5

Administration Settings

This chapter describes the administrative settings for the ATA. It includes the following sections:

- **Management**
- **Logging**
- **Diagnostics**
- **Factory Defaults**
- **Firmware Upgrade**
- **Configuration Management**
- **Reboot**

Management

Use the *Management* pages to manage web access to the configuration utility and to enable protocols for remote configuration and network management.

- **Web Access Management**
- **TR-069**
- **SNMP**
- **User List (Password Management)**
- **Bonjour**
- **Reset Button**

Web Access Management

Use the *Administration > Management > Web Access Management* page to configure the settings for access to the administration of the ATA.

To open this page: Click **Administration** in the menu bar, and then click **Management > Web Access Management** in the navigation tree. After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Web Access

Field	Description
Admin Access	This feature controls access to the configuration utility from devices that are connected via the ETHERNET (LAN) port. Click **Enabled** to enable this feature, or click **Disabled** to disable it. The default setting is Enabled. If you administer and configure the ATA from a computer that is connected to the LAN, this feature must be enabled.
Web Utility Access	Select the protocol to use for access to the configuration utility from a device on the WAN. Choose **HTTP** and/or **HTTPS**. For secure Internet access, select **HTTPS**. The default value is HTTP.

Remote Access

Field	Description
Remote Management	Allows access to the configuration utility from a device that is on the WAN side of the ATA. For example, you could connect from another subnet in your office or from your home computer. Click **Enabled** to enable this feature, or click **Disabled** to disable it. The default setting is Disabled. The other fields in this section of the page are available only if you enable this feature. If you attempt to enable this feature while using the default administrator login credentials, you will be prompted to change the credentials. Click **OK** to acknowledge the warning message. Use the *Administration > Management > User List* page to change administrator password. For more information, see **User List (Password Management), page 185**.
Web Utility Access	Select the protocol to use for access to the configuration utility from a device on the WAN side of the ATA. Choose **HTTP** and/or **HTTPS**. For secure Internet access, select **HTTPS**. The default value is HTTP. Include the specified protocol when you enter the address in your web browser. For example, with the HTTPS protocol, a WAN IP address of 203.0.113.50, and the default Remote Management Port of 80, you would enter: *https://203.0.113.50:80*
Remote Upgrade	If you enabled Remote Management, choose whether or not to allow firmware upgrades from a device on the WAN side of the ATA. Click **Enabled** to enable this feature, or click **Disabled** to disable it. The default value is Disabled. You can change this setting only when your computer is connected to the configuration utility from the LAN.

Field	Description
Allowed Remote IP Address	You can use this feature to limit access to the configuration utility based on the IP address of a device. Choose **Any IP Address** to allow access from any external IP address. To specify an external IP address or range of IP addresses, select the second radio button and then enter the desired IP address or range. The default setting is Any IP Address.
Remote Management Port	Enter the port number to use for access to the configuration utility from a device on the WAN side of the ATA. The default port number is 80. Include the specified port when you enter the address in your web browser. For example, with the HTTPS protocol, a WAN IP address of 203.0.113.50, and the default Remote Management Port of 80, you would enter: *https://203.0.113.50:80*

TR-069

Use the *Administration > Management > TR-069* page to configure communication with an Auto-Configuration Server (ACS) via TR-069 CPE WAN Management Protocol (CWMP). TR-069 (Technical Report 069) provides a common platform to manage all voice devices and other customer-premises equipment (CPE) in large-scale deployments. It provides the communication between the CPE and the ACS.

To open this page: Click **Administration** in the menu bar, and then click **Management > TR-069** in the navigation tree.

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

Field	Description
Status	Click **Enabled** to enable remote provisioning, or click **Disabled** to disable this feature. The default setting is Disabled.

Field	Description
ACS URL	The URL for the ACS. The format should be http(s)://xxx.xxx.xxx.xxx:port or xxx.xxx.xxx.xxx:port. The xxx.xxx.xxx.xxx is the domain name or IP address of the ACS server. Both the IP address and the port number are required.
ACS Username	The username for the ACS. The default username is the Organization Unit Identifier (OUI). This value is required and must match the username configured on the ACS.
ACS Password	The password for the ACS. This value is required and must match the password configured on the ACS.
Connection Request Port	The port to use for connection requests
Connection Request Username	The username for connection requests. This value must match the Connection Request Username configured on the ACS.
Connection Request Password	The password for connection requests. This value must match the Connection Request Password configured on the ACS.
Periodic Inform Interval	If Periodic Inform is enabled, the duration, in seconds, between CPE attempts to connect to the ACS. The default value is 86400 seconds.
Periodic Inform Enable	Click **Enabled** to enable CPE connection requests to the ACS, or click **Disabled** to disable this feature.
Request Download	If applied, ACS may call the Download RPC after it receives the request from the ATA.

SNMP

Use the *Administration > Management > SNMP* page to set up Simple Network Management Protocol (SNMP) for the ATA.

SNMP is a network protocol that allows network administrators to manage, monitor, and receive notifications of critical events as they occur on the network. The ATA supports SNMPv2 and SNMPv3. It acts as an SNMP agent that replies to SNMP commands from SNMP Network Management Systems. It supports the standard SNMP get, next, and set commands. It also generates SNMP traps to notify the SNMP manager when configured alarm conditions occur. Examples include reboots, power cycles, and INTERNET (WAN) events.

To open this page: Click **Administration** in the menu bar, and then click **Management > SNMP** in the navigation tree.

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

Settings for SNMPv2

Field	Description
Enabled, Disabled	Click **Enabled** to enable this feature, or click **Disabled** to disable it. The default setting is Disabled.
Trusted IP	Choose **Any** to allow access from any IP address (not recommended). Click **Address** to specify the IP address and subnet mask of a single SNMP manager or trap agent that can access the ATA through SNMP.
Get/Trap Community	Enter a community string for authentication for SNMP GET commands. The default value is public.
Set Community	Enter a community string for authentication for SNMP SET commands. The default value is private.

Settings for SNMPv3

Field	Description
Enabled, Disabled	Click **Enabled** to enable this feature, or click **Disabled** to disable it. The default setting is Disabled.
R/W User	Enter the user name for SNMPv3 authentication. The default value is v3rwuser.
Auth-Protocol	Choose the SNMPv3 authentication protocol from the drop-down list (HMAC-MD5 or HMAC-SHA).
Auth-Password	Enter the authentication password.
PrivProtocol	Choose a privacy authentication protocol from the drop-down list (None or CBC-DES). If you select CBCDES, the privKey encrypts the data portion of the message that is being sent.
Privacy Password	Enter the key for the authentication protocol to use.

Trap Configuration

Field	Description
IP Address	The IP Address of the SNMP manager or trap agent.
Port	The SNMP trap port used by the SNMP manager or trap agent to receive the trap messages. Valid entries are 162 or 1025~65535. The default value is162.
SNMP Version	The SNMP version in use by the SNMP manager or trap agent. Choose a version from the list.

User List (Password Management)

Use the *Administration > Management > User List* page to manage the two user accounts for the configuration utility. The administrator-level account has the default username **admin** and password **admin**. The user-level account has access to modify a limited set of features. This account has the default username **cisco** and password **cisco**.

For the IVR, no user password is required; the user simply presses # when prompted. The default administrator password is 1234#. You can configure these passwords on the **System** page.

To open this page: Click **Administration** in the menu bar, and then click **Management > User List** in the navigation tree.

To update a password:

STEP 1 In the *User List* table, click the pencil icon for the account that you want to update.

STEP 2 On the *User Account* page, enter the username and password, as described below.

- **Username:** Enter a username.
- **Old Password (administrator account only):** Enter the existing password. The default administrator password is **admin**. The default guest password is **cisco**.
- **New Password:** Enter up to 32 characters for your new password.
- **Confirm New Password:** Enter the new password again, to confirm.

STEP 3 After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Bonjour

Use the Administ*ration* > *Management* > *Bonjour* page to enable or disable Bonjour. Bonjour is a service discovery protocol that locates network devices such as computers and servers on your LAN. It may be required by network management systems that you use. When this feature is enabled, the ATA periodically multicasts Bonjour service records to its entire local network to advertise its existence.

To open this page: Click **Administration** in the menu bar, and then click **Management > Bonjour** in the navigation tree.

Click **Enabled** to enable this feature, or click **Disabled** to disable it. The default setting is Enabled. After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Reset Button

To open this page: Click **Administration** in the menu bar, and then click **Management > Reset Button** in the navigation tree.

Click **Enabled** to enable the reset button, or click **Disabled** to disable it. The default setting is Enabled. After making changes, click **Submit** to save your settings, or click **Cancel** to redisplay the page with the saved settings.

Logging

The ATA allows you to record incoming, outgoing, and DHCP lists for various events that occur on your network.The Incoming Log displays a temporary list of the source IP addresses and destination port numbers for the incoming Internet traffic. The Outgoing Log displays a temporary list of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic.

See these topics:

- **Log Module**
- **Log Setting**
- **Log Viewer**

Log Module

Use the *Administration > Log > Log Module* page to enable and configure logging.

To open this page: Click **Administration** in the menu bar, and then click **Log > Log Module** in the navigation tree.

NOTE

- As a best practice, Cisco recommends that you enable logging only when needed, and disable logging when you finish the investigation. Logging consumes resources and can impact system performance.
- If you want to enable email or syslog server logging, first specify the email or syslog server settings on the *Log Setting* page.

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

Field	Description
Status	Click **Enabled** to enable logging, or click **Disabled** to disable logging. The default setting is Disabled.
Log - Enable	Check the box in the heading row to enable logging for all services (kernel and system). Alternatively, check the box for kernel or system to enable logging for that service.
Service	The type of service to include: kernel or system.

Field	Description
Priority	The types of events to include in the log. The lowest level of logging is Emergency, which is limited to messages about high impact events. The highest level of logging is Debugging, which includes all message types from Emergency upward. ▪ **Emergency:** Messages about events, such as an imminent system crash, that make the system unusable. Typically this type of message is broadcast to all users. ▪ **Alert:** Messages about conditions, such as a corrupted system database, that require immediate corrective action. ▪ **Critical:** Messages about serious conditions, such as a disk failure. ▪ **Error:** Messages about conditions that require corrective action but are not critical. ▪ **Warning:** Warnings about possible issues. ▪ **Notification:** Messages about normal but significant conditions that may require attention. ▪ **Information:** Messages that provide information only. ▪ **Debugging:** Messages that are used to debug programs.
Local	Check the box in the heading row to include all services in the local logs that can be viewed in the Log Viewer. Alternatively, check the box for kernel or system to include that service in the local log.
E-Mail	Check the box in the heading row to include all services in the emailed logs, if configured on the *Log Setting* page. Alternatively, check the box for kernel or system to include that service in the emailed log.

Field	Description
Syslog Server	Check the box in the heading row to include all services in the log file that is transmitted to the syslog server. Alternatively, check the box for kernel or system to include that service in the log file.

Log Setting

If logging is enabled on the *Administration > Log > Log Module* page, the ATA can periodically send the log file to a server or to an email address. Use the *Log Setting* page to enter the information for your syslog server and email account.

NOTE For information about enabling and configuring logging, see **Log Module, page 187**.

To open this page: Click **Administration** in the menu bar, and then click **Log > Log Setting** in the navigation tree.

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

Local

Field	Description
Log Size	Enter the maximum size of the log file in kilobytes. Valid values are from 128 to 1024.

Syslog Server

Field	Description
IP Address	Enter the IP address of the syslog server where the messages will be sent.
Port	Enter the port to use on the server. Valid values are from 1 to 65535.
TLS Enabled	Check the box if enabled.

E-Mail

When logging is enabled, you can send logs to an email address by using SMTP.

NOTE Service providers' requirements vary. Be aware that some providers do not allow SMTP email from a free account. Other providers may require a user to log on to a new mailbox before sending emails. For accurate information, read the support documentation from your provider. In your provider's support or help system, search for information about SMTP server settings.

Field	Description
Sender	If you wish to send log entries to an email account, complete all of the fields in this section. Enter a valid email address to identify the sender of the email. Example: user1@company.com
Receiver	Enter a valid email address where the email will be sent. Example: user2@company.com
SMTP Server	Enter the IP address or domain name of the mail server that you will use to send this email. Example: smtp.gmail.com
SMTP Port	Enter the port to use on the SMTP server. The default value is 25. Use the port specified by your email server administrator or service provider.
Subject	Enter a brief description for the subject line of the email. Example: Log from My ATA
Number of Logs	Enter the number of log entries to include in the email. The valid range is 10 to 200.
Interval	Enter the interval, in minutes, at which to send emails. The valid range is 1 to 1440 (24 hours).
Username	Enter the username for the email account that will be used to send these emails. Use the format required by your service provider. Usually it is the full email address. Example: user1@company.com.
Password	Enter the password for the email account that will be used to send these emails.

Log Viewer

If logging is enabled on the *Administration > Log > Log Module* page, you can use the *Log Viewer* page view the logs online and to download the system log file to your computer. You can limit the contents of the log by choosing the types of entries to include and by specifying keywords.

NOTE For information about enabling and configuring logging, see **Log Module, page 187**.

To open this page: Click **Administration** in the menu bar, and then click **Log > Log Viewer** in the navigation tree.

Field	Description
Download Log	Click this button to download the contents of the log as a file on your computer. In the dialog box, you can open the file or save it. The file can be opened in a text editor such as Notepad.
Clear Log	Click this button to remove all entries from the log.
Display	Choose the type of content to display: All, kernel, or system.
Filter	Enter a keyword to filter the log entries that appear in the viewer. The page will display only the entries that include the keyword.

Diagnostics

The ATA includes two built-in diagnostic tools:

- Ping Test
- Traceroute Test

Ping Test

Use the *Administration > Diagnostics > Ping Test* page to test connectivity between the ATA and a destination.

To open this page: Click **Administration** in the menu bar, and then click **Diagnostics > Ping Test** in the navigation tree.

STEP 1 Enter the IP address or domain name that you want to ping.

STEP 2 Enter a packet size in bytes. The range is 32 to 65500 bytes.

STEP 3 Choose the number of times to send the ping request (5, 10, or Unlimited).

STEP 4 Click **Start to Ping** to start the test. After the test is complete, the test results appear on the page. While the ping test is running, you can click **Stop** to abandon the test.

The test results indicate the number of packets sent and received, the percentage of packet loss, and the round-trip speed.

STEP 5 Click **Close** to close the test results and display the *Ping Test* form.

Traceroute Test

Use the *Administration > Diagnostics > Traceroute* page to view the route between the ATA and a destination.

To open this page: Click **Administration** in the menu bar, and then click **Diagnostics > Traceroute Test** in the navigation tree.

STEP 1 Enter the IP address or domain name of the destination.

STEP 2 Click **Start to Traceroute** to start the test. The results appear on the page and are refreshed every 5 seconds. During the test, you can click **Stop** to abandon the test.

The results display up to 30 hops.

STEP 3 Click **Close** to close the results and display the *Traceroute Test* form.

Factory Defaults

Use the *Administration > Factory Defaults* page to reset the ATA to the default configuration. Alternatively, press and hold the RESET button for 20 seconds. All user-changeable non-default settings will be lost. This may include network and service provider data.

To open this page: Click **Administration** in the menu bar, and then click **Factory Defaults** in the navigation tree.

You can perform the following tasks:

- **Restore Router Factory Defaults:** Choose **Yes** to remove any custom data (router) settings that you have configured. The default settings will be restored when you click **Submit**.
- **Restore Voice Factory Defaults:** Choose **Yes**. to remove any custom settings that you configured on the *Voice* pages of the configuration utility. The default settings will be restored when you click **Submit**.

Fast Factory Reset

RC Unit:

STEP 1 Trigger Factory Reset.

STEP 2 Reset Router after 3 seconds.

STEP 3 Send command 16 to Reset Voice after 3 seconds.

STEP 4 Perform sp default, send /etc/flat_profile.xml to Voice via vsock after 5 seconds.

STEP 5 Reboot after 30 seconds.

Non-RC Unit:

STEP 1 Trigger Factory Reset.

STEP 2 Reset Router after 3 seconds.

STEP 3 Send command 16 to Reset Voice after 3 seconds.

STEP 4 Reboot after 10 seconds.

Firmware Upgrade

Use the *Administration > Firmware Upgrade* page to upgrade the firmware on the ATA. It is not necessary to upgrade unless you are experiencing problems with the ATA or if the new firmware has a feature that you want to use. Before upgrading the firmware, download the firmware upgrade file for the ATA at: www.cisco.com/go/smallbizvoicegateways

To open this page: Click **Administration** in the menu bar, and then click **Firmware Upgrade** in the navigation tree.

STEP 1 Click **Browse** and select the location of the upgrade file that you downloaded.

STEP 2 Click the **Upgrade** button to upgrade the firmware.

CAUTION Upgrading the firmware may take several minutes. Until the process is complete, DO NOT turn off the power, press the hardware reset button, or click the Back button in your current browser.

Configuration Management

Use the *Administration > Config Management* pages to backup and restore the configuration settings for the ATA.

- **Backup Configuration**
- **Restore Configuration**

Backup Configuration

Use the *Administration > Config Management > Backup Configuration* page to back up the ATA configuration settings to a file. You can then later restore these same settings to the ATA.

To open this page: Click **Administration** in the menu bar, and then click **Config Management > Backup Configuration** in the navigation tree.

Click the **Backup** button to save the configuration information of the ATA. When the dialog box appears, choose a location where you want to save the *.cfg* file. **Tip:** Rename the file with a name that includes the date and time when you did the backup.

Restore Configuration

User the *Administration > Config Management > Restore Configuration* page to restore the ATA configuration settings from a previous backup. It is recommended that you back up your current configuration settings before you restore a configuration.

To open this page: Click **Administration** in the menu bar, and then click **Config Management > Restore Configuration** in the navigation tree.

STEP 1 Click **Browse** to locate the *.cfg* file on your computer.

STEP 2 Click **Restore** to restore the settings from the selected file.

Reboot

Use the *Administration > Reboot* page to power cycle the ATA (if necessary) from the configuration utility. Alternatively, accomplish this task by pressing the RESET button.

To open this page: Click **Administration** in the menu bar, and then click **Reboot** in the navigation tree.

Click the **Reboot** button to power cycle the ATA. When the warning message appears, read the information, and then click **OK** to reboot the ATA, or click **Cancel** to abandon the operation. The ATA and any connected devices will lose network connectivity during this operation.

NOTE To avoid reboot upon every resync (when a same parameter appears in multiple profile files), the changed parameters are saved in a temporary table and applied to flash after processing all the profile files.

For example:

—profile A : <_Proxy_1_>1.1.1.1<_Proxy_1_>

—profile B: <_Proxy_1_>2.2.2.2<_Proxy_1_>

After all the profile files are processed, Proxy_1 parameter in the flash is saved with 2.2.2.2 and then reboot once. (Proxy_1 from profile A is overwritten and takes no effect.)

Save the parameter to the table if it is not in the table or is different with current flash value, otherwise remove from the table.