



Cisco ATA 191 Analog Telephone Adapter Release Notes for Firmware Release 12.0(1)SR3

First Published: 2020-11-17

Release Notes

These release notes support the Cisco 191 Analog Telephone Adapter (ATA) running Firmware Release 12.0(1)SR3.

The following table lists the support and protocol compatibility for the Cisco ATA 191.

Table 1: Cisco ATA 191, Support, and Firmware Release Compatibility

Cisco IP Phone	Protocol	Support Requirements
Cisco ATA 191	SIP	Cisco Unified Communications Manager 10.5(1) and later Cisco Unified Communications Manager DST Olsen version D or later
Cisco ATA 191	SIP	CME 12.6

Related Documentation

Use the following sections to obtain related information.

Cisco Unified Communications Manager Documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html>

Cisco Unified Communications Manager Express Documentation

See the Cisco Unified Communications Manager Express publications that are specific to your Cisco Unified Communications Manager Express release. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html>

Cisco ATA 190 Series Documentation

Refer to publications that are specific to your language and call control system. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/products/unified-communications/ata-190-series-analog-telephone-adapters/index.html>

User Guide Accessibility

The *Cisco ATA 191 User Guide for Cisco Unified Communications Manager* is accessible for people with limited sight or who are blind. The HTML version of the document is now compatible with the Job Access With Speech (JAWS) reader, so visually impaired users can access information about their device.

Where to Find More Information

- *Cisco ATA 191 User Guide for Cisco Unified Communications Manager*

Installation

Installation Requirements

Before you install the firmware release, you must ensure that your Cisco Unified Communications Manager (Unified CM) is running the latest device pack. After you install a device pack on the Unified CM servers in the cluster, you need to reboot all the servers.



Note If your Unified CM doesn't have the required device pack to support this firmware release, the firmware may not work correctly.

For information on the Unified CM Device Packs, see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html.

Install the Firmware Release on Cisco Unified Communications Manager

Before you use the Cisco Analog Telephone Adapter with Cisco Unified Communications Manager 10.5, or higher, you must install the latest firmware on all Cisco Unified Communications Manager servers in the cluster.

Besides Cisco Unified Communications Manager, the Cisco ATA 191 can also work with Cisco Unified Communications Manager Express and Cisco Unified Survivable Remote Site Telephony (SRST). Refer to the [Related Documentation, on page 1](#) section for more information.

Procedure

-
- Step 1** Go to the following URL:
<https://software.cisco.com/download/navigator.html?mdfid=268437683&flowid=77852>
 - Step 2** Choose **ATA 190 Series Analog Telephone Adapters > ATA 191 Analog Telephone Adapter**.
 - Step 3** In the Latest Releases folder, choose **12.0.1 SR3**.
 - Step 4** Select **cmterm-ata191.12-0-1-0301-002.k3.cop.sgn** firmware, click the Download or Add to cart button, and follow the prompts.
 - Step 5** Click the + next to the firmware file name in the Download Cart section to access additional information about this file. The hyperlink for the readme file is in the Additional Information section, which contains installation instructions for the corresponding firmware.

- Step 6** Follow the instructions in the readme file to install the firmware.
-

Install the Firmware Zip Files

Before you use the Cisco Analog Telephone Adapter with Cisco Unified Communications Manager 10.5, or higher, you must install the latest firmware on all Cisco Unified Communications Manager servers in the cluster.

Besides Cisco Unified Communications Manager, the Cisco ATA 191 can also work with Cisco Unified Communications Manager Express and Cisco Unified Survivable Remote Site Telephony (SRST). Refer to the [Related Documentation, on page 1](#) section for more information.

Procedure

- Step 1** Go to the following URL:
<https://software.cisco.com/download/navigator.html?mdfid=268437683&flowid=77852>
- Step 2** Choose **ATA 190 Series Analog Telephone Adapters > ATA 191 Analog Telephone Adapter**.
- Step 3** In the Latest Releases folder, choose **12.0.1 SR3**.
- Step 4** Select **cmterm-ata191.12-0-1-0301-002.zip** firmware, click the Download or Add to cart button, and follow the prompts.
- Step 5** Click the + next to the firmware file name in the Download Cart section to access additional information about this file. The hyperlink for the readme file is in the Additional Information section, which contains installation instructions for the corresponding firmware.
- Step 6** Follow the instructions in the readme file to install the firmware.
-

Limitations and Restrictions

Manufacturing Installed Certificate Signature and SHA-256 Support

The manufacturing installed certificate(MIC) signature has been updated from SHA-128 with RSA to SHA-256 with RSA. You must update and install the new SHA-2 certificates on the Cisco Unified Communications Manager for secure mode to function. You can download the new certificate from <http://www.cisco.com/security/pki/certs/cmca2.cer>.

All applications that authenticate the phone MIC should update the MIC, including the following:

- Cisco Unified Communications Manager
- Cisco Unified Survivable Remote Site Telephony
- Cisco Secure Access Control System
- Cisco Identity Services Engine

For additional information about SHA-2 use and support, see *Security Guide for Cisco Unified Communications Manager* (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>).

Phone Behavior During Times of Network Congestion

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack

Caveats

This section describes the resolved and open caveats, and provides information on accessing the Cisco Software Bug Toolkit.

View Caveats

You can search for caveats using the Cisco Bug Search.

Known caveats (bugs) are graded according to severity level, and can be either open or resolved.

Before you begin

To view caveats, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure

-
- Step 1** Perform one of the following actions:
- Use this URL for all caveats: [https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319456&rls=12.0\(1\)SR3&sb=anfr&sts=fd&svr=3nH&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319456&rls=12.0(1)SR3&sb=anfr&sts=fd&svr=3nH&bt=custV)
 - Use this URL for open caveats: [https://bst.cloudapps.cisco.com/bugsearch/search?kw=Customer%20visible%20bug%20for%20ATA191%2012.0\(1\)SR3&pf=prdNm&pfVal=286319456&sb=null&sts=open&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=Customer%20visible%20bug%20for%20ATA191%2012.0(1)SR3&pf=prdNm&pfVal=286319456&sb=null&sts=open&bt=custV)
 - Use this URL for resolved caveats: [https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319456&rls=12.0\(1\)SR3&sb=fr&sts=fd&svr=3nH&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319456&rls=12.0(1)SR3&sb=fr&sts=fd&svr=3nH&bt=custV)
- Step 2** When prompted, log in with your Cisco.com user ID and password.
- Step 3** (Optional) Enter the bug ID number in the Search for field, then press **Enter**.
-

Open Caveats

The following lists shows the severity 1, 2, and 3 defects that are open for the Cisco ATA 191 Analog Telephone Adapter Firmware Release 12.0(1)SR3.

For more information about an individual defect, access the Bug Search toolkit and search for the defect using the Identifier. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, the table reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit as described in [Access Cisco Bug Search, on page 5](#).

There are no open caveats in this release.

Resolved Caveats

The following list shows the severity 1, 2, and 3 defects that are resolved for the Cisco ATA 191 Analog Telephone Adapter Release Firmware Release 12.0(1)SR3.

For more information about an individual defect, access the Bug Search toolkit and search for the defect using the Identifier. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, the table reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit as described in [Access Cisco Bug Search, on page 5](#).

- CSCvr15504 ATA 191 plays voicemail stutter tone when Audible Message Waiting Indicator (AMWI) is off
- CSCvr10149 Support unique ATA hostname in DHCP option 12
- CSCvs12983 ATA191 fails to respond to simultaneous incoming SIP INVITE
- CSCvs13002 ATA191 may not get its configuration if there is a delay in receiving an IP address
- CSCvv86958 Add LED indication for RESET button factory reset case
- CSCvv86951 ATA191 will do unregister when dhcp renew hostname change
- CSCvv86940 ATA191 Message Waiting Indicator (MWI) not functioning on analog phones
- CSCvw22353 ATA191 need to support HTTP provision for CUCM configuration files
- CSCvq23763 Evaluation of ATA 191 for TCP SACK vulnerabilities
- CSCvs38055 CVE-2019-5482: Heap buffer overflow in the TFTP protocol handler in cURL 7.19.4 to 7.65.3
- CSCvs38052 CVE-2019-11190: Linux bypass ASLR on setuid programs vulnerability
- CSCvs38051 CVE-2019-10638: Linux hash collisions vulnerability
- CSCvs38050 CVE-2019-15214: Linux use-after-free vulnerability in the sound
- CSCvs38047 CVE-2019-15916: Linux memory leak register_queue_kobjects
- CSCvs38046 CVE-2018-17972: Linux kernel proc_pid_stack function Vulnerability
- CSCvw30147 ATA191 cannot auto register after receiving 503 service unavailable on cucm12.5
- CSCvw30155 ATA191 doesn't support HTTP auto firmware upgrade

Access Cisco Bug Search

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of the following:

- All severity level 1 or 2 bugs

- Significant severity level 3 bugs

You can search for problems by using Cisco Bug Search.

Before you begin

To access Cisco Bug Search, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure

- Step 1** To access Cisco Bug Search, go to:
<https://tools.cisco.com/bugsearch>
- Step 2** Log in with your Cisco.com user ID and password.
- Step 3** To look for information about a specific problem, enter the bug ID number in the Search for field, then press **Enter**.
-

Cisco IP Phone Firmware Support Policy

For information on the support policy for phones, see <https://cisco.com/go/phonefirmwaresupport>.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.