Network Configuration

Web-Based Configuration Utility

Your phone system administrator can allow you to view the phone statistics and modify some or all the parameters. This section describes the features of the phone that you can modify with the phone web user interface.

Access the Phone Web Interface

If your service provider has disabled access to the configuration utility, contact the service provider before proceeding.

Procedure

Step 1 Ensure that the computer can communicate with the phone. No VPN in use.

Step 2 Start a web browser.

Step 3 Enter the IP address of the phone in your web browser address bar.

- User or Admin Access: **`https://<ip address>:<port>/`**, and then enter the username and password.

For example, `https://10.64.84.147/`

Allow Web Access to the ATA

To view the ATA parameters, enable the configuration profile. To make changes to any of the parameters, you must be able to change the configuration profile. Your system administrator might have disabled the option to make the ATA web user interface viewable or writable.

For more information, see the *Cisco ATA 191 and 192 Multiplatform Firmware Provisioning Guide*

Before you begin

Access the phone administration web page. See Access the Phone Web Interface, on page 1.

Procedure

Step 1 Click **System**.

Step 2 In the **System Configuration** section, set **Enable Web Server** to **Yes**.

Step 3 To update the configuration profile, click **Submit All Changes** after you modify the fields in the phone web user interface.

The phone reboots and the changes are applied.

Step 4 To clear all changes that you made during the current session (or after you last clicked **Submit All Changes**), click **Undo All Changes**. Values return to their previous settings.

Basic Setup

Use the **Network Setup** > **Basic Setup** pages to configure your Internet connection, local network settings (ATA 192 only), and your time settings.

Network Service (ATA 192 Only)

Use the **Network Setup** > **Basic Setup** > **Network Service** page to configure the operating mode of the ATA 192.

After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

You can configure the ATA to operate in one of the following modes:

- **NAT:** Network Address Translation (NAT) allows multiple devices on a private network to share a public, routable IP address. In order for theVoice over IP service to co-exist with NAT, some form of NAT traversal is required either on the ATA or another network device. Use this option if your ATA connects to one network on the WAN port and to another network on the LAN port. This option is selected by default and is suitable for most deployments.

- **Bridge:** Bridged mode is used if the ATA is acting as a bridge device to another router. Choose this option if your ATA bridges a network to its LAN port (with connected devices also in the 10.0.0x range).

- **Monitor Network Drop on Internet Port Only:** This parameter is used for how to report the link state when both Ethernet(LAN) and Network(WAN) ports are connected.

  - **Off**: If you unplug and plug the WAN cable, meanwhile the LAN port state is still UP, then the ATA doesn't perform any operation.

  - **On**: If you unplug and then plug the WAN cable, then the ATA triggers a warm reboot even though the LAN port state is still UP. In this case, the ATA will try to register again.

Note

- The parameter takes effect only when you select the **Bridge** mode.
- The parameter doesn't take effect when only the WAN port is connected.

Basic Settings

Use the **Network Setup** > **Basic Settings** page to set up your basic network settings.

Table 1: Basic Settings

Field	Description
Domain Name	The domain name, if specified by your ISP. Otherwise, leave the field blank.
Host Name	The name of the ATA. The default value is the model number. Your ISP may specify a host name to use.
Stack mode	Choose the stack mode for network; there are three modes can be set: IPv4 only, Pv6 Only, or Dual.
Signaling Preference	Choose the SIP packet preference, either IPv4 or IPv6.
Media Preference	Choose the RTP packet preference, either is IPv4 or IPv6.

IPv4 Settings

Use the **Network Setup** > **Basic Setup** > **IPv4 Settings** page to set up your IPv4 connection.

Enter the settings as described in the table. After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Table 2: Internet Connection Type

Field	Description
Connection Type	Specify the Internet addressing method that your ISP requires. Default setting: Automatic Configuration - DHCP • **Automatic Configuration - DHCP:** Use this setting if your ISP dynamically provides an IP address. No additional settings are required on this page. • **Static IP:** Use this setting if your ISP assigned a static IP address. Complete the fields that appear. • **PPPoE (DSL service):** Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. Complete the fields that appear.

Field	Description
Static IP Settings	• **Internet IP Address and Subnet Mask:** Enter the IP address and subnet mask that was assigned to your account by your service provider. This address is seen by external users on the Internet. • Default Gateway: Enter the Gateway IP Address that was provided by your ISP. If needed, you can adjust the MTU and Optional Settings.
PPPoE Settings	• **User Name and Password:** Enter the user name and password that you use to log in to your ISP network through a PPPoE connection. • Service Name: If provided by your ISP, enter the Service Name. • **Connect on Demand:** You can configure the ATA to disconnect your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has timed out, this feature also enables the ATA to re-establish your connection when you attempt to access the Internet again. If you choose this option, also set the Max Idle Time. • **Keep Alive:** This option keeps you connected to the Internet indefinitely, even when your connection sits idle. If you choose this option, also set the Redial Period, which is the interval at which the ATA verified Internet connectivity. The default period is 30 seconds. If needed, you can adjust the MTU and Optional Settings.
MTU	The Maximum Transmission Unit (MTU) setting specifies the largest protocol data unit (in bytes) permitted for network transmission. Generally, a larger MTU means greater efficiency. However, a larger packet may cause delays for other traffic and is more likely to become corrupted. Usually, you keep the default setting to allow the ATA to choose the appropriate MTU. To specify the MTU, select Manual, and then enter the number of bytes.

Table 3: Optional Settings

Field	Description
DNS Server Order	Choose the preferred method for choosing a DNS server. • **DHCP-Manual—**The DNS server settings from the network server takes precedence, and your entries in the DNS fields are used only as a backup. • **Manual-DHCP—**Your entries in the DNS fields take precedence, and the DNS server settings from the network server are used as a backup. • **Manual—**Your entries in the DNS fields are used to choose a DNS server.
Primary DNS	Set the Primary DNS for IPv4.
Secondary DNS	Set the Secondary DNS for IPv4.

IPv6 Settings

Use the **Network Setup** > **Basic Setup** > **IPv6 Settings** page to set up your IPv6 connection.

Enter the settings as described in the table. After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Table 4: IPv6 Settings

Field	Description
Internet Connection Type	Specify the Internet addressing method that your ISP requires. Default setting: Automatic Configuration - DHCP Automatic Configuration - DHCP: Use this setting if your ISP dynamically provides an IP address. No additional settings are required on this page. Static IP: Use this setting if your ISP assigned a static IP address. Complete the following fields: • Internet IPv6 Address and Prefix Length—Enter the IPv6 address and prefix length that was assigned to your account by your service provider. The public sees this address. • Default Gateway—Enter the Gateway IPv6 Address that was provided by your ISP. PPPoE (DSL service): Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. Complete the following fields: • User Name and Password—Enter the username and password that you use to log in to your ISP network through a PPPoE connection. • Service Name—If provided by your ISP, enter the Service Name. • Connect on Demand—You can configure the ATA to disconnect your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has timed out, this feature enables the ATA to automatically reconnect when you try to access the Internet again. If you choose this option, also set the Max Idle Time. • Keep Alive—This option keeps you connected to the Internet indefinitely, even when your connection sits idle. If you choose this option, also set the Redial Period, which is the interval at which the ATA verified Internet connectivity. The default period is 30 seconds.

Table 5: Optional Settings

Field	Description
DNS Server Order	Choose the preferred method for choosing a DNS server. • DHCP-Manual—The DNS server settings from the network server takes precedence, and your entries in the DNS fields are used only as a backup. • Manual-DHCP—Your entries in the DNS fields take precedence, and the DNS server settings from the network server are used as a backup. • Manual—Your entries in the DNS fields are used to choose a DNS server.
Allow Auto Configuration.	Enable if you want to allow Auto Configuration.
Primary DNS	Set the Primary DNS for IPv6.
Secondary DNS	Set the Secondary DNS for IPv6.

IPv4 LAN Settings (ATA 192 Only)

Use the **Network Setup** > **Basic Setup** > **IPv4 LAN Settings** page to set the IP address and subnet mask for your local network. Also configure the settings for the built-in DHCP server (ATA 192 only).

After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Router IP

Enter the **Local IP Address** and **Subnet Mask** for your local network. The default setting is 192.168.15.1 with a subnet mask of 255.255.255.0.

DHCP Server Setting

Field	Description
DHCP Server	The ATA can use the built-in DHCP server to dynamically assign IP addresses to connected devices. Click **Enabled** to enable the DHCP server, or click**Disabled** to disable this feature. Default setting: Enable

Field	Description
IP Reservation	Click the Show DHCP Reservation button to view and manage the DHCP client list. Click the Hide DHCP Reservation button to hide the list. When the list is displayed, you can perform the following tasks: • To reserve a static IP address for a current DHCP client: Check the box for the client in the **Select Clients from DHCP Tables** list. Click**Add Clients**. The selected clients are added to the *Clients Already Reserved* list. These clients have static IP addresses that do not change. • To add a client that isn't in the Select Clients from DHCP Tables list: Type a name for the client in the **Enter Client Name** box. Enter an IP address for this client in the **Assign IP Address** box. Enter the MAC address in the following format:00:00:00:00:00:00. Click **Add**. • To remove a client from the **Clients Already Reserved** list: Check the box for the client. Click **Remove**.
Default Gateway	Enter the IP address of the default gateway to be used by the DHCP clients. Default setting: 192.168.15.1 (the IP address of the ETHERNET (LAN) interface)
Starting IP Address	Enter the first address in the range of addresses assigned dynamically by the DHCP server. Default setting: 192.168.15.100
Maximum DHCP Users	Enter the maximum number of devices that can dynamically receive, or “lease,” DHCP addresses from the DHCP server. Default setting: 50 **IMPORTANT**: Typically, the ATA can support up to five connected computers for business-related tasks such as web browsing and viewing email. The ATA is not designed to support streaming music, video, games, or other network traffic-intensive tasks.
Client Lease Time	Enter the number of minutes that a dynamically assigned IP address can be in use, or “leased.” After this time elapses, a client device has to request a DHCP lease renewal. Use 0 to represent 1 day, 9999 never expire. Default setting: 0

Field	Description
Option 66	Provides provisioning server address information to hosts that request this option. Server information can be defined in one of three ways: • **None**: The ATA uses its own TFTP server to source provisioning files, so it returns its own local IP address to the client. • **Remote TFTP Server**: The ATA was configured by using this method, and received server information through Option 66 on its WAN interface. In response to client requests, it provides the remote TFTP server information. • **Manual TFTP Server**: Allows the manual configuration of a configuration server address. This option is used to provide either an IP address or a fully qualified hostname. But the ATA also accepts and offers a full URL including protocol, path, and filename to meet the requirements of specific clients. Default setting: None
TFTP Server	If you chose Manual TFTP Server for Option 66, enter the IP address, hostname, or URL of the TFTP server. Default setting: blank
Option 67	Provides a configuration or bootstrap filename to hosts that request this option. This option is used with option 66 to allow a client to form an appropriate TFTP request for the file. Default setting: blank
Option 159	Provides a configuration URL to clients that request this option. An option 159 URL defines the protocol and path information by using an IP address for clients that cannot use DNS. For example: https://10.1.1.1:888/configs/bootstrap.cfg Default setting: blank
Option 160	Provides a configuration URL to clients that request this option. An option 160 URL defines the protocol and path information by using a fully qualified domain name for clients that can use DNS. For example: https://myconfigs.cisco.com:888/configs/bootstrap.cfg Default setting: blank
DNS Proxy	When enabled, the DNS proxy relays DNS requests to the current public network DNS server. It also replies as a DNS resolver to the client device on the network. Click **Enabled** to enable this feature, or click**Disabled** to disable it. If DNS proxy is disabled, then DHCP clients are offered DNS server information by using the Static DNS servers or by using the servers specified for the INTERNET (WAN) interface.

IPv6 LAN Setting (ATA 192 Only)

Use the **Network Setup** > **Basic Setup** > **IPv6 LAN Settings** page to set up your IPv6 LAN connection.

Enter the settings as described in the table. After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Table 6: Internet Connection Type

Field	Description
DHCP Server	Click **Enabled** to enable the DHCP server, or click **Disabled** to disable this feature. Default setting: Enable
Address Assign Type	Choose the address assign type: SLAAC/DHCPv6.
DHCPv6 Delegation	Choose whether to support DHCPv6 delegation, if Yes, user can't configure **IPv6 Address Prefix**.
IPv6 Address Prefix	Set the IPv6 address prefix for IPv6 LAN interface, the Prefix Length is fixed to 64.
IPv6 Address Length	Set the IPv6 address prefix length for IPv6 LAN interface. Range:1-112
IPv6 Static DNS	Set the IPv6 Static DNS.
LAN IPv6 Address	Display the LAN IPv6 address information.

Time Settings

Use the **Network Setup** > **Basic Setup** > **Time Settings** page to set the system time for the ATA. By default, the system time is set automatically by using a Network Time Protocol (NTP) server. You can configure the system time manually. In addition, you can use this page to specify your time zone, enable Daylight Saving adjustments, and modify related settings.

After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Note If the ATA doesn't receive the response from the NTP server, then the system time for the ATA uses the build date and time of the firmware.

User Manual

If you prefer to set the system manually, click **User Manual** and then enter the date and time.

Table 7: Time Settings

Field	Description
Date	Enter the date in the following order: four-digit year, month, day.
Time	Enter the time in the following order: hour (from 1 to 24), minutes, and seconds.

Time Zone

To use a time server to establish the time settings, select Time Zone. Then complete the fields in this section.

Table 8: Time Zone Settings

Field	Description
Time Zone.	Choose the time zone for the site where the ATA is in operation. Default setting: (GMT-08:00) Pacific Time (USA & Canada).
Adjust Clock for Daylight Saving Changes.	Check the box if you want to automatically adjust the time when Daylight Savings Time is in effect. Otherwise, uncheck the box.
Time Server Address.	To use the ATA's default Network Time Protocol (NTP) server, select Auto from the drop-down list. If you want to specify the NTP server, select Manual, and then enter the NTP server address. Default setting: Auto
Resync Timer	Enter the Resync timer interval value (in seconds). This timer controls how often the ATA resynchronizes with the NTP server. Default setting: 3600 seconds
Auto Recovery After Reboot	Choose this option to allow the ATA to automatically reconnect to the time server after a system reboot. Default setting: Disabled

Advanced Settings

Use the **Network Setup** > **Advanced Settings** pages to configure features including port flow control, MAC address cloning, VPN passthrough, and VLAN.

Port Setting (ATA 192 Only)

Use the **Network Setup** > **Advanced Settings** > **Port Setting** page to set the ETHERNET (LAN) port attributes.

After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Table 9: Port Settings

Field	Description
Flow Control	Flow control is a mechanism that temporarily stops the transmission of data on a port. For example, a device is transmitting data faster than some other part of the network can accept it. The overwhelmed network element halts the transmission of the sender for a specified time. Choose **Enabled** to enable this feature, or choose **Disabled** to disable this feature. Default setting: Enabled

Field	Description
Speed Duplex	Choose the duplex mode. You can select from Auto-negotiate, 10 Half, 10 Full, 100 Half and 100 Full. Cisco recommends that choosing Auto-negotiate to automatically select the appropriate mode for the traffic. Use caution with other settings. Problems can result if you choose a setting that is not appropriate for the network devices. Default setting: Auto-negotiate

MAC Address Clone

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification purposes. Some ISPs require that you register a MAC address in order to access the Internet. If you previously registered your account with another MAC address, it may be convenient to assign that MAC address to your ATA. You can use the **Network Setup** > **Advanced Settings** > **MAC Address Clone** page to assign a MAC address that you previously registered with your Service Provider.

After making changes, click Submit to save your settings, or click Cancel to redisplay the page with the saved settings.

Table 10: MAC Address Clone Settings

Field	Description
MAC Clone	Click Enabled to enable MAC address cloning, or click Disabled to disable this feature. Default setting: Disabled.
MAC Address	Enter the MAC address that you want to assign to your ATA. If your computer's MAC address is the address that you previously registered for your ISP account, click **Clone Your PC's MAC**. Your computer's MAC address appears in the *MAC Address* field. Default setting: the current MAC address of your ATA

VPN Passthrough (ATA 192 Only)

Use the **Network Setup** > **Advanced Settings** > **VPN Passthrough** page to configure VPN passthrough for IPsec, PPTP, and L2TP protocols. Use this feature if there are devices behind the ATA that require an independent IPsec tunnel. For example, a device may need to use a VPN tunnel to connect to another router on the WAN.

By default, VPN Passthrough is enabled for IPsec, PPTP, and L2TP.

After making changes, click Submit to save your settings, or click Cancel to redisplay the page with the saved settings.

Table 11: VPN Passthrough Settings

Field	Description
IPsec Passthrough	Internet Protocol Security (IPsec) is a suite of protocols used to implement secure exchange of packets at the IP layer. Click **Enabled** to enable this feature, or click **Disabled** to disable it. Default setting: Enabled
PPTP Passthrough	Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To disable PPTP Passthrough, select Disabled. Default setting: Enabled
L2TP Passthrough	Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions using the Internet on the Layer 2 level. Click **Enabled** to enable this feature, or click **Disabled** to disable it. Default setting: Enabled

VLAN

Use the **Network Setup** > **Advanced Settings** > **VLAN** page to assign a VLAN ID to your network. For example, your call control system may require a particular voice VLAN ID.

After making changes, click Submit to save your settings, or click Cancel to redisplay the page with the saved settings.

Table 12: VLAN Settings

Field	Description
Enable VLAN.	Click Enabled to enable a VLAN, or click Disabled to disable this feature. Default setting: Disabled
VLAN ID	The VLAN ID can be any numeral from 1 to 4094. When VLAN is enabled, the default setting is 1.

CDP and LLDP

Device discovery protocols enable directly connected devices to discover information about each other. You may wish to enable these protocols to allow your network management system to learn about your ATA and endpoints. Use the **Network Setup** > **Advanced Settings** > **CDP & LLDP** page to specify the settings for Cisco Discovery Protocol (CDP) and the Link Layer Discovery Protocol (LLDP). When enabled, the ATA sends messages to a multicast address and listens to the messages sent by other devices using the protocol.

After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Application

Use the **Network Setup** > **Application** pages to support voice service and any servers that you host for public access.

Quality of Service (QoS) (ATA 192 Only)

Use the **Network Setup** > **Application** > **QoS** page to set the upstream bandwidth to suit your broadband service. This feature is enabled by default and helps to ensure that voice is prioritized during periods of heavy network traffic.

After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Table 13: QoS Settings

Field	Description
QoS Policy	Click **Always On** to enable QoS settings always, or click **On When Phone In Use** to enable it only when there is voice traffic. Default setting: On When Phone In Use
Upstream Bandwidth	Enter the maximum available upstream bandwidth value specified by your Internet Service Provider. Default setting: 100000 kbps Important: Do not overstate the upstream bandwidth that you receive from your service provider. Setting this value higher than the available service bandwidth can result in traffic being dropped arbitrarily in the service provider's network.

Port Forwarding (ATA 192 Only)

Use the **Network Setup** > **Application** > **Port Forwarding** page if you require access to specific ports from external devices.

List of Port Forwarding

To add a port forwarding rule, click Add Entry. To edit a port forwarding rule, select it in the list and then click the pencil icon. To remove a port forwarding rule, click the delete icon.

Table 14: Port Forwarding Settings

Field	Description
Number	An identification number for the port forwarding rule.
Type	The type of rule: Single Port Forwarding or Port Range Forwarding.
Status	The status of the rule: Enabled or Disabled.

Field	Description
Application	The application that uses this rule to access a network resource.

Port Forwarding Details

To display the details, click an entry in the **List of Port Forwarding**.

Table 15: Port Settings

Field	Description
External Port	The port that external clients use to set up this connection.
Internal Port	The port that the ATA uses when forwarding traffic to the internal server.
Protocol	The protocol that is used: TCP or UDP.
IP Address	The IP address of the internal server accessed by this rule.

Manually Add Port Forwarding (ATA 192 Only)

Use this page to enter the port forwarding settings for an application.

Enter the settings as described. After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Table 16: Port Forwarding Settings

Field	Description
Port Forwarding Type	Choose the type of port forwarding: • **Single Port Forwarding**: Forwards traffic for a specified port to the same or an alternate port on the target server in the LAN. • **Port Range Forwarding**: Forwards traffic to a range of ports to the same ports on the target server in the LAN. See the Internet application’s documentation for the required ports or ranges.
Application Name	For single port forwarding, choose a common application from the drop-down list (such as Telnet, or DNS). To add an application that is not on the list, choose **Add a new name**, and then enter the name in the **Enter a Name** field.
Enter a Name	If you chose Port Range Forwarding, or if you chose **Add a new name** in the Application Name list for Single Port Forwarding, enter a name to identify the application.

Field	Description
External Port, Internal Port	For Single Port Forwarding, specify the ports to use. For simplicity, the internal and external port numbers are often the same. Different external port numbers could be used to differentiate traffic of the same application type intended for different servers, or for privacy by using non-standard ports. • **External port**: For single port forwarding, enter the port number that external clients use to set up a connection with the internal server. • **Internal port:** For single port forwarding, enter the port number that the ATA uses when forwarding traffic to the internal server. The correct entries appear automatically if you choose a standard application from the Application Name list for Single Port Forwarding.
Start - End Port	For Port Range Forwarding, specify the range of ports to use. Valid values are from 1 to 65535.
Protocol	Select the protocols that can be forwarded: TCP, UDP, or TCP and UDP.
IP Address	Enter the IP address of the local server that receives forwarded traffic. For correct forwarding of traffic, local servers must either be configured with a static IP address, or be assigned a reserved IP address through DHCP. Use the Interface Setup > LAN > DHCP Server page to reserve IP addresses.
Enabled	Check the box to enable this port forwarding rule, or uncheck the box to disable it. Default setting: Disabled

DMZ (ATA 192 Only)

Use the **Network Setup** > **Application** > **DMZ** page if you want a local device exposed to the Internet for a special-purpose service.

The specified network device must have its DHCP client function disabled. It must also have a reserved IP address to ensure that it is reachable at the specified IP address.

Note A Demilitarized Zone (DMZ) is similar to Port Range Forwarding. Both features allow Internet traffic to access a resource on your private network. However, Port Range Forwarding is more secure because it only opens the ports that you specify for an application. DMZ hosting opens all the ports of one device, exposing it to the Internet.

Enter the settings as described. After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Table 17: DMZ Settings

Field	Description
Staus.	Click **Enabled** to enable this feature, or click **Disabled** to disable it. Default setting: Disabled
Private IP.	Specify the local IP address of the device that can be accessed through the DMZ.

HTTP Proxy (ATA 191 and 192)

Use the **Network Setup** > **Application** > **HTTP Proxy** page to set up a proxy server for the ATA to enhance security. A proxy server acts as a firewall between the ATA and Internet. After successful configuration, the ATA connects to Internet through the proxy server which protects the ATA from cyber attack.

You can set up a proxy server by either using an automatic configuration script or by manually configuring the host server (hostname or IP address) and port of the proxy server.

After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

When the ATA is configured with the HTTP proxy feature, the feature applies to all the applications that use the HTTP protocol. The applications include the following:

- Profile Rule B, C, and D
- Log Resync Request, Success, and Failure Msg
- Report Rule
- Upgrade Rule
- Custom CA URL
- E911 Request URL
- EDOS RC Server
- TR69 (ACS URL)
- PRT Upload URL

Table 18: HTTP Proxy Settings

Field	Description
Proxy Mode	Choose the HTTP proxy mode: • **Auto**: The ATA automatically retrieves a Proxy Auto-Configuration (PAC) file to select a proxy server. In this mode, you can determine whether to use Web Proxy Auto-Discovery (WPAD) protocol to retrieve a PAC file or manually enter a valid URL of the PAC file. For details about the fields, see Use Auto Discovery (WPAD) and PAC URL. • **Manual**: You must manually specify a server (hostname or IP address) and a port of a proxy server. For details about the fields, see Proxy Host and Proxy Port. • **Off**: You disable the HTTP proxy feature on the ATA. Default setting: Off
Use Auto Discovery	Click **Yes** to use the Web Proxy Auto-Discovery (WPAD) protocol to retrieve a PAC file automatically. Click **No** to specify the URL of a PAC file manually. For details about the field, see PAC URL. Default setting: Yes
PAC URL	Specify the URL of a PAC file. For example, `http://proxy.department.branch.example.com` TFTP, HTTP, and HTTPS are supported. The field must be configured when the **Proxy Mode** is **Auto** and **Use Auto Discovery** is **No**. Default setting: Blank
Proxy Server Requires Authentication	Enter the authentication credentials (username and password) if the proxy server requires. This field is configured according to the actual behaviour of the proxy server. For details about the fields, see Username and Password. Default setting: No
Proxy Host	IP address or hostname of the proxy host server for the ATA to access. For example: `proxy.example.com` The scheme (http:// or https://) is not required. Default setting: Blank
Proxy Port	Port number of the proxy host server. The value range is from 2 to 65535. Default setting: 3128

Field	Description
Username	Username for a credential user on the proxy server. If **Proxy Mode** is set to **Manual** and **Proxy Server Requires Authentication** is set to **Yes**, you must configure the field. Default setting: Blank
Password	Password of the specified username for the proxy authentication purpose. If **Proxy Mode** is set to **Manual** and **Proxy Server Requires Authentication** is set to **Yes**, you must configure the field. Default setting: Blank