Configure Analog Telephone Adaptors

Analog Telephone Adaptor Overview

The Cisco Analog Telephone Adaptor (ATA) functions as an analog telephone adapter that interfaces regular analog telephones to IP-based telephony networks. The Cisco ATA converts any regular analog telephone into an Internet telephone. Each adapter supports two voice ports, each with its own telephone number.

Like other IP devices, the Cisco ATA receives its configuration file and list of Unified Communications Managers from the TFTP server. If the TFTP server does not have a configuration file, the Cisco ATA uses the TFTP server name or IP address and port number as the primary Unified Communications Manager name or IP address and port number.

The Cisco ATA:

- Contains a single 10 BaseT RJ-45 port and two RJ-11 FXS standard analog telephone ports
- Supports a number of codecs, including G.711 alaw, G.711 mulaw, and G.723 and G.729a voice codecs
- Converts voice into IP data packets
- Supports redial, speed dial, call forwarding, call waiting, call hold, transfer, conference, voice messaging, message-waiting indication, off-hook ringing, caller-ID, callee-ID, and call waiting caller-ID

The ATA 180 series uses SCCP, while the ATA 190 series uses SIP. For more information, see the ATA documentation:

- ATA 180 Series: https://www.cisco.com/c/en/us/support/unified-communications/ata-180-series-analog-telephone-adaptors/tsd-products-support-series-home.html
- ATA 190 Series: https://www.cisco.com/c/en/us/support/unified-communications/ata-190-series-analog-telephone-adapters/tsd-products-support-series-home.html

Configure Analog Telephone Adaptor

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The **Find and List Phones** window appears.

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop down list, select the Analog Telephone Adaptor model you have and click **Next**.
The **Phone Configuration** window appears.

Step 4 Configure the fields in the **Phone Configuration** window.

See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

Step 6 Click **Apply Config** for your changes to take effect and synchronize the phone.

Analog Telephone Adaptor 186 Configuration Fields

Table 1: Analog Telephony Adaptor 186 Configuration Fields

Field	Description
MAC Address	Enter the Media Access Control (MAC) address that identifies ATA 186. Make sure that the value comprises 12 hexadecimal characters. You can determine the MAC address for ATA 186 in any of these ways: • Look at the MAC label on the back of ATA 186. • Display the web page for ATA 186 and click the **Device Information** hyperlink.
Description	Enter a text description of the ATA 186. This field can contain up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Choose the device pool to which you want the ATA 186 assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. To see the Device Pool configuration settings, click the View Details link.
Common Device Configuration	Choose the Common Device Configuration to which you want the ATA 186 assigned. To see the Common Device Configuration settings, click the View Details link.

Field	Description
Phone Button Template	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Common Phone Profile	From the drop-down list, choose a common phone profile from the list of available common phone profiles. To see the Common Phone Profile settings, click the View Details link.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
AAR Calling Search Space	From the drop-down list, choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) or leave the calling search space as the default of <None>.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. If you choose **<None>**, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list, choose the user locale that is associated with the ATA 186. The user locale identifies a set of detailed information to support users, including language and font. If you do not specify a user locale, Cisco Unified CM uses the user locale that is associated with the device pool.
Network Locale	From the drop-down list, choose the network locale that is associated with the ATA 186. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. If you do not specify a network locale, Cisco Unified CM uses the network locale that is associated with the device pool.
Device Mobility Mode	From the drop-down list, turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for a device.
Owner	Select **User** or **Anonymous** (Public/Shared Space, for the owner type.

Field	Description
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from "Unassigned Devices" to "Users" in the License Usage Report. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.
Phone Load Name	Enter the custom software for ATA 186.
Use Trusted Relay Point	Choose one of the following values: • Off—Choose this value to disable the use of a Trusted Relay Point (TRP) with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default— Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Geolocation	From the drop-down list, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Unified Communications Manager ignores any presentation restriction that is received for internal calls. Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call.
Allow Control of Device from CTI	Check this check box to allow CTI to control and monitor this device. If the associated directory number specifies a shared line, the check box should be enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports.
Logged into Hunt Group	When the CTI port gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	Check this box to allocate a buffer for the device when it registers and to bundle SCCP messages to the phone. **Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays.
Hot Line Device	Check this check box to make this device a Hotline device. Hotline devices can only connect to other Hotline devices. This feature is an extension of PLAR, which configures a phone to automatically dial one directory number when it goes off-hook. Hotline provides additional restrictions that you can apply to devices that use PLAR. To implement Hotline, you must also create a softkey template without supplementary service softkeys, and apply it to the Hotline device.

Number Presentation Transformation

Table 2: Caller ID for Calls From This Phone

Field	Description
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.

Field	Description
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.

Table 3: Remote Number

Field	Description
Calling Party Transformation CSS	From the drop-down list, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this device.
Use Device Pool Calling Party Transformation CSS	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this device belongs to transform the remote calling and remote connected number.

Table 4: Protocol Specific Information

Field	Description
BLF Presence Group	From the drop-down list, choose a Busy Lamp Field (BLF) presence group for the end user. The selected group specifies the destinations that the end user can monitor The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list.
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all devices that are configured in Unified Communications Manager Administration.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you can configure a calling search space as you do all calling search spaces.
Unattended Port	Check this check box to indicate an unattended port on this device.

Field	Description
RFCC 2833 Disabled	For devices that are running SCCP, check this check box to disable RFC2833 support.

Table 5: Product-Specific Configuration Layout

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, see the documentation for ATA 186.

Analog Telephone Adaptor 187 Configuration Fields

Table 6: Analog Telephony Adaptor 187 Configuration Fields

Field	Description
MAC Address	Enter the Media Access Control (MAC) address that identifies ATA 187. Make sure that the value comprises 12 hexadecimal characters. You can determine the MAC address for ATA 187 in any of these ways: • Look at the MAC label on the back of ATA 187. • Display the web page for ATA 187 and click the **Device Information** hyperlink.
Description	Enter a text description of the ATA 187. This field can contain up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Choose the device pool to which you want the ATA 187 assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. To see the Device Pool configuration settings, click the View Details link.
Common Device Configuration	Choose the Common Device Configuration to which you want the ATA 187 assigned. To see the Common Device Configuration settings, click the View Details link.
Phone Button Template	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.

Field	Description
Common Phone Profile	From the drop-down list, choose a common phone profile from the list of available common phone profiles. To see the Common Phone Profile settings, click the View Details link.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
AAR Calling Search Space	From the drop-down list, choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) or leave the calling search space as the default of <None>.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. If you choose **<None>**, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list, choose the user locale that is associated with the CTI Port. The user locale identifies a set of detailed information to support users, including language and font. If you do not specify a user locale, Cisco Unified CM uses the user locale that is associated with the device pool.
Network Locale	From the drop-down list, choose the network locale that is associated with the CTI Port. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. If you do not specify a network locale, Cisco Unified CM uses the network locale that is associated with the device pool.
Built in Bridge	Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list. Choose one of the following: • On • Off • Default
Privacy	For Privacy, choose **On** in the Privacy drop-down list.

Field	Description
Device Mobility Mode	From the drop-down list, turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device.
Owner	Select **User** or **Anonymous (Public/Shared Space)** , for the owner type.
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from "Unassigned Devices" to "Users" in the License Usage Report. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.
Phone Load Name	Enter the custom software for ATA 187.
Use Trusted Relay Point	Choose one of the following values: • **Off**—Choose this value to disable the use of a Trusted Relay Point (TRP) with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

Field	Description
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
Geolocation	From the drop-down list, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Unified Communications Manager ignores any presentation restriction that is received for internal calls. Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call.
Logged into Hunt Group	When the ATA 187 gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	Check this box to allocate a buffer for the device when it registers and to bundle SCCP messages to the phone. **Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays.

Field	Description
Protected Device	Check this check box to designate a phone as protected, which enables the phone to play a 2-second tone to notify the user when a call is encrypted and both phones are configured as protected devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are protected and the call occurs over encrypted media. Checking this check box represents only one of several configuration requirements for the secure indication tone to play. For a detailed description of the secure indication tone feature and the configuration requirements, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html. If you check this check box and the system determines that the call is not encrypted, the phone plays nonsecure indication tone to alert the user that the call is not protected.

Number Presentation Transformation

Table 7: Caller ID for Calls From This Phone

Field	Description
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.

Table 8: Remote Number

Field	Description
Calling Party Transformation CSS	From the drop-down list, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this device.
Use Device Pool Calling Party Transformation CSS	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this device belongs to transform the remote calling and remote connected number.

Table 9: Protocol Specific Information

Field	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list: • **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • **Batch Processing Mode**—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.
BLF Presence Group	From the drop-down list, choose a Busy Lamp Field (BLF) presence group for the end user. The selected group specifies the destinations that the end user can monitor The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list.
SIP Dial Rules	If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed. Leave the SIP Dial Rules field set to <None> if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed.
MTP Preferred Originating Codec	From the drop-down list, choose the codec to use if a media termination point is required for SIP calls.

Field	Description
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all devices that are configured in Unified Communications Manager Administration.
Rerouting Calling Search Space	From the drop-down list, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you can configure a calling search space as you do all calling search spaces.
SIP Profile	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security). Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. After you save the phone configuration and apply the configuration update to the phone, the digest credentials for the user get added to the phone configuration file.

Field	Description
Media Termination Point Required	Use this field to indicate whether a media termination point is used to implement features that ATA 187 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features. Use this check box only for ATA 187 clients and those ATA 187 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.
Unattended Port	Check this check box to indicate an unattended port on this device.
Required DTMF Reception	For devices that are running SIP and SCCP, check this check box to require DTMF reception for this phone. **Note** In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.

Table 10: Certification Authority Proxy Function (CAPF) Information

Field	Description
Certificate Operation	From the drop-down list, choose one of the following options: • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone.

Field	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list, choose one of the following options: • By Authentication String—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • By Null String— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. • By Existing Certificate (Precedence to LSC)—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. • By Existing Certificate (Precedence to MIC)—Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Authentication String	If you chose the **By Authentication String** option in the **Authentication Mode** drop-down list, this field applies. Manually enter a string or generate a string by clicking the **Generate String** button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.

Field	Description
Key Size (Bits)	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list. The default setting equals 1024. Other options include 512 and 2048. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Operation Completes by	This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation. The values that display apply for the publisher database server.
Certificate Operation Status	This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot Certificate Operation options. You cannot change the information that displays in this field.

Table 11: Secure Shell User

Field	Description
Secure Shell User	Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include ",%, &, <, >, and \. This field displays when the phone device that you are configuring supports SSH access. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH credentials to the phone in the clear.
Secure Shell Password	Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 200 characters. Invalid characters include ",%, &, <, >, and \. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Table 12: Product-Specific Configuration Layout

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, see the documentation for ATA 187.

Analog Telephony Adaptor 190 Configuration Fields

Table 13: Analog Telephony Adaptor 190 Configuration Fields

Field	Description
MAC Address	Enter the Media Access Control (MAC) address that identifies ATA 190. Make sure that the value comprises 12 hexadecimal characters. You can determine the MAC address for ATA 190 in any of these ways: • Look at the MAC label on the back of ATA 190. • Display the web page for ATA 190 and click the **Device Information** hyperlink.
Description	Enter a text description of the ATA 190. This field can contain up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Choose the device pool to which you want the ATA 190 assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. To see the Device Pool configuration settings, click the View Details link.
Common Device Configuration	Choose the Common Device Configuration to which you want the ATA 190 assigned. To see the Common Device Configuration settings, click the View Details link.
Phone Button Template	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Common Phone Profile	From the drop-down list, choose a common phone profile from the list of available common phone profiles. To see the Common Phone Profile settings, click the View Details link.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.

Field	Description
AAR Calling Search Space	From the drop-down list, choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) or leave the calling search space as the default of <None>.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. If you choose **<None>**, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list, choose the user locale that is associated with the CTI Port. The user locale identifies a set of detailed information to support users, including language and font. If you do not specify a user locale, Cisco Unified CM uses the user locale that is associated with the device pool.
Network Locale	From the drop-down list, choose the network locale that is associated with the CTI Port. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. If you do not specify a network locale, Cisco Unified CM uses the network locale that is associated with the device pool.
Built in Bridge	Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list. Choose one of the following: • On • Off • Default
Privacy	For Privacy, choose **On** in the Privacy drop-down list.
Device Mobility Mode	From the drop-down list, turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device.
Owner	Select **User** or **Anonymous (Public/Shared Space)** , for the owner type.

Field	Description
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from "Unassigned Devices" to "Users" in the License Usage Report. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.
Phone Load Name	Enter the custom software for ATA 190.
Use Trusted Relay Point	Choose one of the following values: • **Off**—Choose this value to disable the use of a Trusted Relay Point (TRP) with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default— Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone • Default— Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Geolocation	From the drop-down list, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Unified Communications Manager ignores any presentation restriction that is received for internal calls. Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call.
Logged into Hunt Group	When the ATA 190 gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	Check this box to allocate a buffer for the device when it registers and to bundle SCCP messages to the phone. **Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays.
Protected Device	Check this check box to designate a phone as protected, which enables the phone to play a 2-second tone to notify the user when a call is encrypted and both phones are configured as protected devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are protected and the call occurs over encrypted media. Checking this check box represents only one of several configuration requirements for the secure indication tone to play. For a detailed description of the secure indication tone feature and the configuration requirements, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html. If you check this check box and the system determines that the call is not encrypted, the phone plays nonsecure indication tone to alert the user that the call is not protected.

Number Presentation Transformation

Table 14: Caller ID for Calls From This Phone

Field	Description
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.

Table 15: Remote Number

Field	Description
Calling Party Transformation CSS	From the drop-down list, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this device.
Use Device Pool Calling Party Transformation CSS	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this device belongs to transform the remote calling and remote connected number.

Table 16: Protocol Specific Information

Field	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list: • **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • **Batch Processing Mode**—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.

Field	Description
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.
BLF Presence Group	From the drop-down list, choose a Busy Lamp Field (BLF) presence group for the end user. The selected group specifies the destinations that the end user can monitor The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list.
SIP Dial Rules	If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed. Leave the SIP Dial Rules field set to <None> if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed.
MTP Preferred Originating Codec	From the drop-down list, choose the codec to use if a media termination point is required for SIP calls.
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all devices that are configured in Unified Communications Manager Administration.
Rerouting Calling Search Space	From the drop-down list, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.

Field	Description
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you can configure a calling search space as you do all calling search spaces.
SIP Profile	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security). Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. After you save the phone configuration and apply the configuration update to the phone, the digest credentials for the user get added to the phone configuration file. For more information on digest authentication, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html .
Media Termination Point Required	Use this field to indicate whether a media termination point is used to implement features that ATA 190 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features. Use this check box only for ATA 190 clients and those ATA 190 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.
Unattended Port	Check this check box to indicate an unattended port on this device.

Field	Description
Required DTMF Reception	For devices that are running SIP and SCCP, check this check box to require DTMF reception for this phone. **Note** In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.

Table 17: Certification Authority Proxy Function (CAPF) Information

Field	Description
Certificate Operation	From the drop-down list, choose one of the following options: • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone. For more information on CAPF operations, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Field	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list, choose one of the following options: • By Authentication String—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • By Null String— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. • By Existing Certificate (Precedence to LSC)—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. • By Existing Certificate (Precedence to MIC)—Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Authentication String	If you chose the **By Authentication String** option in the **Authentication Mode** drop-down list, this field applies. Manually enter a string or generate a string by clicking the **Generate String** button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.

Field	Description
Key Size (Bits)	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list. The default setting equals 1024. Other options include 512 and 2048. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Operation Completes by	This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation. The values that display apply for the publisher database server.
Certificate Operation Status	This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot Certificate Operation options. You cannot change the information that displays in this field.

Table 18: Secure Shell User

Field	Description
Secure Shell User	Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include ",%, &, <, >, and \. This field displays when the phone device that you are configuring supports SSH access. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH credentials to the phone in the clear.

Field	Description
Secure Shell Password	Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 127 characters. Invalid characters include ",%, &, <, >, and \. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH passwords to the phone in the clear.

Table 19: Product-Specific Configuration Layout

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, see the documentation for ATA 190.

Analog Telephony Adaptor 191 Configuration Fields

Table 20: Analog Telephony Adaptor 191 Configuration Fields

Field	Description
MAC Address	Enter the Media Access Control (MAC) address that identifies ATA 191. Make sure that the value comprises 12 hexadecimal characters. You can determine the MAC address for ATA 191 in any of these ways: • Look at the MAC label on the back of ATA 191. • Display the web page for ATA 191 and click the **Device Information** hyperlink.
Description	Enter a text description of the ATA 191. This field can contain up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Choose the device pool to which you want the ATA 191 assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. To see the Device Pool configuration settings, click the View Details link.

Field	Description
Common Device Configuration	Choose the Common Device Configuration to which you want the ATA 191 assigned. To see the Common Device Configuration settings, click the View Details link.
Phone Button Template	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Common Phone Profile	From the drop-down list, choose a common phone profile from the list of available common phone profiles. To see the Common Phone Profile settings, click the View Details link.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
AAR Calling Search Space	From the drop-down list, choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) or leave the calling search space as the default of <None>.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. If you choose **<None>**, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list, choose the user locale that is associated with the CTI Port. The user locale identifies a set of detailed information to support users, including language and font. If you do not specify a user locale, Cisco Unified CM uses the user locale that is associated with the device pool.
Network Locale	From the drop-down list, choose the network locale that is associated with the CTI Port. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. If you do not specify a network locale, Cisco Unified CM uses the network locale that is associated with the device pool.

Field	Description
Built in Bridge	Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list. Choose one of the following: • On • Off • Default
Privacy	For Privacy, choose **On** in the Privacy drop-down list.
Device Mobility Mode	From the drop-down list, turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device.
Owner	Select **User** or **Anonymous (Public/Shared Space)** , for the owner type.
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from "Unassigned Devices" to "Users" in the License Usage Report. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.
Phone Load Name	Enter the custom software for ATA 191.
Use Trusted Relay Point	Choose one of the following values: • **Off**—Choose this value to disable the use of a Trusted Relay Point (TRP) with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

Field	Description
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
Geolocation	From the drop-down list, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified Communications Manager ignores any presentation restriction that is received for internal calls. Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call.
Logged into Hunt Group	When the ATA 191 gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	Check this box to allocate a buffer for the device when it registers and to bundle SCCP messages to the phone. **Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays.

Field	Description
Protected Device	Check this check box to designate a phone as protected, which enables the phone to play a 2-second tone to notify the user when a call is encrypted and both phones are configured as protected devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are protected and the call occurs over encrypted media. Checking this check box represents only one of several configuration requirements for the secure indication tone to play. For a detailed description of the secure indication tone feature and the configuration requirements, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html. If you check this check box and the system determines that the call is not encrypted, the phone plays nonsecure indication tone to alert the user that the call is not protected.

Number Presentation Transformation

Table 21: Caller ID for Calls From This Phone

Field	Description
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.

Table 22: Remote Number

Field	Description
Calling Party Transformation CSS	From the drop-down list, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this device.
Use Device Pool Calling Party Transformation CSS	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this device belongs to transform the remote calling and remote connected number.

Table 23: Protocol Specific Information

Field	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list: • **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • **Batch Processing Mode**—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.
BLF Presence Group	From the drop-down list, choose a Busy Lamp Field (BLF) presence group for the end user. The selected group specifies the destinations that the end user can monitor The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list.
SIP Dial Rules	If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed. Leave the SIP Dial Rules field set to <None> if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed.
MTP Preferred Originating Codec	From the drop-down list, choose the codec to use if a media termination point is required for SIP calls.

Field	Description
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all devices that are configured in Unified Communications Manager Administration.
Rerouting Calling Search Space	From the drop-down list, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the "405 Method Not Allowed" message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you can configure a calling search space as you do all calling search spaces.
SIP Profile	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security). Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. After you save the phone configuration and apply the configuration update to the phone, the digest credentials for the user get added to the phone configuration file. For more information on digest authentication, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html .

Field	Description
Media Termination Point Required	Use this field to indicate whether a media termination point is used to implement features that ATA 191 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features. Use this check box only for ATA 191 clients and those ATA 191 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.
Unattended Port	Check this check box to indicate an unattended port on this device.
Required DTMF Reception	For devices that are running SIP and SCCP, check this check box to require DTMF reception for this phone. **Note** In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.

Table 24: Certification Authority Proxy Function (CAPF) Information

Field	Description
Certificate Operation	From the drop-down list, choose one of the following options: • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone. For more information on CAPF operations, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Field	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list, choose one of the following options: • By Authentication String—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • By Null String— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. • By Existing Certificate (Precedence to LSC)—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. • By Existing Certificate (Precedence to MIC)—Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Authentication String	If you chose the **By Authentication String** option in the **Authentication Mode** drop-down list, this field applies. Manually enter a string or generate a string by clicking the **Generate String** button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.

Field	Description
Key Size (Bits)	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list. The default setting equals 1024. Other options include 512 and 2048. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Operation Completes by	This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation. The values that display apply for the publisher database server.
Certificate Operation Status	This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot Certificate Operation options. You cannot change the information that displays in this field.

Table 25: Secure Shell User

Field	Description
Secure Shell User	Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include ",%, &, <, >, and \. This field displays when the phone device that you are configuring supports SSH access. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH credentials to the phone in the clear.

Field	Description
Secure Shell Password	Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 127 characters. Invalid characters include ",%, &, <, >, and \. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH passwords to the phone in the clear.

Table 26: Product-Specific Configuration Layout

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, see the documentation for ATA 191.