic and extended services, Entitlement Control Message Generator (ECMG) devices, code downloads, package support, Emergency Alert System (EAS), and Authorization Management Messages (AMMs) for DTA authorization.

These release notes contain the following information:

- New feature descriptions
- Media and software versions for this release
- Site Requirements
- Descriptions of implemented and open BRs (Bug Reports)
- General information on contacting Cisco® Services

Purpose

The purpose of this release note is to inform system administrators of the new features, feature enhancements and software fixes associated with DTACS 5.2.

Scope

This release note provides an executive overview of DTACS 5.2. If you have questions or need detailed information about the release, 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.

Highlights

This section describes the new feature introduced in DTACS 5.2.

DTACS Monitoring

DTACS 5.2 includes a new feature referred to as DTACS Monitoring. When this feature is enabled, the nbiAgent process will be installed on the DTACS server. NBI (North Bound Interface) will monitor the DTACS and generate SNMP traps when a status change occurs for processes managed by dtacsInitd. It will then forward the trap to an external SNMP-based NMS. On receiving traps, NMS then translates the TRAP OID and OBJECTS OID into the names defined in the MIB.

DTACS operators can enable/disable this feature using the .ADF script.

Browser Requirements

DTACS 5.2 has been tested and verified against the Mozilla Firefox Extended Support Release (ESR) version 52.1 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 DTACS 5.2.

Known Issues

There are no known issues at the time of this release.

Site Requirements

This section provides information to help you prepare for the upgrade to DTACS 5.2. Read the 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 10).

Note: The Bug Search Tool website is under password control. If necessary, contact the representative who handles your account for instructions.

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 DTACS 5.2.

Time to Complete

The entire upgrade to DTACS 5.2 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 of the DTACS, 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 7), for additional details.

Supported Migration Path

To perform the software migration, the DTACS must currently be operating at DTACS 5.0 or DTACS 4.1.

Note: Refer to the *DTACS 5.2 Installation and Migration Guide* for upgrade instructions from DTACS 5.0/4.1 to DTACS 5.2. Rollback procedures are also provided in the event the upgrade is unsuccessful.

System Performance Impact

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

DTACS Server Hardware Platforms

Introduction

This section describes the hardware that is supported by DTACS 5.2.

DTACS Hardware Configuration

Ensure that your site meets the following DTACS hardware requirements before upgrading to DTACS 5.2.

- Cisco UCS C240 M3
- Cisco UCS C240 M4

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 the 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	<ul style="list-style-type: none"> ■ Backing up the system ■ Backup DTACS components ■ Backup DTACS server files ■ Complete system checks 	These activities do not impact the system.
Upgrade	6-8 hours total: 2-3 hours require system outage Note: Actual time may vary based on the number of devices being upgraded	<ul style="list-style-type: none"> ■ Upgrade DBDS network ■ Backup DTACS database ■ Install DTACS software ■ Determine which optional features (licenses or unlicensed) need enabled ■ Reboot hardware ■ Complete functional tasks 	2-3 hours of the upgrade require system outage

Site Requirements

Process	Length of Time	Activity	Impact
Post-Upgrade	3-4 hours	<ul style="list-style-type: none">■ Backup the system■ Backup database & key files	These activities do not impact the system.

Software Configuration

View Installed Software Versions

Complete the following steps to view the versions of software installed with DTACS 5.2.

- 1 Click the **Navigation** menu (). The DTACS 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 From a Web browser, go to <https://tools.cisco.com/bugsearch/>.
- 2 On the **Log In** screen, enter your registered cisco.com User Name and Password. Then click **Log In**. The Bug Search Tool window displays.
Note: If you do not have a cisco.com account, click **Register Now** from the Create A New Account area of the window.
- 3 To search for bugs in the current release, execute one of the following options:
 - a From the **Search For** field, enter a specific bug ID and press **Enter**. Information for the bug is displayed.
 - b To search for bugs in the current release, specify the following criteria:
 - i From the **Product** dropdown list box, select **Series/Model**.
 - ii In the adjacent text box, enter **Cisco DTA Control System (DTACS)**.
 - iii From the **Releases** dropdown list, select an appropriate option and then in the adjacent text box, enter **5.2**.
 - iv From the **Filter** options — define custom criteria for an advanced search by selecting an appropriate value from the dropdown lists by choosing either one Filter or multiple filters from the available categories. After each selection, the results page will automatically load below the filters pane. If you select multiple filters, it behaves like an AND condition
 - **Modified Date** — select one of these options to filter bugs: Last Week, Last 30 days, Last 6 months, Last year, or All
 - **Status** — select Fixed, Open, Other, or Terminated.
 - Select **Fixed** to view fixed bugs. To filter fixed bugs, uncheck the **Fixed** check box and select the appropriate option (Resolved or Verified) that appears below the Fixed check box.
 - Select **Open** to view all open bugs. To filter the open bugs, uncheck the Open check box and select the appropriate options that appear below the Open check box.
 - Select **Other** to view any bugs that are duplicates of another bug.
 - Select **Terminated** to view terminated bugs. To filter terminated bugs, uncheck the Terminated check box and select the appropriate sub-option (Closed, Junked, or Unreproducible) that appears below the Terminated check box. Select multiple options as required.

- **Severity** — select the severity level:
 - 1: Catastrophic
 - 2: Severe
 - 3: Moderate
 - 4: Minor
 - 5: Cosmetic
 - 6: Enhancement
 - **Rating** — select the bug's quality rating: 5 Stars (excellent), 4 or more Stars (good), 3 or more Stars (medium), 2 or more Stars (moderate), 1 or more Stars (poor), or No Stars
 - **Support Cases** — select whether the bug Has Support Cases or No Support Cases
 - **Bug Type** — select whether the bug is Employee Visible & Customer Visible or Customer Visible Only.
- c The Bug Search tool displays the list of bugs based on the specified search criteria. You can save or email the current search by clicking their respective option.
- 4 If you have any problems using the Bug Search tool, log into the Technical Support website at <http://www.cisco.com/cisco/web/support/index.html> or contact the Cisco Technical Assistance Center (TAC).

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.

© 2018 Cisco and/or its affiliates. All rights reserved.

December 2018