Cisco ATA 191 and 192 Analog Telephone Adapter Multiplatform Phones Release Notes for Firmware Release 11.1(0)

First Published: 2018-02-05

Last Modified: 2018-04-03

Introduction

These release notes support the Cisco ATA 191 and 192 Analog Telephone Adapter Multiplatform Phones running SIP Firmware Release 11.1(0).

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

Table 1: Cisco IP Phones, Support, and Firmware Release Compatibility

Cisco IP Phone	Protocol	Support Requirements
Cisco ATA 191 and 192	SIP	BroadSoft BroadWorks 21.0 Asterisk 13.1

Related Documentation

Use the following sections to obtain related information.

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

New and Changed Features

The following sections describe the features that are new or have changed in this release.

Cisco ATA 191 and 192 Analogue Telephone Adapter

The Cisco ATA 191 and 192 Analog Telephone Adapter allow you to turn an analogue phone or fax communication devices into an IP phone. With these devices, you can retain your investment in your current equipment, but also benefit from an IP-based telephony network.

The ATA 191 and 192 support many of the current telephony features, including shared lines, conferencing, and voicemail. Both devices have two images or partitions in permanent storage, which allows the device to recover if the initial image is corrupted. With the dedicated Problem Report Tool button, you can quickly and easily collect troubleshooting information.

The Cisco ATA 191 and 192 both support IPv6, and SSH.

The ATA 191 and 192 easily integrate into your current network. Both devices have two RJ11 ports, each with a phone number. Both ATA devices have a RJ45 port that provides access to an Ethernet network. The Cisco ATA 192 has a RJ45 port for LAN use.

Basic network configuration can be done through an IVR system, and you use a web interface to monitor logs, view device information or do advanced configurations.

Where to Find More Information

- *Cisco ATA 191 and ATA 192 Analog Telephone Adapter Administration Guide for MultiPlatform Firmware*
- *Cisco ATA 191 and ATA 192 Analog Telephone Adapter User Guide for MultiPlatform Firmware*

Installation

Upgrade Firmware

The Cisco ATA 191 and 192 support dual image upgrades by TFTP, HTTP, or HTTPS.

Step 1 Go to the following URL:
http://software.cisco.com/download/navigator.html?mdfid=284883944&i=rm

Step 2 Choose **Cisco ATA 190 Series**.

Step 3 Choose your ATA model.

Step 4 In the Latest Releases folder, choose **11.1(0)**.

Step 5 Download the file ATA19x.11-1-0MPP-23.zip.

Step 6 Unzip the files.

Step 7 Put the files on the tftp/http/https download directory.

Step 8 Configure the Upgrade Rule on the **Provisioning** tab in the web page with the valid URL. The format is:
`<schema>://<serv_ip[:port]>/filepath/ATA19x.11-1-0MPP-23.img`

Here is an example,

http://10.74.10.225/firmware/ATA19x.11-1-0MPP-23.img

Note The loads file is put in the file path of the above url. The zip file contains other file types also. Only the loads file is used in the above URL.

After the firmware upgrade completes, the phone reboots automatically.

Caveats

View Caveat

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

Step 1 Perform one of the following actions:

- Use this URL for all open caveats:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319456&sb=anfr&sts=open&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**.

Limitations and Restrictions

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone voice and video quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

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

Caller Identification and Other Phone Functions

Caller identification or other phone functions have not been verified with third-party applications for the visually or hearing impaired.

Cisco IP Phone Firmware Support Policy

For information on the support policy for phones, see http://www.cisco.com/c/en/us/support/docs/collaboration-endpoints/unified-ip-phone-7900-series/116684-technote-ipphone-00.html.

Documentation, Service Requests, and Additional Information

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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 NONINFRINGEMENT 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.

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/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. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.