



Cisco ATA 191 Analog Telephone Adapter Administration Guide for Cisco Unified Communications Manager

First Published: 2017-11-22

Last Modified: 2024-02-23

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

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)

© 2024 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Cisco ATA 191 Analog Telephone Adapter Overview 1

Your Analog Telephone Adapter	1
Session Initiation Protocol	1
SIP Capabilities	2
SIP Components	2
Cisco ATA 191 Hardware	4
ATA 191 Top Panel	4
ATA 191 Back Panel	6
Software Features	7
Secure Real-Time Transport Protocol	7
Fax Passthrough	7
Transport Layer Security Protocol	7
T.38 Fax Relay	7
Supported Voice Codecs	8
Other Supported Protocols	8
Supported SIP Services	8
Supported Call Services	9
802.1X Authentication	10
Modem Standards	10
Fax Services	11
Supported Methods	11
Supported ATA Call Features	12
Installation and Configuration Overview	12

CHAPTER 2

Prepare to Install the ATA 191 on Your Network 13

Interactions with Other Cisco Unified IP Communications Products	13
--	----

- Interaction with Cisco Unified Communications Manager 13
- Power Guidelines 14
- Power Outage 14
- Phone Configuration Files 14
- ATA 191 Startup Process 15
- Start up Process with Standby Image 16
- Addition of the ATA 191 to the Cisco Unified CM Database 16
 - Addition with Autoregistration 17
 - Addition with Cisco Unified Communications Manager Administration 17
- Determine the MAC Address of the ATA 18

CHAPTER 3

- Install the ATA 191 19**
 - ATA 191 Installation Information 19
 - Network Requirements 19
 - Safety Recommendations 19
 - Package Contents 20
 - Install Your Cisco ATA 20
 - Attach a Phone to the ATA 191 21
 - Startup Process Verification 21
 - Configure Startup Network Settings 21
 - Security on the ATA 191 22

CHAPTER 4

- Configure the ATA 191 23**
 - Telephony Features 23
 - Product-Specific Configuration Parameters 28
 - Add Users to Cisco Unified Communications Manager 34
 - Emergency Call Support Background 34
 - Emergency Call Support Terminology 35
 - Configure the ATA to Make Emergency Calls 35

CHAPTER 5

- Configure Fax Services 37**
 - Fax Services 37
 - Fax Mode 37
 - Fax Modem Standards 38

Fax Modem Speeds 38

CHAPTER 6

Troubleshoot and Maintenance 41

Configure Syslog Reports 41

Practice 43

Turn On Debug flag for Media or SIP 43

Resolve Startup Problems 44

The ATA 191 Does Not Register with Cisco Unified Communications Manager 44

Check Network Connectivity 44

Verify TFTP Server Settings 45

Verify DNS Settings 45

Verify Cisco Unified Communications Manager Settings 45

Cisco Unified Communications Manager and TFTP Services Are Not Running 45

Create a New Configuration File 46

Search for the ATA in Cisco Unified Communications Manager 47

ATA 191 Unable to Obtain IP Address 47

ATA 191 Resets Unexpectedly 48

Verify the Physical Connection 48

Identify Intermittent Network Outages 48

Verify DHCP Settings 49

Check Static IP Address Settings 49

Verify Voice VLAN Configuration 49

Eliminate DNS or Other Connectivity Errors 49

Troubleshoot ATA 191 Security 50

General Troubleshooting Tips 51

Problem Report Tool 52

Configure a Customer Support Upload URL 52

Generate a Problem Report 53

Clean the ATA 191 54

CHAPTER 7

ATA 191 Specifications 55

Physical Specifications 55

Electrical Specifications 56

Environmental Specifications 56

Physical Interfaces 56
 Ringing Characteristics 57
 Software Specifications 57
 SIP Compliance Reference Information 59

CHAPTER 8

Voice Menu Codes 61

Access the IVR and Configure Your ATA Settings 61
 IVR Tips 62
 IVR Configuration Menu Options 62

CHAPTER 9

ATA 191 Country-Specific Tones and Cadences 65

ATA 191 Country-Specific Tones and Cadences 65
 Mechanism 65
 Link a Tone File with a Device 65
 Tone Configuration 66



CHAPTER 1

Cisco ATA 191 Analog Telephone Adapter Overview

- [Your Analog Telephone Adapter, on page 1](#)

Your Analog Telephone Adapter

The ATA 191 analog telephone adapter is a telephony-device-to-Ethernet adapter that allows regular analog phones to operate on IP-based telephony networks. The ATA 191 supports two voice ports, each with an independent phone number. The ATA 191 also has an RJ-45 10/100BASE-T data port.

Figure 1: Cisco Analog Telephone Adapter



Session Initiation Protocol

Session Initiation Protocol (SIP) is the Internet Engineering Task Force (IETF) standard for real-time calls and conferencing over Internet Protocol (IP). SIP is an ASCII-based, application-layer control protocol (defined in RFC3261). It is used to establish, maintain, and terminate multimedia sessions or calls between two or more endpoints.

Like other Voice over IP (VoIP) protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management is used to control the attributes of an end-to-end call.



Note SIP for the ATA 191 is compliant with RFC2543.

SIP Capabilities

Session Initiation Protocol (SIP) provides these capabilities:

- Determines the availability of the target endpoint. If the target endpoint is unavailable, SIP determines whether the called party is already on the phone or didn't answer in the allotted number of rings. SIP then returns a message indicating why the target endpoint was unavailable.
- Determines the location of the target endpoint. SIP supports address resolution, name mapping, and call redirection.
- Determines the media capabilities of the target endpoint. Using the Session Description Protocol (SDP), SIP determines the lowest level of common services between endpoints. Conferences are established using only the media capabilities that all endpoints support.
- Establishes a session between the originating and target endpoint. If the call can be completed, SIP establishes a session between the endpoints. SIP also supports midcall changes, such as adding another endpoint to the conference or changing the media characteristic or codec.
- Handles the transfer and termination of calls. SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP establishes a session between the transferee and a new endpoint (specified by the transferring party). SIP also terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties. Conferences can consist of two or more users and can be established using multicast or multiple unicast sessions.

SIP Components

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function in one of these roles:

- User agent client (UAC)—A client application that initiates the SIP request.
- User agent server (UAS)—A server application that contacts the user when a SIP request is received and returns a response on behalf of the user.

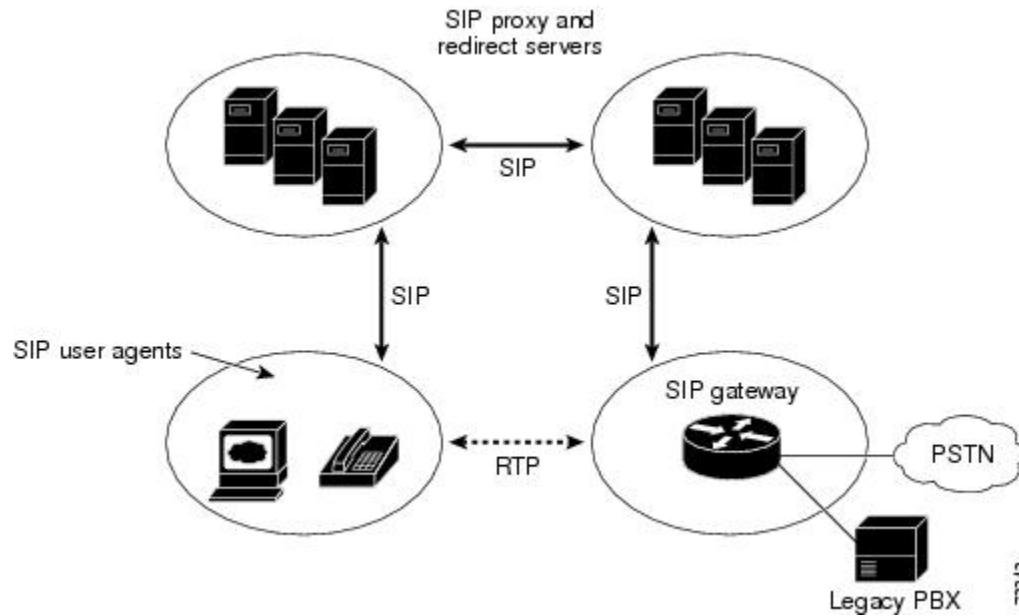
Typically, a SIP endpoint is capable of functioning as both a UAC and a UAS, but functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request.

From an architectural standpoint, the physical components of a SIP network can also be grouped into two categories—Clients and servers. The following figure shows the architecture of a SIP network.



Note SIP servers can interact with other application services, such as Lightweight Directory Access Protocol (LDAP) servers, a database application, or an extensible markup language (XML) application. These application services provide back-end services such as directory, authentication, and billable services.

Figure 2: SIP Architecture



SIP Clients

SIP clients include:

- Gateways—Provide call control. Gateways provide many services, the most common being a translation function between SIP conferencing endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway also translates between audio and video codecs and performs call setup and clearing on both the LAN side and the switched-circuit network side.
- Phones—Can act as either a UAS or UAC. The ATA 191 can initiate SIP requests and respond to requests.

SIP Servers

SIP servers include:

- Proxy server—The proxy server is an intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. Proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
- Redirect server—Receives SIP requests, strips out the address in the request, checks its address tables for any other addresses that may be mapped to the address in the request, and then returns the results of the address mapping to the client. Redirect servers provide the client with information about the next hop or hops that a message should take, then the client contacts the next hop server or UAS directly.
- Registrar server—Processes requests from UACs for registration of their current location. Registrar servers are often colocated with a redirect or proxy server.

Cisco ATA 191 Hardware

The ATA 191 and ATA 192 are compact, easy to install devices.

The unit provides these connectors:

- 5V DC power connector.
- Two RJ-11 FXS (Foreign Exchange Station) ports—Your ATA has two RJ-11 ports that work with any standard analog phone device. Each port supports either voice calls or fax sessions, and both ports can be used simultaneously.
- One WAN network port—An RJ-45 10/100BASE-T data port to connect an Ethernet-capable device to the network.

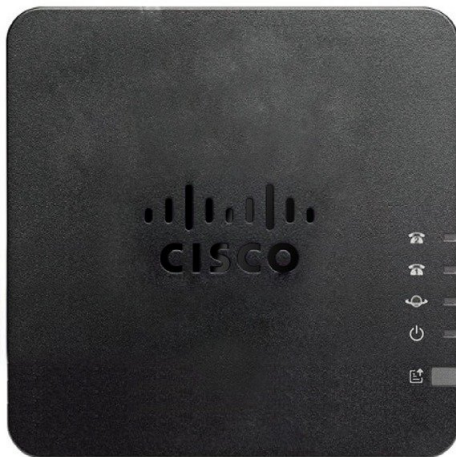


Note The ATA network port performs autonegotiation for duplex and speed. It supports speeds of 10/100Mbps and full-duplex.

ATA 191 Top Panel





The top panel of your ATA has several LEDs that are used to show the device's status.

Figure 3: ATA 191 Top Panel



The following table describes the LEDs located on your ATA.

Table 1: ATA 191 Top Panel Items

Item	Description
Power LED 	<p>Steady green: System booted up successfully and is ready for use.</p> <p>Slow flashing green: System is booting up.</p> <p>Fast flashing green three times, then repeats: System failed to boot up.</p> <p>Fast flashing green: The LED behaviour occurs in the following situations:</p> <ul style="list-style-type: none"> • System detects a factory reset. <p>To perform a factory reset, press and hold the RESET button for about 10 seconds.</p> <ul style="list-style-type: none"> • A factory reset is performed successfully. <p>Off: Power is off.</p>
Network LED 	<p>Flashing green: Data transmission or reception is in progress through the WAN port.</p> <p>Off: No link.</p>
Phone 1 LED Phone 2 LED 	<p>Steady green: On hook.</p> <p>Slow flashing green: Off hook.</p> <p>Fast flashing green three times, then repeats: The analog device failed to register.</p> <p>Fast flashing green: A factory reset is performed successfully.</p> <p>Off: The port is not configured.</p>
Problem Report Tool (PRT) Button	<p>Press this button to create a problem report using the Problem Report Tool.</p> <p>Note This is not a power button. When you press this button, a problem report is generated and uploaded to a server for the system administrator.</p>
Problem Report Tool (PRT) LED 	<p>Flashing amber: The PRT is preparing the data for the problem report.</p> <p>Fast Flashing amber: The PRT is sending the problem report log to the PRT server.</p> <p>Solid green for five seconds, then off: The PRT report was sent successfully.</p> <p>Fast flashing green: A factory reset is performed successfully.</p> <p>Flashing red: The PRT report failed. Press the PRT button to turn the LED off. Once it is off, another press triggers a new PRT report.</p>

Problem Report Tool Button

The Problem Report Tool (PRT) button is on the ATA top panel. Press the PRT button, and a log file is prepared and uploaded to the server for troubleshooting your network.

You can instruct your analog phone users to press the PRT button on the ATA device to start the PRT log file process.

One of the following must be completed to upload the PRT log file from the ATA:

- Set up the HTTP server to upload the PRT log file from the ATA.
- Configure the customer support upload URL to best suit your needs, and apply it to the ATA.

Related Topics

[Problem Report Tool](#), on page 52

ATA 191 Back Panel

The back panel of your ATA has several ports used to connect your device and to power it. The back panel also has the reset button for resetting the device to the factory settings.

Figure 4: ATA 191 Back Panel



The following table describes the ports that are located on the back panel of your ATA.

Table 2: ATA 191 Back Panel Ports

Port or Button	Description
RESET	To restart the ATA, use a paper clip or similar object to press this button briefly. To restore the factory default settings, press and hold for 10 seconds. The LED behaviour for the factory reset: <ol style="list-style-type: none"> 1. After you press and hold the button for about 10 seconds, the Power LED is fast flashing green. 2. After the factory reset is performed successfully, all LEDs are fast flashing green for about 5 seconds.
PHONE 1	Use an RJ-11 phone cable to connect an analog phone or fax machine.
PHONE 2	Use an RJ-11 phone cable to connect a second analog phone or fax machine.
NETWORK	Use an Ethernet cable to connect to the network.

Port or Button	Description
DC 5V POWER	Use the provided power adapter to connect to a power source.

Software Features

The ATA 191 supports these protocols, services, and methods:

- [Secure Real-Time Transport Protocol, on page 7](#)
- [Fax Passthrough, on page 7](#)
- [Transport Layer Security Protocol, on page 7](#)
- [T.38 Fax Relay, on page 7](#)
- [Supported Voice Codecs, on page 8](#)
- [Other Supported Protocols, on page 8](#)
- [Supported SIP Services, on page 8](#)
- [Modem Standards, on page 10](#)
- [Fax Services, on page 11](#)
- [Supported Methods, on page 11](#)
- [Supported ATA Call Features, on page 12](#)

Secure Real-Time Transport Protocol

Secure Real-Time Transport Protocol secures voice conversations on the network and provides protection against replay attacks.

Fax Passthrough

Name Signaling Event (NSE)-based and re-INVITE-based passthrough provide transport of fax communications using the G.711a/u codec.

Transport Layer Security Protocol

Transport Layer Security (TLS) is a cryptographic protocol that secures data communications such as email on the Internet. TLS is functionally equivalent to Secure Sockets Layer (SSL).

T.38 Fax Relay

The T.38 fax relay feature enables devices to use fax machines to send files over the IP network. In general, when a fax is received, it is converted to an image, then sent to the T.38 fax device. When the target T.38 fax device receives this image, the device converts the image back to an analog fax signal.

T.38 fax relays configured with voice gateways decode or demodulate the fax signals before they are transported over IP. With the SIP call control protocol, the Session Description Protocol (SDP) entries in the initial SIP INVITE message indicate that T.38 fax relay is present. After the initial SIP INVITE message, the call is

established to switch from voice mode to T.38 mode. Cisco Unified Communications Administration allows you to configure a SIP profile that supports T.38 fax communication.

The ATA 191 only supports T38 Fax Relay Version 0 (G3).

Supported Voice Codecs

The ATA 191 supports these voice codecs:

- G.711 mu-law
- G.711 A-law
- G.729a
- G.729ab

Check your other network devices for the codecs they support.

Other Supported Protocols

The ATA supports these additional protocols:

- 802.1Q VLAN tagging
- Cisco Discovery Protocol (CDP)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP) v4 and IPv6
- Link Layer Discovery Protocol (LLDP)
- Secure Real-Time Transport Protocol (SRTP)
- Transmission Control Protocol (TCP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)
- Transport Layer Security (TLS)
- Secure Socket Shell (SSH)
- Network Time Protocol (NTP)
- HyperText Transfer Protocol (HTTP)

Supported SIP Services

The following SIP services are supported on the ATA:

- IP address assignment—DHCP-provided or statically configured
- ATA 191 configuration by Cisco Unified Communications Manager configuration interface

- VLAN configuration
- Cisco Discovery Protocol (CDP)
- Low-bit-rate codec selection
- User authentication
- Configurable tones (ringback tone, reorder tone, dialing tone, outside dialing tone, busy tone, call waiting tone)
- Dial plan and PLAR
- SIP Proxy Server redundancy
- Privacy features
- User-configurable, call waiting, permanent default setting
- Comfort noise during silent period when using G.711u/a and G.729ab
- Caller ID format
- Ring frequency/voltage adjustment
- Hookflash detection timing configuration
- Type of Service (ToS) configuration for audio and signaling Ethernet packets
- Debugging and diagnostic tools

Supported Call Services

The following call services are supported on the ATA:

- IP address assignment—DHCP-provided or statically configured
- ATA191 configuration by Cisco Unified Communications Manager configuration interface
- VLAN configuration
- Cisco Discovery Protocol (CDP)
- Low-bit-rate codec selection
- User authentication
- Configurable tones (ringback tone, reorder tone, dialing tone, outside dialing tone, busy tone, call waiting tone)
- Dial plan and PLAR
- SIP Proxy Server redundancy
- Privacy features
- User-configurable, call waiting, permanent default setting
- Comfort noise during silent period when using G.711u/a and G.729ab
- Caller ID format

- Ring frequency/voltage adjustment
- Hookflash detection timing configuration
- Type of Service (ToS) configuration for audio and signaling Ethernet packets
- Debugging and diagnostic tools

802.1X Authentication

Support for 802.1X authentication requires several components:

- The ATA 191: The ATA initiates the request to access the network. The ATA contains an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of ATAs to the LAN switch ports. The current release of the ATA 802.1X supplicant uses the EAP-FAST and EAP-TLS options for network authentication.
- Cisco Secure Access Control Server (ACS) (or other third-party authentication server): The authentication server and the ATA must both be configured with a shared secret that authenticates the ATA.
- A LAN switch supporting 802.1X: The switch acts as the authenticator and pass the messages between the ATA and the authentication server. After the exchange completes, the switch grants or denies the ATA access to the network.

You must perform the following actions to configure 802.1X.

- Configure the other components before you enable 802.1X authentication on the ATA.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
 - Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
 - Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.



Note Currently, the ATA doesn't support the IPv6 network access through 802.1X authentication.

To check the status of the 802.1X authentication, use one of the following methods:

- On the ATA web page, go to **Status > Network Status > 802.1x authentication information**.
- On the phone connected to the ATA, use IVR number 803.

Modem Standards

The ATA supports these modem standards:

- V.90
- V.92
- V.44

- K56Flex
- ITU-T V.34 Annex 12
- ITU-T V.34
- V.32bis
- V.32
- V.21
- V.22
- V.23

Fax Services

The ATA 191 supports two modes of fax services:

- Fax pass-through mode: Receiver-side Called Station Identification (CED) tone detection with automatic G.711A-law or G.711 μ -law switching.
- T.38 Fax Relay mode: The T.38 fax relay feature enables devices to use fax machines to send files over the IP network. In general, when a fax is received, it is converted to an image, then sent to the T.38 fax device. When the target T.38 fax device receives this image, the device converts the image back to an analog fax signal. T.38 fax relays configured with voice gateways decode or demodulate the fax signals before they are transported over IP.



Note Success of fax transmission depends on network conditions and fax modem response to these conditions. The network must have reasonably low network jitter, network delay, and packet loss rate.

Related Topics

[Configure Fax Services](#) , on page 37

Supported Methods

The ATA 191 supports these methods:

- REGISTER
- REFER
- INVITE
- BYE
- CANCEL
- NOTIFY
- OPTIONS
- ACK
- SUBSCRIBE

For more information, see RFC3261, SIP: Session Initiation Protocol.

Supported ATA Call Features

SIP supplementary services are services that you can use to enhance your phone service.

The ATA supports these SIP supplementary services:

- Caller ID
- Call-waiting caller ID
- Voice mail indication
- Making a conference call
- Call waiting
- Call forwarding
- Calling-line identification
- Unattended transfer
- Attended transfer
- Shared Line
- SpeedDial
- Meet-Me Conference
- Call Pickup/Group Call Pickup
- Redial
- Secure Call
- C-Barge

Installation and Configuration Overview

The following basic steps are required to install and configure the ATA. The steps also make the ATA operational in a typical SIP environment where many ATAs are deployed.

1. Plan the network and the ATA configuration.
2. Install the Ethernet connection.
3. Install and configure the other network devices.
4. Install the ATA but do not power it up yet.
5. Power up the ATA.

Related Topics

[Prepare to Install the ATA 191 on Your Network](#) , on page 13

[Install the ATA 191](#) , on page 19



CHAPTER 2

Prepare to Install the ATA 191 on Your Network

- Interactions with Other Cisco Unified IP Communications Products, on page 13
- Power Guidelines, on page 14
- Power Outage, on page 14
- Phone Configuration Files, on page 14
- ATA 191 Startup Process, on page 15
- Start up Process with Standby Image, on page 16
- Addition of the ATA 191 to the Cisco Unified CM Database, on page 16
- Determine the MAC Address of the ATA, on page 18

Interactions with Other Cisco Unified IP Communications Products

The ATA 191 enables you to communicate using voice over a data network. To provide this capability, the ATA 191 depends upon and interacts with several other key Cisco Unified IP Telephony and Network components, including Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, media resources, and so on.

To function in the IP telephony network, the ATA 191 must be connected to a networking device, such as a Cisco Catalyst switch. You must also register the ATA 191 with a Cisco Unified Communications Manager system before you can send and receive calls.

For related information about voice and IP communications, see this URL:

<https://www.cisco.com/c/en/us/products/unified-communications/index.html>

Interaction with Cisco Unified Communications Manager

Cisco Unified Communications Manager is an open industry-standard call process system. Cisco Unified Communications Manager software sets up and tears down calls between analog phones that are connected to the ATA, and thus integrates traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system: the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

- Firmware for devices

- Authentication and encryption (if configured for the telephony system)
- Configuration and CTL files via the TFTP service
- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager

For information about configuring Cisco Unified Communications Manager to work with the IP devices described in this chapter, see *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*, *System Configuration Guide for Cisco Unified Communications Manager*, and *Security Guide for Cisco Unified Communications Manager*.

Power Guidelines

The ATA is powered with external power. External power is provided through a separate power supply.

The following power type and guideline applies to external power for the ATA:

- Power Type—External power (provided through the Universal AC external power supply).
- Guidelines—The ATA uses the Universal AC power supply 100/240V.

Related Topics

[Electrical Specifications](#), on page 56

Power Outage

Your accessibility to emergency service through the phone depends the phone being powered. If there is an interruption in the power supply, Service and Emergency Calling Service dialing will not function until power is restored. In the case of a power failure or disruption, you may need to reset or reconfigure equipment before using the Service or Emergency Calling Service dialing.

Phone Configuration Files

Configuration files for a phone are stored on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. When you make a change in Cisco Unified Communications Manager that requires the ATA 191 line to be reset, the phone configuration file is automatically updated. If a system reset or restart is required, both lines must reset or restart at the same time.

Configuration files also contain information about which image load the ATA 191 should be running. If this image load differs from the one currently loaded on an ATA 191, the phone contacts the TFTP server to request the required load files. These files are digitally signed to ensure the authenticity of the file source.

If the device security mode in the configuration file is set to Authenticated and the CTL file on the ATA 191 has a valid certificate for Cisco Unified Communications Manager, the phone establishes a TLS connection to Cisco Unified Communications Manager. Otherwise, the ATA 191 establishes a TCP/UDP connection. You can go to **Voice > Line > SIP Settings** on the ATA 191 web GUI, where the SIP Transport should correspond to the transport type in the Phone Security Profile in Cisco Unified Communications Manager.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file contains sensitive information. To ensure the privacy of a configuration file, configure it for encryption. For detailed information, see the “Encrypted Phone Configuration Setup” chapter of the *Security Guide for Cisco Unified Communications Manager* at:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

If the ATA 191 has registered before, the ATA 191 accesses the configuration file named `ATA<mac_address>.cnf.xml`, where `mac_address` is the MAC address of the phone. If the ATA 191 cannot access that configuration file, then it accesses the default XML `Default.cnf.xml` configuration file.

If autoregistration is not enabled and you did not add the ATA 191 to the Cisco Unified Communications Manager database, the ATA 191 does not attempt to register with Cisco Unified Communications Manager.

For the ATA 191, the TFTP server generates these SIP configuration files:

- SIP IP Phone:
 - For unsigned and unencrypted files—`ATA<mac>.cnf.xml`
 - For signed files—`ATA<mac>.cnf.xml.sgn`
 - For signed and encrypted files—`ATA<mac>.cnf.xml.enc.sgn`

The filenames are derived from the MAC Address in the Phone Configuration window of Cisco Unified Communications Manager Administration. The MAC address uniquely identifies the phone. For more information, see the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*.

For more information about how the phone interacts with the TFTP server, see the “Configure TFTP Servers” chapter of the *System Configuration Guide for Cisco Unified Communications Manager* at:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>

ATA 191 Startup Process

When the ATA 191 connects to the VoIP network, it goes through a standard startup process. Depending on your specific network configuration, not all these process steps may occur on your ATA.

Table 3: ATA 191 Startup Process

Task		Related Topics
1	Obtaining power. The ATA 191 uses external power.	See Power Guidelines , on page 14 .
2	Loading the Stored Image. The Cisco ATA 191 has nonvolatile flash memory in which it stores firmware images and user-defined preferences. At startup, the ATA 191 runs a bootstrap loader that loads an ATA 191 image stored in flash memory. Using this image, the ATA 191 initializes its software and hardware.	

Task		Related Topics
3	<p>Obtaining an IP Address.</p> <p>If the Cisco ATA 191 is using DHCP to obtain an IP address, the device queries the DHCP server to obtain one. If you are not using DHCP in your network, assign static IP addresses to each device locally.</p>	
4	<p>Requesting the CTL file.</p> <p>The TFTP server stores the CTL file. This file contains the certificates necessary for establishing a secure connection between the device and Cisco Unified Communications Manager.</p>	<p>See the “Cisco CTL Client Setup” chapter <i>Security Guide for Cisco Unified Communications Manager</i> at: http://www.cisco.com/cisco/en/products/voice/ata/docs/secure/ata_secure_setup.html</p>
5	<p>Requesting the Configuration File.</p> <p>The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the ATA 191.</p>	See Phone Configuration Files , on page 14
6	<p>Contacting Cisco Unified Communications Manager.</p> <p>The configuration file defines how the ATA 191 communicates with Cisco Unified Communications Manager and provides a device with its load ID. After obtaining the file from the TFTP server, the device attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list. If the device is configured for secure signaling (encrypted or authenticated), and the Cisco Unified Communications Manager is set to Mixed (security) mode, the device makes a TLS connection. Otherwise, it makes a nonsecure TCP/UDP connection.</p>	See Phone Configuration Files , on page 14

Start up Process with Standby Image

The ATA 191 has two images or partitions in permanent storage. The second image allows the device to recover if the initial image is corrupted.

Press the PRT button when the power is on, and you switch to the standby partition. Startup is similar to the normal process, except that the LED for Phone 2 flashes amber indicating that the second partition is being used.

Related Topics

[Startup Process Verification](#), on page 21

Addition of the ATA 191 to the Cisco Unified CM Database

Before you install the ATA 191, choose a method for adding the devices to the Cisco Unified Communications Manager database.

The following table provides an overview of these methods for adding the ATA 191 to the Cisco Unified Communications Manager database.

Table 4: Add the ATA to the Cisco Unified Communications Manager Database

Method	Requires MAC Address?	Notes
Autoregistration	No	Results in automatic assignment of directory numbers. Not available when mixed mode is enabled.
Using the Cisco Unified Communications Manager Administration	Yes	Requires phones to be added individually.

Addition with Autoregistration

By enabling autoregistration before you begin installing the ATA 191, you can:

- Automatically add devices without first gathering MAC addresses from the ATA 191.
- Automatically add an ATA 191 to the Cisco Unified Communications Manager database when you physically connect the phone to your IP telephony network. During autoregistration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone.
- To change any settings, quickly enter devices into the Cisco Unified Communications Manager database and modify settings, such as directory numbers, from Cisco Unified Communications Manager.
- Move autoregistered devices to new locations and assign them to different device pools without affecting their directory numbers.



Note Support exists for autoregistration for several devices in the Unified CM at the same time.

Autoregistration is disabled by default. Sometimes, you may not want to use autoregistration. For example, if you want to assign a specific directory number to the phone or if you plan to use secure connection with Cisco Unified Communications Manager. For information about enabling autoregistration, see the Enabling Auto-Registration in the *Cisco Unified Communications Manager Administration Guide*.



Note For mixed mode, autoregistration is automatically disabled and cannot be changed. For nonsecure mode, autoregistration is disabled by default but can be enabled manually.

Addition with Cisco Unified Communications Manager Administration

You can add the ATA 191 individually to the Cisco Unified Communications Manager database using Cisco Unified Communications Manager Administration. To do so, first obtain the MAC address for each device.

After you have collected MAC addresses, in Cisco Unified Communications Manager Administration, choose **Device > Phone** and click **Add New** to begin.



Note The ATA 191 has two FXS ports, and each port has its own MAC address. The first ATA 191 port uses the MAC address and the second ATA 191 port uses the shifted MAC address (example, AABBCCDDEEFF to BBCCDDEEFF01). You can add two devices (either an analog phone or a fax machine) from the Unified CM administration page.

For complete instructions and conceptual information about Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*.

Determine the MAC Address of the ATA

Procedure

Choose one of the following methods to determine the MAC address:

- Look at the MAC label on the back of the ATA.
- Go to **Voice > Information** on the web page of the device and check the MAC address.



CHAPTER 3

Install the ATA 191

- [ATA 191 Installation Information, on page 19](#)
- [Network Requirements, on page 19](#)
- [Safety Recommendations, on page 19](#)
- [Package Contents, on page 20](#)
- [Install Your Cisco ATA , on page 20](#)
- [Attach a Phone to the ATA 191, on page 21](#)
- [Startup Process Verification, on page 21](#)
- [Configure Startup Network Settings, on page 21](#)
- [Security on the ATA 191, on page 22](#)

ATA 191 Installation Information

You connect the ATA 191 hardware and configure the ATA 191 by loading the QED and firmware files. Install the QED file first, then install the firmware file. For more information about loading the QED and firmware files, see the "Installation Notes" section of the "Release Notes for Cisco ATA 191 Analog Telephone Adapter".

Network Requirements

The ATA 191 acts as an endpoint on an IP telephony network. The following equipment is required:

- Call Control system
- Voice packet gateway—Required if you are connecting to the Public Switched Telephone Network (PSTN). A gateway is not required if an analog key system is in effect.
- Ethernet connection

Safety Recommendations

To ensure general safety, follow these guidelines:

- Do not get this product wet or pour liquids into this device.

- Do not open or disassemble this product.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Use only the power supply that comes with the ATA.
- Ultimate disposal of this product should be handled according to all national laws and regulations.
- Read the installation instructions before you connect the system to its power source.
- The plug-socket combination must always be accessible because it serves as the main disconnecting device.
- Do not work on the system or connect or disconnect cables during periods of lightning activity.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

For translated warnings, see the *Regulatory Compliance and Safety Information for the Cisco ATA 191* document.

Package Contents

The ATA 191 package contains the following items:

- Cisco ATA 191 Analog Telephone Adapter
- Regulatory Compliance and Safety Information for the ATA 191
- 5V power adapter with appropriate country clip
- Ethernet cable



Note The ATA is intended for use only with the 5V DC power adapter that comes with the unit.

Install Your Cisco ATA

You can use either Category 3/5/5e/6 cabling for 10-Mbps connections, but you must use Category 5/5e/6 for 100-Mbps connections.

Procedure

- Step 1** Connect the power supply to the Cisco DC Adapter port.
- Step 2** Connect a straight-through Ethernet cable from the network to the network port on the ATA. Each ATA ships with one Ethernet cable in the box.
-

Attach a Phone to the ATA 191

Before you begin

You can attach one or two phones to an ATA 191.

Procedure

Connect one or more phones to a phone port of the ATA with an RJ11 cable.

The PHONE1 and PHONE2 LEDs on the ATA light as solid green when there is activity on that port.

Startup Process Verification

After your ATA has power connected to it, it begins the startup process by cycling through these steps:

1. The Power LED flashes during the startup process.
2. The Problem Report Tool (PRT) LED lights solid amber during initial bootup. The LED then flashes amber and then green while the application and kernel are booting.
If the PRT LED lights red during bootup, then either the MIC certificate failed, or the ATA failed to obtain a network address.
3. The LED for Phone 1 flashes while the Phone1 port boots, followed by the LED for Phone 2.
After the Phone1 and Phone2 ports register with Cisco Unified CM successfully, the corresponding LEDs are lit with solid green. If a phone port fails to register, the LED rapidly flashes in green three times, then repeats.
4. When the ATA has successfully booted, the Power LED lights solid green and the PRT LED turns off. The Network LED flashes as traffic is detected.

When you go offhook on the phone, the phone LED begins to flash, and you hear the dial tone. The ATA has completed the startup process.

Related Topics

[Start up Process with Standby Image](#), on page 16

Configure Startup Network Settings

Before you begin

Perform this configuration if you are not using DHCP in your network.

Procedure

- Step 1** Configure these network settings on the ATA after you install the device on the network:
- IP subnet information (subnet mask and gateway)
 - TFTP server IP address
- Step 2** Configure these optional settings as necessary:
- Administration VLAN ID
- Step 3** Collect this information.
-

Security on the ATA 191

Security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified Communications Manager server, and digitally sign files before they are delivered.

For more information about the security features, see the *Security Guide for Cisco Unified Communications Manager*.

You can start the installation of a Locally Significant Certificate (LSC) on the device profile from Cisco Unified Communications Manager. Use the **Device > Phone > Phone Configuration** menu option. You can also use this menu option to update or remove an LSC.

Before you begin, make sure that the appropriate Cisco Unified Communications Manager and the CAPF security configurations are complete:

- On Cisco Unified Communications Operating System Administration, verify that the CAPF certificate has been installed.
- The CAPF is running and configured.

See the *Security Guide for Cisco Unified Communications Manager* for more information.



CHAPTER 4

Configure the ATA 191

- [Telephony Features](#), on page 23
- [Product-Specific Configuration Parameters](#), on page 28
- [Add Users to Cisco Unified Communications Manager](#), on page 34
- [Emergency Call Support Background](#), on page 34

Telephony Features

The following table lists the supported telephony features. Use Cisco Unified Communications Manager Administration to configure many of these features.

Table 5: Telephony Features for the ATA 191

Feature	Description	Configuration Reference
Audible Message Waiting Indicator	<p>A stutter tone from the handset or speakerphone indicates that a user has one or more new voice messages on a line.</p> <p>Note The stutter tone is line-specific. You hear it only when using the line with the waiting messages.</p>	<p>For more information, refer to</p> <ul style="list-style-type: none"> • <i>Administration Guide for Cisco Unified Communications Manager</i>, “IM and Presence Service Overview” chapter • <i>System Configuration Guide for Cisco Unified Communications Manager</i>, “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide for Cisco Unified Communications Manager</i>, “Audible Message Waiting” chapter

Feature	Description	Configuration Reference
cBarge	<p>Allows a user to join a nonprivate call on a shared phone line. cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features.</p> <p>Your ATA supports Barge on a conference bridge.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>System Configuration Guide Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide Unified Communications Manager</i> “Barge” chapter
Call forward	<p>Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, and Call Forward No Answer.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>System Configuration Guide Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide Unified Communications Manager</i> “Call Forwarding” chapter
Call pickup	<p>Allows users to redirect a call that is ringing on another phone within their pickup group to their phone.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Feature Configuration Guide Unified Communications Manager</i> “Call Pickup” chapter
Call waiting	<p>Indicates (and allows users to answer) an incoming call that rings while on another call. Displays incoming call information on the phone screen.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>System Configuration Guide Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter
Caller ID	<p>Displays caller identification such as a phone number, name, or other descriptive text on the phone screen.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>System Configuration Guide Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Administration Guide for Cisco Unified Communications Manager IM and Presence Service and Presence Service</i>, Cisco Unified Phone Configurations.

Feature	Description	Configuration Reference
Conference	<ul style="list-style-type: none"> • Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Adhoc Conference, cBarge, and Meet-Me. • Allows a noninitiator in a standard (ad hoc) conference to add or remove participants. 	For more information, refer to <ul style="list-style-type: none"> • <i>System Configuration Guide for Cisco Unified Communications Manager</i>, “Configure Analog Telephony Adapters” chapter • <i>Feature Configuration Guide for Cisco Unified Communications Manager</i>, “Conferencing Features” chapter
Direct transfer	Allows users to connect two calls to each other (without remaining on the line).	For more information, refer to <ul style="list-style-type: none"> • <i>System Configuration Guide for Cisco Unified Communications Manager</i>, “Configure Analog Telephony Adapters” chapter • <i>Feature Configuration Guide for Cisco Unified Communications Manager</i>, “Call Transfer” chapter
Forced authorization codes (FAC)	Controls the types of calls that certain users can place.	For more information, refer to <ul style="list-style-type: none"> • <i>System Configuration Guide for Cisco Unified Communications Manager</i>, “Configure Analog Telephony Adapters” chapter • <i>Feature Configuration Guide for Cisco Unified Communications Manager</i>, “Speed Dial and Abbreviated Numbers” chapter
Group call pickup	Allows a user to answer a call that is ringing on a directory number in another group.	For more information, refer to <ul style="list-style-type: none"> • <i>System Configuration Guide for Cisco Unified Communications Manager</i>, “Configure Analog Telephony Adapters” chapter • <i>Feature Configuration Guide for Cisco Unified Communications Manager</i>, “Call Pickup” chapter

Feature	Description	Configuration Reference
Hold/Resume	<p>Allows the user to move a connected call between an active state and a held state.</p> <p>Note No support for resuming a call from a shared line party.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>System Configuration Guide Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide Unified Communications Manager</i> “Secure Tone” chapter
Meet–Me conference	<p>Allows a user to host a Meet-Me conference in which other participants call a predetermined number at a scheduled time.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>System Configuration Guide Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide Unified Communications Manager</i> “Meet-Me Conferencing” chapter
Message Waiting	<p>Defines directory numbers for message-waiting on and message-waiting off indicator. A directly connected voice-messaging system uses the specified directory number to set or to clear a message-waiting indication for a particular Cisco Unified IP Phone.</p>	<p>For more information refer to:</p> <ul style="list-style-type: none"> • <i>System Configuration Guide Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide Unified Communications Manager</i> “Audible Message Waiting” chapter
Music on hold	<p>Plays music while callers are on hold.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>System Configuration Guide Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide Unified Communications Manager</i> “Music On Hold” chapter

Feature	Description	Configuration Reference
Privacy	Prevents users who share a line from adding themselves to a call.	For more information refer to <ul style="list-style-type: none"> • <i>System Configuration Guide for Cisco Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide for Cisco Unified Communications Manager</i> “Privacy” chapter
Redial	Allows users to call the most recently dialed phone number by pressing the *# feature code.	Requires no configuration.
Shared line	Allows a user to have several devices that share the same phone number or allows a user to share a phone number with a coworker.	For more information, refer to <ul style="list-style-type: none"> • <i>System Configuration Guide for Cisco Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide for Cisco Unified Communications Manager</i> “Manager Assistant” chapter
Speed dialing	Allows users to speed dial a phone number by entering * and an assigned index code (1 to 199) on the phone keypad. Example: Press *199 to dial the phone number with index code 199. Users assign index codes on Line configuration from the Cisco Unified Communications Manager Device window.	For more information, refer to <ul style="list-style-type: none"> • <i>System Configuration Guide for Cisco Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter • <i>Feature Configuration Guide for Cisco Unified Communications Manager</i> “Speed Dial and Abbreviated Numbers” chapter
Time Zone Update	Updates the device with time zone changes.	For more information, refer to <ul style="list-style-type: none"> • <i>System Guide for Cisco Unified Communications Manager</i> “Analog Telephone Adapter” chapter
Voice-messaging system	Enables callers to leave messages if calls are unanswered.	For more information refer to <ul style="list-style-type: none"> • <i>System Configuration Guide for Cisco Unified Communications Manager</i> “Configure Analog Telephone Adapters” chapter

Product-Specific Configuration Parameters

Cisco Unified Communications Manager Administration allows you to set some product-specific configuration parameters for the ATA 191. The following table lists the configuration windows and their paths to configure the parameters.

Table 6: Configuration Information

Configuration Window	Path
Phone Configuration window	Device > Phone ; Product Specific Configuration portion of window

The following table lists the configuration parameters you can set using Cisco Unified Communications Manager Administration. You can set the configuration parameters using the Phone configuration window. Options with an asterisk in the window are required.



Note Set the following ATA 191 parameters from port 1 only: IVR Password, CDP, Impedance, Input/Output Audio Level, Timers, Call Sequence, Ring1 Cadence, Ring2 Cadence, CPC Delay, CPC Duration, and MTU Size. Setting these parameters from port 2 has no effect.

Table 7: Product-Specific Configuration Parameters for the ATA 191

Parameter	Description
Line 2 Support	Enable and disable the Phone 2 port on the ATA 191. Default: Enabled
Web Access	Enable the ATA 191 to accept web connections or an HTTP client. If this option is disabled, then access to the ATA 191's internal web page is blocked. In addition, the Problem Report Tool (PRT) is disabled. Default: Disabled
HTTPS Server	Enable both HTTPS and HTTP connections to the ATA 191, or restrict connections to HTTPS only. Default: HTTPS and HTTP
Admin Password*	Set the password to access the Web Administrator interface. The password can be from 8 to 127 characters.
SSH Access	Set whether the ATA 191 accepts SSH connections. If you block SSH connections, then access to the ATA 191 is blocked. Default: Disabled
Cisco Discovery Protocol (CDP)	Enable or disable the CDP function of the ATA 191. Default: Enabled

Parameter	Description
Link Layer Discovery Protocol (LLDP)	Enable or disable LLDP on the ATA 191. Default: Enabled
LLDP Asset ID	Set the Asset ID from LLDP. The maximum length is 32.
802.1x Authentication	Enable or disable the 802.1x authentication. Default: User Controlled If the parameter is set to User Controlled, the feature is disabled on the ATA. User needs to enable it through the IVR setting on the phone that is connected to the ATA. For other values (Enabled or Disabled), the setting in CUCM takes preference.
Log Server	If using IPv4, specify an IP address and port of a remote system where log messages are sent.
IPv6 Log Server	If using IPv6, specify an IP address and port of a remote system where log messages are sent.
Remote Log	Specify where to send the log data by serviceability. If enabled, log data is copied to the location specified by the Log Server or IPv6 Log Server parameters. If disabled, log data is not copied to the log server location. Default: Disabled

Parameter	Description
Log Profile	<p>Run the pre-defined debug command remotely:</p> <ul style="list-style-type: none"> • Default—Resets the debug level to default. • Preset—Use log module settings on Phone Adapter Configuration Utility for debug flags. • Telephony—Turn on debug flag for provisioning (including auto upgrade) and call features. • SIP—Turn on debug flag for SIP messages. • UI—Turn on debug flag for key event such as DTMF, PRT, and reset button. • Network—Turn on debug flag for network events, such as DHCP, VLAN, link status change. • Media—Turn on debug flags for RTP, Fax, Tone, and SLIC-related issues. • System—Turn on debug flag for system events, such as reboot, or factory reset. • Web—Turn on debug flag for web operation and event logs. • NTP—Turn on debug flag for NTP related logs. • CDPLLD—Turn on debug flag for CDP and LLDP logs. • Security—Turn on debug flag for security related logs.
Customer support upload URL	Provides the URL for the Problem Report Tool (PRT).
Load Server	If using IPv4, the ATA uses an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server.
IPv6 Load Server	If using IPv6, the ATA uses an alternate server to obtain firmware loads and upgrades, rather than the defined TFTP server.
Auto Barge	Auto Barge adds a user to an active call. An offhook phone automatically adds the user (initiator) to the shared line call (target), and the users currently on the call receive a tone (if configured). Barge supports conference bridges.
Echo Cancellation	Enable or Disable the use of echo canceler.

Parameter	Description
Fax Mode	<p>The Cisco ATA 191 supports these fax modes:</p> <ul style="list-style-type: none"> • Fax Pass-Through—Allows fax and modem traffic to pass through a voice port using the re-INVITE method (codec can be g711ulaw or g711alaw). • NSE Fax Pass-through g711ulaw—Allows fax traffic to pass through a voice port using the NSE method by codec g711ulaw. • NSE Fax Pass-through g711alaw—Allows fax traffic to pass through a voice port using the NSE method by codec g711alaw. • T.38 Fax Relay—Allows for a quicker protocol for fax transmission over packet networks.
Fax Error Correction Mode Override	<p>You can set the fax error correction mode override values to one of the following settings:</p> <ul style="list-style-type: none"> • Default • On • Off
FAX Disable ECAN	Set this parameter to yes to automatically disable Echo Canceler when FAX tone is detected.
Modem Line	If you set this parameter to yes , the call is treated as a modem call. The ATA191 tunes VAD, Jitter buffer, and echo canceler automatically.
Fax T38 Return To Voice	Set this parameter yes if voice callback is needed after the T.38 fax is completed.
Fax Tone Detect Mode	<p>This option controls which side detects fax tone (trigger fax):</p> <ul style="list-style-type: none"> • Caller Or Callee • Caller Only • Callee Only <p>The default is Caller Or Callee.</p>
IVR Password	ATA 191 IVR password.
Input Audio Level	Gain value of Network-to-Phone
Output Audio Level	Gain value of Phone-to-Network
Impedance	The ATA 191 provides multiple impedance values, such as 600ohm for use in the United States.

Parameter	Description
Caller Connect Polarity	Control the line polarity of the Cisco ATA FXS ports when Cisco ATA is the caller and a call is connected. Default: User forward polarity
Caller Disconnect Polarity	Control the line polarity of the Cisco ATA FXS ports when Cisco ATA is the caller and a call is disconnected. Default: User forward polarity
Callee Connect Polarity	Control the line polarity of the Cisco ATA FXS ports when Cisco ATA is the callee and a call is connected. Default: User forward polarity
Callee Disconnect Polarity	Control the line polarity of the Cisco ATA FXS ports when Cisco ATA is the callee and a call is disconnected. Default: User forward polarity
Caller ID	<ul style="list-style-type: none"> • BT FSK • Bellcore FSK • ETSI FSK
Call Sequence	<ul style="list-style-type: none"> • Bellcore FSK • ETSI FSK
Mute Progress Tone	Set this parameter to On to mute all progress tones on the Cisco ATA 191 during call establishment. Default setting: Off.
Ring1 Cadence	Cadence script for distinctive ring pattern. Default setting: 60(2/4).
Ring2 Cadence	Cadence script for the alternative ring pattern triggered by SIP message. Default setting: 60(.8/.4,.8/4).
CPC Delay (0-255s)	CPC(Calling Party Control) delay time in seconds after caller hangs up when the ATA 191 starts removing the tip-and-ring voltage to the attached equipment of the called party. Note When remote party hangs up, without CPC enabled, reorder tone will be played after a configurable delay. If CPC is enabled, dial tone will be played when tip-to-ring voltage is restored. Value range: 0–255(s). Default setting: 2(s)

Parameter	Description
CPC Duration (0-1.000s)	<p>CPC(Calling Party Control) duration time in seconds for which the tip-to-ring voltage is removed after the caller hangs up. After that, the tip-to-ring voltage is restored and dial tone will apply if the attached equipment is still off hook. CPC is disabled if this value is set to 0.</p> <p>Note When remote party hangs up, without CPC enabled, reorder tone will be played after a configurable delay. If CPC is enabled, dial tone will be played when tip-to-ring voltage is restored.</p> <p>Value range: 0-1.000(s). Default setting: 0(s)</p>
MTU Size (576-1500)	<p>Maximum Transmission Unit (MTU) size that can be communicated in a single network layer transaction. For IPv4 only mode case, the MTU size can be set from 576 to 1500; for dual mode case, the MTU size can be set from 1281 to 1500.</p> <p>Value range: 576–1500 Default setting: 1500</p>
Ring and Call Waiting Tone Specs	
Ring Waveform	<p>Waveform for the ringing signal.</p> <p>Choices are Sinusoid or Trapezoid.</p> <p>Default setting: Trapezoid.</p>
Ring Frequency(15-50Hz)	<p>Frequency of the ringing signal.</p> <p>Value range: 15-50 (Hz). Default setting: 20.</p>
Ring Voltage(60-90V)	<p>Voltage of the ringing signal.</p> <p>Value range: 60-90 (V). Default setting: 85.</p>
Timers	
Offhook Validation Timer (50-1000ms)	Indicates the time to validate an offhook event.
Onhook Validation Timer (50-1000ms)	Indicates the time to validate an onhook event.
Hookflash Timer (100 to 1500ms)	Indicates the time to validate a hookflash event.

Parameter	Description
Onhook Delay Timer (0 to 155ms)	Indicates the time to delay an onhook event.
Reorder Delay (0-30s)	Delay after far end hangs up before reorder tone is played.
RTP Packet Time (10-90ms)	Packet size in milliseconds for RTP. Default setting: 20.

You can access the ATA 191 web page and perform limited configuration. In Admin mode, most information and settings are available.

Add Users to Cisco Unified Communications Manager

Adding users to Cisco Unified Communications Manager allows you to display and maintain information about users. Each added user can perform these tasks:

- Access the corporate directory and other customized directories from an ATA 191.
- Create a personal directory.
- Set up speed dial and call forwarding numbers.
- Subscribe to services that are accessible from an ATA 191.

You can add users to Cisco Unified Communications Manager using this method:

- To add users individually, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Refer to the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* for more information about adding users. Refer to the *System Configuration Guide for Cisco Unified Communications Manager* for details about the user information.

Emergency Call Support Background

Emergency call service providers can register an ATA's location for each IP-based phone in a company. The location information server (LIS) transfers the emergency response location (ERL) to the ATA. The ATA stores its location during registration, after the ATA restarts. The location entry can specify the street address, building number, floor, room, and other office location information.

When you place an emergency call, the ATA transfers the location to the call server. The call server forwards the call and the location to the emergency call service provider. The emergency call service provider forwards the call and a unique call-back number (ELIN) to the emergency services. The emergency service or public safety answering point (PSAP) receives the ATA's location. The PSAP also receives a number to call you back, if the call disconnects.

See [Emergency Call Support Terminology, on page 35](#) for the terms used to describe emergency calls from the phone.

The phone requests new location information for the following activities:

- You register the ATA with the call server.
- You or the user restarts the ATA and the ATA was previously registered with the call server.
- You change the network interface used in the SIP registration.
- You change the IP address of the ATA.

If both of the location servers do not send a location response, the phone resends the location request every two minutes.

Emergency Call Support Terminology

The following terms describe emergency call support for the ATA.

- **Emergency Location ID Number (ELIN)**—A number used to represent one or more ATA lines that locate the person who dialed emergency services.
- **Emergency Response Location (ERL)**—A logical location that groups a set of ATA lines.
- **HTTP Enabled Location Delivery (HELD)**—An encrypted protocol that obtains the PIDF-LO location for the ATA from a location information server (LIS).
- **Location Information Server (LIS)**—A server that responds to a SIP-based ATA HELD request and provides the ATA location using a HELD XML response.
- **Emergency Call Service Provider**—The company that responds to an ATA HELD request with the ATA's location. When you make an emergency call (which carries the ATA's location), a call server routes the call to this company. The emergency call service provider adds an ELIN and routes the call to the emergency services (PSAP). If the call is disconnected, the PSAP uses the ELIN to reconnect with the ATA used to make the emergency call.
- **Public Safety Answering Point (PSAP)**—Any emergency service (for example, fire, police, or ambulance) joined to the Emergency Services IP Network.
- **Universally Unique Identifier (UUID)**—A 128-bit number used to uniquely identify a company using emergency call support.

Configure the ATA to Make Emergency Calls

Before you begin

Obtain an E911 location URL and a company ID for the ATA from your emergency calling service provider (for example, Redsky admin). You can use the same location URL and company ID for PHONE1 and PHONE2.

Procedure

- Step 1** Sign into On Cisco Communication Manager Administration as an administrator.
- Step 2** Configure a service profile:

- a) Select **User Management > > User Settings > Service Profile**.
- b) Create a new service profile with a unique name. For example, "Emergency Calling Profile".
- c) Configure the fields in the section **Emergency Calling Profile**.

The **Organization ID**, **Secret**, and **Location Url** are provided by your emergency calling service provider.

For **Emergency Numbers**, enter the emergency service numbers, separated by commas. For example, **911 , 933**

- d) Click **Save**.

Step 3 Associate an end user with the created service profile:

- a) Select **User Management > End User**.
- b) Create a new user or modify an existing user.
- c) In the **Service Settings** section, select the service profile that you created from the **UC Service Profile** drop-down list.
- d) Click **Save**.

Step 4 Associate a phone with the created or modified user:

- a) Select **Device > Phone** to find an existing phone.
- b) In the **Device Information** section, select **User** for the **Owner** field, and then select the user from the **Owner User ID** drop-down list.
- c) Click **Save**.

Step 5 Create or modify an SIP dial rule for the emergency number:

- a) Select **Call Routing > Dial Rules > SIP Dial Rules**.
- b) Create a new SIP dial rule or modify an existing one.
- c) If you choose to create a new SIP dial rule, select **7940_7960_OTHER** from the **Dial Pattern** drop-down list.
- d) Enter a name and relevant descriptions for the SIP dial rule.
- e) In the **Pattern Information** section, add patterns of the emergency number (such as, "911" and "933").
- f) Click **Save**.

Step 6 Associate a phone with the created or modified SIP dial rule:

- a) Select **Device > Phone**.
- b) In the **Protocol Specific Information** section, select the SIP dial rule from the **SIP Dial Rules** drop-down list.
- c) Click **Save**.

Step 7 Verify the E911 configurations on the ATA web page:

- a) Select **Voice > Line <n>**.
- b) Go to the section **Call Feature Settings**, check whether the parameter **Emergency Number** is configured as expected.
- c) Go to the section **E911 Geolocation Configuration**, check whether the parameters are configured as expected.
- d) Go to the section **Dial Plan**, check whether the parameter is configured as expected.



CHAPTER 5

Configure Fax Services

- [Fax Services, on page 37](#)
- [Fax Mode, on page 37](#)

Fax Services

The ATA 191 provides two modes of fax services that provide internetworking with Cisco IOS gateways over IP networks. These modes are called fax pass-through mode and T.38 fax relay mode.

With fax pass-through mode, the ATA 191 encodes fax traffic within the G.711 voice codec. The fax traffic is then passed through the Voice Over IP (VoIP) network as though the fax were a voice call.

With T.38 fax relay mode, the ATA 191 supports the transmission of faxes, in real time, between two standard fax terminals communicating over SIP networks. T.38 fax relay mode provides a more reliable and error-free method of sending faxes over an IP network.

Fax Mode

You can choose the preferred fax mode on the phone configuration page of the Unified CM administration page. From the fax mode pull-down window, choose one of the following modes:

- Fax passthrough
- T.38 fax relay
- NSE Fax passthrough—G711ulaw
- NSE Fax passthrough—G711alaw

You can set the Fax Error correction mode override values. From the fax mode pull-down window, choose one of the following modes:

- On
- Off
- Default

Fax Modem Standards

The ATA 191 supports the following fax modem standards:

- ITU-T V.34
- ITU-T V.34 Annex 12
- K56flex
- V.21
- V.22
- V.23
- V.32
- V.32bis
- V.44
- V.90
- V.92



Note V.34 is not supported for T.38 relay fax.

Fax Modem Speeds

The ATA 191 supports the following fax modem speeds:

- 33.6 kb/s
- 31.2 kb/s
- 28.8 kb/s
- 26.4 kb/s
- 24 kb/s
- 21.6 kb/s
- 19.2 kb/s
- 16.8 kb/s
- 14.4 kb/s
- 12 kb/s
- 9.6 kb/s
- 7.2 kb/s
- 4.8 kb/s

- 2.4 kb/s



Note The speeds that are only used in V.34 do not apply for fax using T.38 relay.



CHAPTER 6

Troubleshoot and Maintenance

- [Configure Syslog Reports, on page 41](#)
- [Resolve Startup Problems, on page 44](#)
- [ATA 191 Resets Unexpectedly, on page 48](#)
- [Troubleshoot ATA 191 Security, on page 50](#)
- [General Troubleshooting Tips, on page 51](#)
- [Problem Report Tool, on page 52](#)
- [Clean the ATA 191, on page 54](#)

Configure Syslog Reports

Debug information can be configured from the administration section of the Cisco Unified Communications Manager. Refer to the Product-Specific Configuration Parameters for information about configuring debug parameters. Note the following when configuring debug parameters from the Cisco Unified Communications Manager:

- Log Server / IPv6 Log Server: Syslog server in IPv4 and IPv6 format
- Remote Log: Enabled or Disabled. Log messages are not sent to server if set to Disabled.
- Log Profiles: Debug flag settings of log modules.

The Log Module, the Log Setting, and the Log Viewer can be generated from the administration section of the phone web page. Note the following:

- Log Module: To configure debug flags; these parameters are overwritten by the Unified Communications Manager Log Profile unless Preset is selected.
- Log Setting: To configure log server, port and size. Server settings are overwritten after provisioning.
- Log Viewer: To view, clear or download debug messages being logged.

Because debugging captures detailed information, the communication traffic can slow down the phone, making it less responsive. After you capture the logs, turn off debugging.

Debug information includes a single digit code that reflects the severity of the situation. Situations are graded as follows:

- 0 - Emergency

- 1 - Alert
- 2 - Critical
- 3 - Error
- 4 - Warn
- 5 - Notification
- 6 - Information
- 7 - Debug

Only high severity messages are logged unless its debug flag is turned on.

If you are experiencing phone problems that you cannot resolve, Cisco TAC can assist you. You will need to turn on debugging for the phone, reproduce the problem, turn debugging off, and send the logs to TAC for analysis.

The following table summarizes the Log Profile and Log Module Settings available to you.

Table 8: Log Profile and Log Module Settings

Parameter	Configured from Cisco Unified Communications Manager Log Profile	Configured from Phone Adapter Configuration Utility Log Module	Description
Default	X	Not Available	Resets the debug level to default (All debug off).
Preset	X	Not Available	Use log module settings on Phone Adapter Configuration Utility for debug flags.
Telephony	X	X	Turn on debug flag for provisioning (including auto upgrade) and call features.
SIP	X	X	Turn on debug flag for SIP messages.
UI	X	X	Turn on debug flag for key events, such as DTMF, PRT, and reset button.
Network	X	X	Turn on debug flag for network events such as DHCP, VLAN, or link status change.

Parameter	Configured from Cisco Unified Communications Manager Log Profile	Configured from Phone Adapter Configuration Utility Log Module	Description
Media	X	X	Turn on debug flag for RTP, Fax, Tone, and SLIC -related issues.
System	X	X	Turn on debug flag for system events, such as reboot, or factory reset.
Web	X	X	Turn on debug flag for web operation and event logs.
NTP	X	X	Turn on debug flag for NTP related logs.
CDPLLDP	X	X	Turn on debug flag for CDP and LLDP logs.
Security	X	X	Turn on debug flag for security-related logs.

Related Topics

[Product-Specific Configuration Parameters](#), on page 28

Practice

This section provides practice exercises for getting your voice syslog information.

Turn On Debug flag for Media or SIP

Procedure

-
- Step 1** Sign into Cisco Unified Communications Manager Administration as an administrator.
 - Step 2** Select **Device > Phone**
 - Step 3** Locate the phone associated with the user.
 - Step 4** Navigate to the Product Specific Configuration Layout pane and set the fields.
 - Step 5** Navigate to the Product Specific Configuration Layout pane.
 - Step 6** In the Log Server field, enter an IP address and port of a remote system where log messages are to be sent.
 - Step 7** In the Remote Log field, select **Enabled**.
 - Step 8** In the Log Profile field, select **Media**.
Select **SIP** if you are configuring the SIP module to debug.
 - Step 9** Click **Save**.

Step 10 Click **Apply Config**.

Resolve Startup Problems

After installing an ATA 191 into your network and adding it to Cisco Unified Communications Manager, the phone starts up. If the phone does not start up properly, see the following sections for troubleshooting information:

- [The ATA 191 Does Not Go Through Its Normal Startup Process](#)
- [The ATA 191 Does Not Register with Cisco Unified Communications Manager, on page 44](#)
- [ATA 191 Unable to Obtain IP Address, on page 47](#)

Related Topics

[Phone Configuration Files](#), on page 14

The ATA 191 Does Not Register with Cisco Unified Communications Manager

If the ATA proceeds past the first stage of the startup process, with LED indicators flashing, but continues to cycle through the messages, the ATA is not starting up properly. The ATA cannot successfully start up unless it is connected to the Ethernet network and it has registered with a Cisco Unified Communications Manager server.

These sections can assist you in determining the reason the phone is unable to start up properly:

- [Check Network Connectivity, on page 44](#)
- [Verify TFTP Server Settings, on page 45](#)
- [Verify DNS Settings, on page 45](#)
- [Verify Cisco Unified Communications Manager Settings, on page 45](#)
- [Cisco Unified Communications Manager and TFTP Services Are Not Running, on page 45](#)
- [Create a New Configuration File, on page 46](#)
- [Search for the ATA in Cisco Unified Communications Manager, on page 47](#)

Check Network Connectivity

If the network is down between the ATA and the TFTP server or Cisco Unified Communications Manager, the ATA cannot start up properly.

Procedure

Ensure that the network is currently running.

Verify TFTP Server Settings

You can determine the IP address of the TFTP server used by the ATA 191 by entering **http://x.x.x.x** where x.x.x.x is the IP address of the ATA 191.

Procedure

- Step 1** If you have assigned a static IP address to the phone, manually enter a setting for the TFTP Server 1 option.
- Step 2** If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address that is configured in Option 150 or Option 66.
- Step 3** You can also enable the phone to use an alternate TFTP server. Such a setting is very useful if the phone was recently moved from one location to another.

Related Topics

[Access the IVR and Configure Your ATA Settings](#), on page 61

Verify DNS Settings

Procedure

- Step 1** If you are using DNS to refer to the TFTP server or to Cisco Unified Communications Manager, ensure that you have specified a DNS server. Verify this setting by entering *http://x.x.x.x* where x.x.x.x is the IP address of the ATA 191.
- Step 2** Verify that there is an A entry in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.
- Step 3** Ensure that DNS is configured to do reverse look-ups.

Verify Cisco Unified Communications Manager Settings

Procedure

Enter *http://x.x.x.x* where x.x.x.x is the IP address of the ATA 191 to find the active Cisco Unified Communications Manager settings.

Cisco Unified Communications Manager and TFTP Services Are Not Running

If the Cisco Unified Communications Manager or TFTP services are not running, phones may not be able to start up properly. In such a situation, it is likely that you are experiencing a system-wide failure, and that other phones and devices are unable to start up properly.

If the Cisco Unified Communications Manager service is not running, all devices on the network that rely on it to make phone calls are affected. If the TFTP service is not running, many devices cannot start up successfully.

Before you begin

A service must be activated before it can be started or stopped. To activate a service, choose **Tools > Service Activation**.

Procedure

-
- Step 1** From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list.
- Step 2** Choose **Tools > Control Center - Network Services**.
- Step 3** Choose the primary Cisco Unified Communications Manager server from the Server drop-down list.
The window displays the service names for the server that you chose, the status of the services, and a service control panel to stop or start a service.
- Step 4** If a service has stopped, click its radio button and then click the **Start** button.
The Service Status symbol changes from a square to an arrow.
-

Create a New Configuration File

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

Before you begin

When you remove a phone from the Cisco Unified Communications Manager database, its configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone's directory number or numbers remain in the Cisco Unified Communications Manager database. They are called "unassigned DN's" and can be used for other devices.

If unassigned DN's are not used by other devices, delete them from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. See the *Administration Guide for Cisco Unified Communications Manager* for more information.

Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but there is no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

Procedure

-
- Step 1** From Cisco Unified Communications Manager, choose **Device > Phone > Find** to locate the phone experiencing problems.
- Step 2** Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.
- Step 3** Add the phone back to the Cisco Unified Communications Manager database.

- Step 4** Power cycle the phone.

Related Topics

[Attach a Phone to the ATA 191](#), on page 21

Search for the ATA in Cisco Unified Communications Manager

An ATA can register with a Cisco Unified Communications Manager server only if it has been added to the server or if autoregistration is enabled.

Before you begin

Ensure that the ATA has been added to the Cisco Unified Communications Manager database.

Procedure

-
- Step 1** To search for a device, sign-in to the Cisco Unified Communications Manager Administration.
- Step 2** **Device**
- Step 3** Choose **Phone > Find**
-

What to do next

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged.

Related Topics

[Attach a Phone to the ATA 191](#), on page 21

[Determine the MAC Address of the ATA](#), on page 18

[Add Users to Cisco Unified Communications Manager](#), on page 34

ATA 191 Unable to Obtain IP Address

If a phone is unable to obtain an IP address during startup, the phone may not be on the same network or VLAN as the DHCP server. Or, the switch port to which the phone is connected may be disabled.

Procedure

-
- Step 1** Ensure that the network or VLAN to which the phone is connected has access to the DHCP server.
- Step 2** Ensure that the switch port is enabled.
-

ATA 191 Resets Unexpectedly

If users report that their phones are resetting during calls or while idle on their desk, investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, an ATA 191 should not reset on its own.

Typically, a phone resets if it has problems connecting to the Ethernet network or to Cisco Unified Communications Manager. These sections can help you identify the cause of a phone resetting in your network:

- [Verify the Physical Connection, on page 48](#)
- [Identify Intermittent Network Outages, on page 48](#)
- [Verify DHCP Settings, on page 49](#)
- [Check Static IP Address Settings, on page 49](#)
- [Verify Voice VLAN Configuration, on page 49](#)
- [Eliminate DNS or Other Connectivity Errors, on page 49](#)

Verify the Physical Connection

Procedure

Verify that the ATA's Ethernet connection is up.

For example, check whether the particular port or switch to which the phone is connected is down and that the switch is not rebooting.

Make sure that there are no cable breaks.

Identify Intermittent Network Outages

Intermittent network outages affect data and voice traffic differently. Your network might have been experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect its network connection.

Procedure

If you are experiencing problems with the voice network, investigate whether an existing problem is simply being exposed.

Verify DHCP Settings

Follow this process to help determine if the phone has been properly configured to use DHCP:

Procedure

- Step 1** Verify that you have properly configured the phone to use DHCP.
- Step 2** Verify that the DHCP server has been set up properly.
- Step 3** Verify the DHCP lease duration. Cisco recommends that you set it to 8 days.

The ATA sends the DHCP request message to update the IP Address at half of the lease time. If no response is received from the server, the ATA starts the DHCP Discover process to get the new IP address.

Related Topics

[Configure Startup Network Settings](#), on page 21

Check Static IP Address Settings

Procedure

If the phone has been assigned a static IP address, verify that you have entered the correct settings.

Related Topics

[Phone Configuration Files](#)

Verify Voice VLAN Configuration

If the ATA appears to reset during heavy network usage, it is likely that you do not have a voice VLAN configured. An example of heavy network usage can be extensive web surfing on a computer connected to the same switch as the phone.

Procedure

Isolate the phones on a separate auxiliary VLAN.

This increases the quality of the voice traffic.

Eliminate DNS or Other Connectivity Errors

If the phone continues to reset, follow these steps to eliminate DNS or other connectivity errors:

Procedure

-
- Step 1** Use the IVR to reset phone settings to their default values.
 - Step 2** Modify the DHCP and IP settings:
 - a) Disable DHCP.
 - b) Assign static IP values to the phone. Use the same default router setting used for other functioning ATA units.
 - c) Assign the TFTP server. Use the same TFTP server used for other functioning ATA units.
 - Step 3** On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.
 - Step 4** From Cisco Unified Communications Manager, choose **System** > **Server** and verify that the server is referred to by its IP address and not by its DNS name.
 - Step 5** From Cisco Unified Communications Manager, choose **Device** > **Phone** and verify that you have assigned the correct MAC address to this ATA.
 - Step 6** Power cycle the phone.

Related Topics

- [Access the IVR and Configure Your ATA Settings](#), on page 61
- [Phone Configuration Files](#)
- [Determine the MAC Address of the ATA](#), on page 18

Troubleshoot ATA 191 Security

The following table provides troubleshooting information for the security features on the ATA 191. For information relating to solutions for any of these issues, and for more troubleshooting information about security, see the *Security Guide for Cisco Unified Communications Manager*.

Table 9: ATA 191 Security Troubleshooting

Problem	Possible Cause
CTL File Problems	
Device authentication error.	CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.
ATA cannot authenticate the CTL file.	The security token that signed the updated CTL file does not exist in the CTL file on the phone.
ATA cannot authenticate any of the configuration files other than CTL file.	The configuration file may not be signed by the corresponding certificate in the phone’s Trust List.
ATA does not register with Cisco Unified Communications Manager.	The CTL file does not contain the correct information for the Cisco Unified Communications Manager server.

Problem	Possible Cause
ATA does not request signed configuration files.	The CTL file does not contain any TFTP entries with certificates.
ATA cannot update the CTL file.	When the CTL file is updated on Cisco Unified Communications Manager, a factory reset of the ATA is required to update the CTL file.

General Troubleshooting Tips

The following table provides general troubleshooting information for the ATA 191.

Table 10: ATA 191 Troubleshooting

Summary	Explanation
Poor quality when calling mobile phones using the G.729 protocol	In Cisco Unified Communications Manager, you can configure the network to use the G.729 protocol (the default is G.711). When using G.729, calls between a phone and a mobile phone have poor voice quality. Use G.729 only when absolutely necessary.
Prolonged broadcast storms cause phones to reset, or be unable to make or answer a call.	A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.
Dual-Tone Multi-Frequency (DTMF) delay	When you are on a call that requires keypad input, if you press the keys too quickly, some of them may not be recognized.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is being used for a conversation between this ATA and the other device. These values should match. If they do not, verify that the other device can handle the codec conversation or that a transcoder is in place to handle the service.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the voice packet sizes that are being used in a conversation between this ATA and the other device. The values of these statistics should match.
Gaps in voice calls	Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics may indicate a problem with jitter on the network or periodic high rates of network activity.
One-way audio	When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configurations in routers and switches to ensure that IP connectivity is properly configured.

Summary	Explanation
Phone call cannot be established.	<p>The phone does not have a DHCP IP address and is unable to register with Cisco Unified Communications Manager.</p> <p>Verify the following:</p> <ol style="list-style-type: none"> 1. The Ethernet cable is attached. 2. The Cisco Unified Communications Manager service is running on the Cisco Unified Communications Manager server. 3. Both phones are registered to the same Cisco Unified Communications Manager.

Problem Report Tool

To issue a problem report, press the **PRT** button on the ATA.

The Problem Report Tool logs are required by Cisco TAC when troubleshooting problems. The logs are cleared if you restart the phone. Collect the logs before you restart the phones.

You must add a server address to the **Customer Support Upload URL** field on Cisco Unified Communications Manager.

Related Topics

[ATA 191 Top Panel](#), on page 4

Configure a Customer Support Upload URL

You must use a server with an upload script to receive PRT files. The PRT uses an HTTP POST mechanism, with the following parameters included in the upload (utilizing multipart MIME encoding):

- devicename (example: “SEP001122334455”)
- serialno (example: “FCH12345ABC”)
- username (the username configured in Cisco Unified Communications Manager, the device owner)
- prt_file (example: “probrep-20141021-162840.tar.gz”)

A sample script is shown below. This script is provided for reference only. Cisco does not provide support for the upload script installed on a customer's server.

```
<?php
// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used: upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
```

```

$devicename = trim($devicename, "\\");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "\\");

$username = $_POST['username'];
$username = trim($username, "\\");

// where to put the file
$fullfilename = "/var/prtuploads/". $filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
    header("HTTP/1.0 500 Internal Server Error");
    die("Error: You must select a file to upload.");
}

?>

```

Procedure

- Step 1** Set up a server that can run your PRT upload script.
- Step 2** Write a script that can handle the parameters listed above, or edit the provided sample script to suit your needs.
- Step 3** Upload your script to your server.
- Step 4** In Cisco Unified Communications Manager, go to the Product Specific Configuration Layout area of the individual device configuration window, Common Phone Profile window, or Enterprise Phone Configuration window.
- Step 5** Check **Customer support upload URL** and enter your upload server URL.
Example:
<http://example.com/prtscript.php>
- Step 6** Save your changes.

Related Topics

[Problem Report Tool](#), on page 52

Generate a Problem Report

You can generate a problem report for the ATA 191 using the Problem Report Tool. When you generate a problem report, a log file is generated and sent to the system administrator.

Procedure

You can generate a problem report using one of the following methods:

- Press the PRT button on the top panel of the ATA 191.

The problem report is generated and sent to the system administrator. The LED turns green if the report is sent successfully, or turns red if the report failed. Press the PRT button again to retry.

- On the web interface for the device, go to **Administration > PRT Viewer**. Click **Generate PRT** to start the PRT process and generate a problem report.
-

Clean the ATA 191

To clean your ATA, use a soft, dry cloth to wipe the surface. Do not apply liquids or powders directly on the device. As with all non-weather-proof electronics, liquids and powders can damage the components and cause failures.



CHAPTER 7

ATA 191 Specifications

- [Physical Specifications, on page 55](#)
- [Electrical Specifications, on page 56](#)
- [Environmental Specifications, on page 56](#)
- [Physical Interfaces, on page 56](#)
- [Ringing Characteristics, on page 57](#)
- [Software Specifications, on page 57](#)
- [SIP Compliance Reference Information, on page 59](#)

Physical Specifications

Table 11: Physical Specifications

Description	Specification
Regulatory compliance	FCC (Part 15 Class B), CE, ICES-003, A-Tick certification, Restriction of Hazardous Substances (RoHS), and UL
Power supply	DC input voltage: 5V DC at 2.0A maximum power consumption: 5W Switching type (100-240V): Automatic Power adapter: 100-240V and 50-60 Hz (26-34 VA) input with 1.8m cord
Indicator lights and LEDs	Phone 1, phone 2, network, Problem Report Tool (PRT), and power
Documentation	User Guide (online) Administration Guide (online) Regulatory Compliance and Safety Information guide (online)
Dimensions (W x H x D)	3.98 x 3.98 x 1.10 in. (101 x 101 x 28mm)
Unit weight	5.40 oz (153 g)

Electrical Specifications

Table 12: Electrical Specifications

Description	Specification
Power	0.25 to 12W (idle to peak)
DC input voltage	5.0 VDC at 2.0A maximum
Power adapter	Universal AC/DC ~4.05 x 1.93 x 1.31 in. (~10.3 x 4.9 x 3.35 cm) ~4.23 oz (120 g) for the AC-input external power adapter ~4.9 ft (1.5 m) DC cord 6 ft (1.8 m) cord UL/cUL, CE approved Class I adapter

Environmental Specifications

Table 13: Environmental Specifications

Description	Specification
Operating temperature	32 to 113°F (0 to 45°C)
Nonoperating temperature	-13 to 158°F (-25 to 70°C)
Operating humidity	10% to 90% noncondensing
Storage humidity	10% to 90% noncondensing

Physical Interfaces

Table 14: Physical Interfaces

Description	Specification
Ethernet	One RJ-45 connector, IEEE 802.3 100BaseT standard
Analog phone	Two RJ-11 FXS voice ports
Power	5 VDC power connector

Ringing Characteristics

Table 15: Ringing Characteristics

Description	Specification
Tip/ring interfaces for each RJ-11 FXS port (SLIC)	
Ring voltage	70VRMS (typical, balanced ringing only)
Ring frequency	20 Hz
Ring waveform	Trapezoidal with 1.2 to 1.6 crest factor
Ring load	1400 ohm + 40 μ F
Ringer equivalence number (REN)	Up to 3 REN per RJ-11 FXS port
Loop impedance	Up to 200 ohms (plus 430-ohm maximum phone DC resistance)
On-hook/off-hook characteristics	
On-hook voltage (tip/ring)	-47V
Off-hook current	24 mA (nominal)
RJ-11 FXS port terminating impedance option	The ATA 191 provides multiple impedance, such as 600 ohm for American SKU, 900 ohm for European SKU, 220 ohm (820 ohm 120nF) for Australian SKU, and so on.

Software Specifications

Table 16: Software Specifications (All Protocols)

Description	Specification
Call progress tones	Configurable for two sets of frequencies and single set of on/off cadence
Dual-tone multifrequency (DTMF)	DTMF tone detection and generation

Description	Specification
Fax	<p>Fax pass-through and T.38 fax relay mode.</p> <p>V34 fax is supported for pass-through mode. Success of fax transmissions up to 33.6 kb/s depends on network conditions, and fax modem/fax machine tolerance to those conditions. The network must have reasonably low network jitter, network delay, and packet-loss rate.</p> <p>The ATA 191 only supports T38 Fax Relay Version 0 (G3).</p>
Line-echo cancellation	<ul style="list-style-type: none"> • Echo canceler for each port • 8 ms echo length • Nonlinear echo suppression (ERL > 28 dB for frequency = 300 to 2400 Hz) • Convergence time = 250 ms • ERLE = 10 to 20 dB • Double-talk detection
Out-of-band DTMF	<p>RFC 2833 AVT tones for SIP</p> <p>Note Cannot transmit RFC 2833 and in-band signaling, simultaneously.</p>
Configuration	<ul style="list-style-type: none"> • DHCP (RFC 2131) • Web configuration via built-in web server • Basic boot configuration (RFC 1350 TFTP Profiling) • Dial plan configuration • Cisco Discovery Protocol
Quality of Service	<ul style="list-style-type: none"> • Class-of-service (CoS) bit-tagging (802.1P) • Type-of-service (ToS) bit-tagging
Security	Encryption for TFTP configuration files
Voice coder-decoders (codecs)	<ul style="list-style-type: none"> • G.729A, G.729AB • G.711A-law • G.711μ-law
Voice features	<ul style="list-style-type: none"> • Voice activity detection (VAD) • Comfort noise generation (CNG) • Dynamic jitter buffer (adaptive)

Description	Specification
Voice-over-IP (VoIP) protocols	SIP (RFC 3261)

SIP Compliance Reference Information

Information on how the ATA 191 complies with the IETF definition of SIP as described in RFC 2543 is found at the following URL:

<http://www.ietf.org/rfc/rfc2543.txt>



CHAPTER 8

Voice Menu Codes

- [Access the IVR and Configure Your ATA Settings, on page 61](#)

Access the IVR and Configure Your ATA Settings

Before you begin

If you set the IP mode to static IP, you must go on-hook to make it effective. Then, you can configure the IP address, subnet mask, and default gateway.

The network cable must be connected to set a static IP.



Note You can change the IVR password on the Device window of Cisco Unified Communications Manager.

Procedure

- Step 1** To access the IVR, go off-hook on the phone connected to PHONE1 or PHONE2.
- Step 2** Press **** from the phone keypad.
The IVR prompts for a password.
The ATA 191 allows you to enter only numerical values for the password.
- Step 3** Enter the IVR password by pressing the number keypad, followed by #.
You are at the IVR main configuration menu.
- Step 4** Follow the voice prompts on the IVR. See [IVR Configuration Menu Options, on page 62](#) for information on navigating the IVR.
- Step 5** To return to the main configuration menu, press *.
- Step 6** To exit the IVR, end the call.
-

IVR Tips

When using the IVR to manage the ATA, note the following tips:

- Enter the numbers slowly, listening for the audio confirmation before entering the next number.
- After you select an option, press the # (pound) key.
- To exit the menu, hang up the phone.
- After entering a value such as an IP address, press the # (pound) key to indicate that you have finished your selection. Then proceed as needed:
 - To save a setting, press **1**.
 - To review a setting, press **2**.
 - To re-enter a setting, press **3**.
 - To cancel your entry and return to the main menu, press * (star).
- When entering a value, you can cancel the changes by pressing the * (star) key twice within half a second. Be sure to press the key quickly, or the * is treated as a decimal point entry.
- If the menu is inactive for more than one minute, the IVR times out. Re-enter the IVR menu by pressing ****. Your settings take effect after you hang up the phone or exit the IVR. The ATA may reboot now.
- To enter special characters, use the following key combinations:
 - To enter a dot (.) or colon (:) that separates octets in the IP Address, press star (*).
 - To enter the hexadecimal A, press the 2 key two times quickly.
 - To enter the hexadecimal B, press the 2 key three times quickly.
 - To enter the hexadecimal C, press the 2 key four times quickly.
 - To enter the hexadecimal D, press the 3 key two times quickly.
 - To enter the hexadecimal E, press the 3 key three times quickly.
 - To enter the hexadecimal F, press the 3 key four times quickly.

For example, to enter the IP address 191.168.1.105, perform the following tasks:

- Press these keys: 191*168*1*105
- Press the # (pound) key to indicate that you have finished entering the IP address.
- Press **1** to save the IP address or press the * (star) key to cancel your entry and return to the main menu.

IVR Configuration Menu Options

The following table describes the various options in the IVR Configuration Menu.

Table 17: Navigating the IVR Configuration Menu

Menu Option	IVR Action	Notes
100	(IPv4) Check the Internet Addressing Method	Answers with 0, the default option (DHCP).
101	(IPv4) Set the Internet Addressing Method	0: DHCP; 1: Static IP
102	Check Stack Mode.	0: IPv4; 1:IPv6; 2: Dual
110	(IPv4) Show the ATA IP address	
111	(IPv4) Configure the ATA's static IP address	Available in static IP mode only.
120	(IPv4) Show the subnet mask	
121	(IPv4) Configure the subnet mask	Available in static IP mode only.
130	(IPv4) Check the gateway IP address	
131	(IPv4) Configure the gateway IP address	Available in static IP mode only.
160	(IPv4) Check the primary DNS Server setting	
161	(IPv4) Set the primary DNS Server	
220	(IPv4) Show the TFTP server address	
221	(IPv4) Configure the TFTP server address	
230	Show the VLAN.	
231	Configure a VLAN.	To enable a VLAN, set the VLAN ID from 1 to 4094. To disable a VLAN, set the VLAN ID to 4095.
600	(IPv6) Check the IPv6 Internet addressing method	
601	(IPv6) Set the IPv6 Internet Addressing Method	0: DHCP; 1: Static IP
606	Check IPv6 Auto Configuration.	0: Disabled; 1: Enabled.
610	(IPv6) Show the ATA IP address	
611	(IPv6) Configure the ATA's static IP address	Available in IPv6 static IP mode only.
620	(IPv6) Check the IP address prefix length	

Menu Option	IVR Action	Notes
621	(IPv6) Configure the static IP address prefix length	Available in IPv6 static IP mode only.
622	(IPv6) Check the TFTPv6 server address	
623	(IPv6) Set the TFTPv6 server address	
630	(IPv6) Check the gateway IP address	
631	(IPv6) Configure the gateway IP address	Available in IPv6 static IP mode only.
660	(IPv6) Check the primary DNS Server setting	
661	(IPv6) Set the primary DNS Server	
73738	Factory Reset	
802	Configure the 802.1x authentication	0: Disabled; 1: Enabled
803	Check the 802.1x authentication configuration	Respond with a number: 0 or 1. 0: Disabled; 1: Enabled



CHAPTER 9

ATA 191 Country-Specific Tones and Cadences

- [ATA 191 Country-Specific Tones and Cadences, on page 65](#)

ATA 191 Country-Specific Tones and Cadences

Mechanism

The administrator can upload an XML file named `g3-tones.xml` that describes the tones and cadences to the directory on the Cisco Unified Communications Manager TFTP server. The directory name is actually a locale name, such as **Australia**.

During provisioning, the device knows the network locale setting and tries to download **[locale name]/g3-tones.xml** from the Cisco Unified CM TFTP server. For example, if the network locale is set to **Australia**, the path is **Australia/g3-tones.xml**.

Link a Tone File with a Device

Procedure

Use one of the following methods to link the tone file with the device.

- Method 1: In Cisco Unified Communications Manager, navigate to **System > Device Pool**, and set the Network Locale value to specify the locale option.
- Method 2: In Cisco Unified Communications Manager, navigate to **Device > Phone**. On the device window, set the value of Network Locale, which overwrites the value that is set in method 1.

Note For method 2, network locale from **Device > Phone** is not configurable currently because there are only two choices: none and United States. There is a known issue for Cisco Unified Communications Manager that countries other than the United States cannot be selected from this menu. Method 2 has a higher priority than method 1.

Tone Configuration

- Only the ATA 191 Line1 network locale setting is applied. The line2 network locale always applies the line1 option, even if the configured value of line2 network locale differs from the line1 value.
- Only these tones can be configured:
 - Ringback tone
 - Reorder tone
 - Dialing tone
 - Outside dialing tone
 - Busy tone
 - Call waiting tone

Any tone specification that appears in the tone profile but is not supported or has invalid data fields (even if the tone is supported) is ignored.

- **Example:** A tone profile includes a valid reorder tone specification, an invalid busy tone specification (has invalid data fields), and a recording tone spec (not supported). Only the reorder tone spec would be applied.
- The name of the XML file that describes tones and cadences is **g3-tones.xml**.
- Each tone can specify at most four c/i pairs (about frequency and gain) and four cadence segments (each is an on/off pair). Any additional data gets discarded.