Central Provisioning of Algo IP Endpoints

Guide

AL-*UG-00000008012024*
support@algosolutions.com
January 8, 2024

Algo Communication Products Ltd.
4500 Beedie Street, Burnaby
V5J 5L2, BC, Canada
1-604-454-3790
www.algosolutions.com

Information Notices

Warning

Warning indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury

Caution

Caution indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury and/or damage to the equipment or property

Important

Important indicates a key piece of updates, information, and instructions that need to be followed for correct and safe use of the device

Note

Note indicates useful updates, information, and instructions that should be followed

Tips & Tricks

Tips & Tricks indicate helpful instructions that could help you with your device

Disclaimer

The information contained in this document is believed to be accurate in all respects but is not warranted by Algo. The information is subject to change without notice and should not be construed in any way as a commitment by Algo or any of its affiliates or subsidiaries. Algo and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. Algo assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware.

No part of this document can be reproduced or transmitted in any form or by any means – electronic or mechanical – for any purpose without written permission from Algo.

For additional information or technical assistance in North America, please contact Algo's support team:

Algo Technical Support
1-604-454-3792
support@algosolutions.com

Table of Contents

1 INTRODUCTION

Central provisioning allows system administrators to manage and configure a large number of devices, eliminating the need to log into each endpoint web interface. As a result, central provisioning can save time and ensure consistent configuration setups.

Most Algo IP Endpoints support provisioning. After configuration or firmware files are placed on a central server, Algo IP Endpoints can be instructed to fetch these files and apply the settings.

To provision an Algo IP Endpoint:

1. Provide the Algo endpoint with the address of the provisioning server.
2. Generate and download the desired files and place these on the provisioning server.
3. Reboot the device.

These steps are described in more detail in the sections below.

Zero-touch provisioning (ZTP) can be used along with regular provisioning for most Algo IP Endpoints. The ZTP service is meant to be used as a redirection service to your provisioning server or an Algo Device Management Platform (ADMP) account. More information on ZTP is available here.

Supported Algo Endpoints

The following Algo endpoints support central provisioning:

IP Speakers • 8180 IP Audio Alerter (G1 and G2) • 8186 IP Horn Speaker • 8188 IP Ceiling Speaker • 8189 IP Surface Mount Speaker • 8198 IP PoE+ Ceiling Speaker • 8196 IP PoE+ Horn Speaker • 8190 IP Speaker – Clock • 8190S IP Speaker – Clock & Visual Alerter	**IP Intercoms** • 8028 IP Doorphone (G1 and G2) • 8201 IP PoE Intercom • 8039 IP Video Mullion Intercom • 8036 IP Multimedia Intercom (*SIP configuration and directory file only; excluding UI configuration) • 8063 IP Door Controller • 8061 IP Relay Controller
IP Paging Adapters • 8301 IP Paging Adapter & Scheduler • 8373 IP Zone Paging Adapter	**IP Visual Alerters** • 8128 IP Visual Alerter (G1 and G2) • 8138 IP Color Visual Alerter
IP Displays • 8410 IP Display Speakers • 8420 IP Dual-Sided Display Speaker	

Note

G1 endpoints and the 8061 have limitations. Contact support@algosolutions.com for more information.

2 PROVISIONING SETTINGS

The provisioning settings are in the web interface under **Advanced Settings → Provisioning**.

The following parameters are available:

Provisioning Mode	Enable or disable all provisioning functions.
Server Method	The server address can be obtained from the DHCP server via Option 66/150/160 (default), or a static address can be specified.
Static Server	This field can contain the server address along with the protocol and path. All the following examples are valid: • 192.168.1.1 • provserver.mydomain.com • ftp://192.168.1.1 • 192.168.1.1/files • user: pwd@192.168.1.1
Download Method	Select a protocol supported by server TFTP (default), FTP, HTTP, or HTTPS.
Username/Password:	Login credentials to access the server (not applicable in TFTP mode).
Validate Server Certificate	Validate the server against common certificate authorities. To validate against additional certificates, use the System → File Manager tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the certs/trusted folder (only applicable in HTTPS mode).
Config Download Path	The path on the server to request config files from. Do not add any extra leading or trailing characters or slashes.
Firmware Download Path	The path on the server to request firmware files from. Do not add any extra leading or trailing characters or slashes.
Partial Provisioning	Allow support for incremental provisioning files. This mode does not set omitted settings to their default value. Instead, they are left untouched.
Check-sync Behavior	Reboot behavior upon receiving a check-sync event.
Sync Start Time	Schedule a time (HH:mm:ss) for the device to sync according to the “Check-sync Behavior”.
Sync End Time	If set, the device will sync randomly in the window between Start Time and End Time.
Sync Frequency	Select daily syncs or sync on specific days of the week.
Sync Days	Select specific days of the week to sync.

3 DEFAULT METHOD FOR PROVISIONING (TFTP)

To provision an Algo IP Endpoint:

1. Set up a TFTP server on your network.
2. Create the desired .conf file and place it on the server.
3. Generate a .md5 file for the configuration and put it on the server.

Note

A .md5 checksum file is always required to provision configuration or tone files via TFTP. Generating the MD5 file is explained in Section 5.

4. On your DHCP server, populate Option 66 with the TFTP server's IP address.
5. Connect the Algo IP Endpoint to the network or reboot if already connected.

4 ALTERNATIVE METHODS FOR PROVISIONING

An Algo IP Endpoint can be configured manually with the address for the Provisioning Server or automatically by obtaining the address at bootup via the DHCP Option 66/150/160 field. Using the DHCP options allows the device to be provisioned with no initial configuration, while the manual provisioning option provides an alternative if access to the DHCP server is unavailable.

TFTP, FTP, HTTP & HTTPS are supported download methods.

4.1 Automatic Configuration (DHCP Option 66/160/150)

Dynamic Host Configuration Protocol (DHCP) options are additional parameters provided by a DHCP server to configure various network settings such as IP addresses, subnet masks, and gateway addresses on client devices.

The DHCP Option 66, 160, and 150 field can provide the provisioning server address to an Algo IP Endpoint. A full URL, including the protocol, server address, and path, can be provided.

The highest priority Option returned in the DHCP response is the only one that will be used even if no provisioning files are found on this server. A configuration option is also provided to manually specify which DHCP Option number to use if you wish to override the automatic selection.

The priority order from highest to lowest is:

1. Option 66
2. Option 160
3. Option 150

4.2 Manual Configuration (Static Server Method)

As an alternative to DHCP Options, a static address can be provided for the provisioning server by logging into the web interface of the Algo endpoint and configuring the **Server Method** to **Static** under **Advanced Settings → Provisioning**. Other settings available under **Provisioning** include selecting a protocol type (TFTP, FTP, HTTP & HTTPS) and the option to provide a path on the server to download the configuration and firmware files.

5 PROVISIONING CONFIGURATION FILES

Configuration files contain all settings used by Algo IP Endpoints. Complete configuration files must be provided to the device. Any settings omitted from the configuration file will be set to their factory default value.

Support can also be enabled for partial provisioning using incremental files (described below). This mode leaves omitted settings as-is and does not set them to default values.

5.1 Generic Configuration Files

All devices of the matching product model will download the generic configuration file if a device-specific file is not provided. Generic configuration files can be used to apply settings common to all devices but cannot be used to apply unique SIP credentials to individual devices.

Note

If a generic file is used to first set common settings and SIP credentials are later applied manually via the web interface of each device, the generic provisioning file must be removed, or the provisioning option must be disabled on the device so the provisioning file is not accidentally applied again later, thus deleting the modified settings.

5.2 Device-Specific Configuration Files

Device-specific configuration files contain the MAC address in the filename and are only retrieved by a single target device. These files can be used to completely configure a device. If the provisioning server is left active after the initial configuration, it can also be used to ensure that the device configuration is restored to these intended settings at each reboot.

If a device-specific file is not found on the provisioning server, the endpoint will attempt to download the generic file instead.

5.3 Disabling Provisioning After Completion

The simplest way to generate a configuration file is by downloading a settings backup from a device using the web interface (**System → Maintenance tab → Download Configuration File**).

This file is in the same format used for provisioning and will contain all the currently applied device settings. This file can be modified by hand, in a text editor, or using custom programming scripts to populate values from a database.

Advanced Tip:

The easiest way to identify the name of a parameter is to inspect the web interface. This will allow you to view which parameter a setting is associated with. To do this:

1. Right-click on the desired setting in the web interface and click **Inspect** or **Inspect Element**.
2. View the code window that appears. The code representing the interface setting you selected will be highlighted. You may need to click on the triangle on the left side of the line to expand the block if it is not already visible. Look for the tag **name** to find the parameter name. For example, you'll see **name="sip.poxy"** for the **SIP Domain** field.

5.4 Configuration Filenames and File Format

The following filenames are examples for the 8188 IP Ceiling Speaker. For other products, replace the "8188" portion of the filename with the appropriate 4-digit number for your product. Some of the firmware components apply to specific products only.

Configuration files:

Generic configuration file	algopPRODUCT_ID.conf *Example*: *algop8188.conf*
Device-specific configuration file	algomMACADDRESS.conf *Example*: *algom0022EE010203.conf* ***Note*** MAC address must be in all uppercase

Other optional files related to provisioning:

Tone files	filename.zip *Example: algop8188-tones.zip*
Firmware image	*Example: algo-8188-5.4f.sfw*
Incremental provisioning file	algomMACADDRESS-i.conf or algopPRODUCT_ID-i.conf *Example: algop8188-i.conf*
md5 (for TFTP server only)	algomMACADDRESS8188.md5 or algopPRODUCT_ID.md5 *Example: algop8188.md5*
mTLS Certificate(s) file	filename.zip *Example: my_cert.zip*

It is important to note that:

- Incremental provisioning is disabled by default
- The names of the configuration files are all case-sensitive.
- A .md5 file is always required, regardless of the download method, when using provisioning to upload a tone or directory file (see Section 10 for more details).

These filenames will be combined with the other provisioning parameters to form the full request that is sent to the provisioning server. For example:

- *Download {tftp,ftp,http,https}://server/[Config_Download_Path]/algop8188.conf*

5.5 MD5 Checksum for Configuration Files (TFTP Server Only)

An .md5 checksum file must also be generated and uploaded to the provisioning server. This checksum file is used to verify that the .conf file is transferred correctly without error.

There are various ways to generate an md5 file. You may choose your preferred method.

Generate an md5 file on Linux / macOS:

1. Use the following command in the terminal: md5sum <filename>
   - Example: md5sum *algop8180.conf*
2. Copy the generated md5 code to the clipboard and save it as an md5 file (Example: algop8180.md5).

Generate an md5 file on Windows:

1. Download and open Notepad++. Click **Tools → MD5 → Generate from files**.
2. Click **Choose files to generate MD5** and upload the config. file.
3. Copy the generated md5 code to the clipboard and save it as an md5 file (Example: *algop8180.md5).*

If the md5 checksum file is not present on the TFTP server or does not correctly match the .conf file, this provisioning file will be ignored.

6 REBOOT

Once the provisioning server is ready, each Algo IP Endpoint must be rebooted to trigger a fetch of the configuration file(s). This can be done in several ways:

- Plug in a new unit into the network.
- Remove and restore PoE power via the Ethernet switch/router.
- Send a “check-sync” NOTIFY command via the network (note: check-sync is only supported when Provisioning Mode is enabled).

7 DETAILED PROVISIONING BEHAVIOR

This section provides a detailed list of the steps the device takes as part of the provisioning process. Note that any time a changed provisioning file is successfully accepted, the device will apply these changes, reboot, and start from the top of the list again.

On the next pass through these steps, the device should detect a match at the most recently completed stage and continue from that point. Once all configuration and firmware on the device match with that on the provisioning server, the device will proceed through all the steps without further action and will begin normal operation.

At powerup or reboot, the device will go through the following steps:

1. Verify provisioning is enabled (on by default). Exit if disabled.
2. Obtain provisioning server address from DHCP Option 66/150/160 (default) or static address if set.
3. Download config files.

   TFTP:

   a. Attempt download of Mac-specific config file.
   b. Attempt download of md5 file for Mac-specific config (if config file was found)
   c. Attempt download of incremental Mac-specific config file (if the previous file was not found; and if supported by device/firmware)
   d. Attempt download of md5 file for incremental Mac-specific config (if config file was found)
   e. Attempt download of the generic config file (if the previous file was not found)
   f. Attempt download of md5 file for generic config (if config file was found)
   g. Attempt download of the incremental generic config file (if the previous file was not found; and if supported by device/firmware)
   h. Attempt download of md5 file for incremental generic config (if config file was found)
      - If the downloaded config & md5 files do not match, this config file is ignored.
      - If the config file matches the config file already on the device, this config file is ignored (file is diff'ed with existing file).
      - If the downloaded config & md5 files do match, and the config is new, the config file is applied, and the device will immediately reboot (and thus start the process again).

   FTP, HTTP & HTTPS:

   a. Attempt download of Mac-specific config file.
   b. Attempt download of incremental Mac-specific config file (if the previous file was not found
   c. Attempt download of the generic config file (if the previous file was not found)
   d. Attempt download of the incremental generic config file (if the previous file was not found)
   - If the downloaded config file differs from that currently on the device, the config file is applied and the device will immediately reboot and start the process again.
4. Check the config file for the firmware version.
   a. If the firmware version parameter is present in the config file and this version does not match the currently installed firmware version, then attempt to download the appropriate. fw & .md5 or .sfw files.
   b. If firmware & md5 files match, install firmware and reboot to restart the provisioning from the beginning.

5. Tones
    a. Attempt to download the md5 file for the tones file (if the tones parameter is present in the config file).
    b. Attempt to download tones file .zip (if md5 was found and different than last stored md5).
        - If the downloaded .zip & md5 files match, the tones are unzipped and saved on the device. They can be found on the web interface under **System → File Manager**. Any existing tone files with matching names are overwritten.
6. Scheduler Data (Only applies to the 8301 IP Paging Adapter)
    a. Attempt to download the md5 file for the scheduler data file (if the scheduler parameter is present in the config file).
    b. Attempt to download the scheduler file .db (if md5 was found and different than the last stored md5).
7. Image/Icon/Slide (Only applies to the 8410 and 8420 IP Displays)
    a. Attempt to download md5 file(s) if one of the parameters is in the config file.
    b. Attempt to download the corresponding file .zip or .db file if md5 was found and different than the last stored md5.
8. Certificates
    a. Attempt to download the md5 file for the certificates file if the certificates parameter is in the config file.
    b. Attempt to download certificates file .zip if md5 was found, and different than last stored md5.

8 PARTIAL PROVISIONING USING INCREMENTAL FILES

Unlike the regular provisioning method described previously where omitted parameters are set to factory default values, any parameters omitted from an incremental provisioning file will retain their original settings as currently stored on the device. This allows settings such as SIP credentials or a new speaker volume level to be assigned to a device without affecting other device settings.

Enable Partial Provisioning: Enable partial provisioning in web interface by navigating to **Advanced Settings → Provisioning → Partial Provisioning**. This setting is disabled by default.

Incremental provisioning files can be generic or device-specific, as described above, and are created by adding a "-i" suffix to either of these types of filenames before the file extension.

For example: *algop8188-i.conf*, or *algom0022EE010203-i.conf* and the same for the .md5 if using TFTP.

Note

Any given endpoint will only download a single provisioning file from the server. Multiple file types (e.g., generic and incremental) cannot be combined on the same server. If multiple files are found on the server, the search order is as follows: algom, algom-i, algop, algop-i. Only the first file that is found will be used. See Section 7 on Detailed Provisioning Behavior for more details.

9 FIRMWARE UPGRADE VIA PROVISIONING

Configuration files can also contain an optional parameter that specifies the desired firmware version. If this version number does not match the current firmware installed on the device, the new firmware will be downloaded from the provisioning server and installed.

For example, the firmware parameter could be:

prov.version.firmware = 5.4f

The full filename will be generated automatically based on the parameter name, version number, and product that it is applied to. For example, "prov.version.firmware = 5.4f" when applied on the 8180, will request the following file: *algo-8180-5.4f.sfw*.

Note

If you are upgrading from 1.7.6 to 3.2.5, you will need the following:

- Both the firmware file and the matching md5 checksum must be present on the provisioning server for the upgrade to be successful. The.md5 file is provided by Algo.
- Update the config file with the parameter "prov.download.bundle =1" and "prov.version.firmware = 3.2.5".
- Contact Algo support for more details.

Firmware files should always be used as-is. You will never need to change the file names or content of the. fw & .md5 files (in case of 3.2.5) provided by Algo when using provisioning. Only the version number portion needs to be specified in the provisioning parameter. The rest of the filename will be matched automatically.

Note

The device will reboot twice when upgrading the firmware via provisioning. After the device installs the new configuration file it will reboot to apply the changes. Next, the device will parse the new parameter requesting the firmware version to download and install the firmware. The device will reboot again at the end of the firmware upgrade process.

It is important to ensure that the provisioning setting is still enabled in the config file that specifies the target firmware version otherwise the firmware changes will not be applied.

10 TONE FILES INSTALLATION VIA PROVISIONING

Audio tone files can be installed on a device using provisioning by placing one or more .wav or .mp3 files within a .zip file using the following method.

To enable tone file provisioning on Algo products:

1. Add the parameter "prov.data.tone" to the configuration file and provide the full file name of the desired tones package including the .zip extension (note that the filename is case-sensitive). For example: **prov.data.tone = tone_file.zip**
2. Create a valid checksum (.md5) for the tone zip file using the same process described for the configuration files. The filename should be the same but with the file extension .md5. For example: **tone_file.md5**

Like with the firmware upgrade process, the device will first download and apply the new configuration file, followed by a reboot, before attempting to download the specified tone files. The provisioning feature must still be enabled in the newly applied config file.

The tone .zip file must be placed in the same folder on the provisioning server as the firmware files. The "Firmware Download Path" parameter will also be used for the tones. Only the filename can be specified in “prov.data.tone”. This parameter must not contain a path.

10.1 New vs. Same Tones File

To identify whether the tones file is new, each time the device boots and provisions the .md5 file is saved internally for future comparison. If no changes are made to the tones, the device will not download and install the same .zip file next time.

Three cases will trigger the device to identify if the tones .zip file is new, download it, and install it the next time provisioning occurs:

1. Different .md5 and .zip file is found on the provisioning server.
2. Renaming or deleting any tone files from the web interface.
3. Remove the “prov.data.tone” parameter from the config file and add it again. In this case, if the device provisioning is successful with no tones file specified, the next time it sees the tones file specified again, it will be treated as a new file and installed.

11 UPLOAD CERTIFICATE VIA PROVISIONING

Certificate files can be installed on a device using provisioning by placing one or more files within a .zip file by using the following method:

1. Add the parameter “prov.data.cacert” to the configuration file.
2. Provide the full file name of the desired zipped cert folder, including the .zip extension. For example: prov.data.cacert = my_cert.zip. The filename is case-sensitive.

If provisioning via TFTP server, you must provide an md5 file as well.

The cert.zip file must be placed in the same folder on the provisioning server as the firmware files (i.e. the "Firmware Download Path" parameter will be used for the certificates). Only the filename can be specified in “prov.data.cacert”. This parameter must not contain a path.

As with the firmware upgrade process, the device will first download and apply the new configuration file, followed by a reboot, before attempting to download the specified certificate. The provisioning feature must still be enabled in the newly applied config file.

12 8301 IP PAGING ADAPTER SCHEDULER FILE PROVISIONING

Like with tone files, the 8301 IP Paging Adapter scheduler data file may be uploaded via provisioning.

To enable the scheduler file provisioning, add the parameter “prov.data.sched” below to the configuration file and provide the full file name, including the .db extension. Note that the filename is case-sensitive. For example: prov.data.sched = scheduler_data.db

Also create a valid checksum (.md5) for the db file using the same process described for the configuration files. The filename should be the same, just with a suffix of .md5.

Note that the scheduler_data.db file must be generated and downloaded from a device. To do so, use an 8301 as the template.

1. Add a schedule to the calendar in **Scheduler → Calendar/Schedules.**
2. Navigate to **Scheduler → Data**.
3. Use the option **Download Scheduler Data File** to download the .db file.
4. Place this file in the same folder on the provisioning server as the firmware files and rename it if desired.

Note

The "Firmware Download Path" parameter will also be used for the scheduler. Only the filename can be specified. This parameter must not contain a path.

13 IMAGE PROVISIONING FOR IP DISPLAYS (8410 AND 8420)

Images, icons, and full slides can be uploaded via provisioning by placing one or more .png or .jpg files within a .zip file, like with tone files. This is intended only for the 8410 IP Display Speaker and 8420 IP Dual-Sided Display Speaker.

To enable image file provisioning, add one of the parameters below to the configuration file and provide the full file name of the desired image package(s) including the .zip extension (note that the filename is case-sensitive). For example:

- prov.data.display = filename.db
- prov.data.icon = icons.zip
- prov.data.image = images.zip

You must also create a valid checksum (.md5) for the zip files using the same process described for the configuration files. The filename should be the same but have the file extension .md5.

The display.db file must be generated and downloaded from a device. To do so, use an 8410 or 8420 as the template.

1. Upload all desired images and icons. Configure the displays as desired via the web interface.
2. Navigate to **Display → Data**.
3. Use the option **Download Slide Data File** to download the .db file.
4. Place this file in the provisioning server and rename it if desired.

The .zip files must be placed in the same folder on the provisioning server as the firmware files (i.e., the "Firmware Download Path" parameter will also be used for these files). Only the filename can be specified. This parameter must not contain a path.

14 8036 DIRECTORY FILE

The directory txt data file for the 8036 IP Multimedia Intercom can be uploaded via provisioning, similar to tone files.

To enable the directory file provisioning, add the parameter “prov.prod.dir” to the configuration file and provide the full file name of the desired txt file. Note that the filename is case-sensitive. For example: prov.prod.dir = directory.txt

Also create a valid checksum (.md5) for the txt file using the same process described for the configuration files. The filename should be the same but have the file extension .md5.

The .txt file must be placed in the same folder on the provisioning server as the firmware files (i.e., the "Firmware Download Path" parameter will also be used for the directory file). Only the filename can be specified. This parameter must not contain a path.

15 ADVANCED PROVISIONING

15.1 Two-Stage Provisioning (provisioning from two different servers)

Example: You have an existing provisioning server that supports only FTP (with a required password) that you wish to use to provision many Algo 8186 IP Horn Speakers. This server has a static IP address.

Solution: Set up a temporary TFTP server and use DHCP Option 66/150/160 to point the 8186 Horns to this server. Note that this step could be done at a different location, for example, at a vendor’s office before installation with the end customer. To do this:

1. Log in to the web interface on one 8186 and set the options required to access the FTP provisioning server (i.e., provisioning server static IP address, the FTP mode, and login credentials).
2. Under **System → Maintenance**, click the **Backup** button to download the configuration file from this device.
3. Save this file to the TFTP server. This file contains all the settings necessary to configure the remainder of the 8186s to use the regular FTP server.
4. Create the necessary .md5 file.
5. Plugin or reboot all 8186 devices to configure them with these changes and have them begin communicating with the desired provisioning server.

Explanation: When a new 8186 is booted in this scenario, it will receive the address of the temporary TFTP via the DHCP Option 66/150/160 field. It will then contact this TFTP server and download the configuration file you created that contains the settings necessary to contact the existing FTP provisioning system. The 8186 will apply these new settings, reboot, and now contact the FTP server this time and log in successfully. It will then pull the configuration files stored on that server, which are typically specific to each endpoint and contain the SIP account details and other desired settings. Once this first TFTP step is completed on all units, the TFTP server can be removed, and the DHCP Option 66/150/160 field can be cleared.

15.2 Disabling Provisioning After Completion

It is important to consider whether you wish provisioning to remain enabled after completion. Devices are often provisioned once before installation and then installed at a site. If a static provisioning server is configured, the device will still attempt to contact this server, which may lead to a delay in booting since the server does not exist at this location.

If settings such as SIP accounts or volume control will be adjusted individually on each device after initial provisioning, it is important that provisioning is disabled so these settings are not overwritten at the next bootup.

16 TROUBLESHOOTING

Troubleshooting provisioning issues can be challenging since the device will not provide any output during this process. Be sure to observe the logs from your provisioning server and the device logs on the web interface under **System → System Log** to see any file requests the device might be making.

See the list below for other troubleshooting methods:

- Verify that provisioning has not been disabled in the web interface.
- Verify that your provisioning server supports the protocol selected on the device (TFTP, FTP, HTTP, or HTTPS).
- Compare the file request logs seen on your server with the steps outlined in the above sections to determine which step the device is getting to.
- Verify that the md5 checksum (if applicable) file is correct. This is typically the most common source of failure.
- Verify that provisioning is not enabled when not expected. This can cause settings to get overwritten since any changes in the web interface will be lost the next time the device is rebooted, and it will download the original provisioning file again.