Aruba Instant 8.11.0.x

REST API Guide

a Hewlett Packard
Enterprise company

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

The Aruba Instant REST API Guide describes the configuration procedures and monitoring functions that can be performed using REST APIs. To assist you better, the range of values for each configuration parameter is included, along with relevant sample configurations. For more information, refer to Supported APIs and Components on page 14.

Related Documents

The following guides are part of the documentation for Aruba Instant:

- *Aruba Instant Release Notes*
- *Aruba Instant User Guide*
- *Aruba Instant CLI Reference Guide*

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://asp.arubanetworks.com/

Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

Chapter 2
Overview of REST APIs

Currently Instant APs can be configured using the CLI, WebUI, and Central. Starting from Aruba Instant 8.5.0.0, users can now configure and monitor Instant APs through REST APIs. The REST API will serve as a programmable interface that dynamically configures the Instant APand also provides visibility to supported monitoring functions. In this release, the REST APIs are supported on both cluster and standalone modes of the Instant AP.

Before getting started, note the prerequisites listed below and develop a basic understanding of the interface used and the **curl** commands used to login and logout of an Instant AP.

Prerequisites

- Complete understanding of the configuration hierarchy.
- Knowledge of the CLIs is required for the first time as all objects are based on the equivalent CLIs.
- The user can run **curl** commands from any machine supporting **curl** configuration.

Ensure to prefix escape character (\ ) when including - \n, \r, double quotes, or any other special characters – as part of JSON input parameter values.

Enabling or Disabling REST API on the Instant AP

The REST API function is disabled by default. To access the API, you must first enable it using the Instant CLI. REST API configuration is supported on both cluster and standalone modes. In the cluster mode, only the master Instant AP will provide the REST API access.

The below CLI command enables the REST API on a master or a standalone Instant AP:

```
(Instant AP)(config)# allow-rest-api
(Instant AP)(config)# end
(Instant AP)# commit apply
```

The below CLI command disables the REST API on a master or a standalone Instant AP:

```
(Instant AP)(config)# no allow-rest-api
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Interface

The interface used to access the configuration elements on Instant AP is **HTTPS**. HTTPS is used because it provides transport layer security, and hence the passwords and other secret information can be sent over in plain text without worrying about anyone interfering.

Login

To access any configuration element—whether it is **action**, **configuration**, or **monitoring**, the user first has to login to the Instant AP.

The following is a sample **CURL** command used to log in to the master Instant AP:

```
curl "https://<Master-iap-ip>:4343/rest/login" -H "Content-Type: application/json"  --
data '{"user": "<username>", "passwd": "<password>}' --insecure
```

The following is a sample **CURL** command used to log in to the standalone Instant AP:

```
curl "https://<Standalone-iap-ip>:4343/rest/login" -H "Content-Type: application/json"  -
-data '{"user": "<username>", "passwd": "<password>}' --insecure
```

NOTE

The **--insecure** option can be used with the curl command if the certificate of the Instant AP cannot be validated.

The following table shows the parameters used in the login command:

Table 3: *Login Command Parameters*

Parameters	Description
<username>	Username of the user.
<password>	Password of the user.
<Master-iap-ip>	IPv4 address of the master Instant AP.
<Standalone-iap-ip>	IPv4 address of the standalone Instant AP.

The following is an example response for a successful login:

```
curl "https://172.68.104.253:4343/rest/login" -H "Content-Type: application/json"  --data
'{"user": "admin", "passwd": "admin"}' --insecure
{
"Status": "Success",
"sid":  "m7zI7bicqELh4g5bBSNJ"
}
```

NOTE

The sid has to be used in all configuration, action, and monitoring REST-API calls after the login.

Once logged in, the user can run configuration, action, monitoring REST-API calls. The session has an inactivity timeout of 15 minutes. Which means, if there is no transaction for 15 minutes, the session will expire.

The following is an example response for a failed login:

```
{
"Status": "Failed",
"Error message": "Login failed"
}
```

Logout

To close all the interactions, you need to logout from the master or standalone Instant AP.

The following is a sample **CURL** command used to log out of the master Instant AP:

```
curl "https://<Master-iap-ip>:4343/rest/logout" -H "Content-Type: application/json" --
data '{"sid":"<sid>"}' --insecure -k
```

The following is a sample **CURL** command used to log out of the standalone Instant AP:

```
curl "https://<Standalone-iap-ip>:4343/rest/logout" -H "Content-Type: application/json" -
-data '{"sid":"<sid>"}' --insecure -k
```

NOTE

The **--insecure** option can be used with the curl command if the certificate of the Instant AP cannot be validated.

The following table shows the parameters used in the logout command:

Table 4: *Logout Command Parameters*

Parameters	Description
<Master-iap-ip>	IPv4 address of the master Instant AP.
<Standalone-iap-ip>	IPv4 address of the standalone Instant AP.
<sid>	A unique string that the server generates and returns to the user when a login authentication is successful. User has to include this SID in all API calls of this session. It is valid until the user explicitly logs out, or, until the inactivity timeout expires.

The following is an example response for a successful logout:

```
{
"Status": 0,
"message":"User logout successfully"
}
```

Once logged out, no configuration, action, or monitoring REST API calls can be run on the master or standalone Instant AP.

The following table lists the response messages for REST-API GET or POST calls:

Table 5: *REST API Response Messages*

REST API Call / Scenario	Response Message
If a REST API call is sent to an Instant AP with the REST API function is disabled	REST API Service is not enabled
If a REST API call is sent to a slave Instant AP in a cluster.	REST API service is available only on the master Instant AP.

Successful login to the REST API	<pre>{
	"Status": "Success",
	"sid": "rTUlBBbolbriCTHQ8cM3"
	}</pre> **NOTE:** sid is one of the input parameters in the URL for the REST-API GET/POST calls, that facilitates the Instant AP to authenticate the request.

Failed login (when the login credentials are invalid)	<pre>{
	"Status": "Failed",
	"Error message": "Login failed"
	}</pre>

Successful logout from the REST API	<pre>{
	"Status-code": 0,
	"message": "User logout successfully"
	}</pre>

Invalid SID (Session ID)	<pre>{
	"Status-code": 1,
	"message": "Invalid session id or session id has expired"
	}</pre>

If the SID has expired	<pre>{
	"Status-code": 1,
	"message": "Invalid session id or session id has expired"
	}</pre>

If the API in the URL is invalid	For Example :
	■ Valid Monitoring API in URL is /rest/show-cmd
	■ Invalid Monitoring API in URL is /rest/show-cm
	<pre>{
	"Status": "Failed",
	"Status-code": 2,
	"IAP IP address": "172.68.104.253",
	"Error message": "Invalid API /rest/sow-cmd"
	}</pre>

REST API Call / Scenario	Response Message

If the json format is incorrect in the json payload	<pre>{
	"Status-code": 3,
	"message": "Failed to parse JSON input for /rest/ssid"
	}</pre>

If a mandatory input parameter is missing	For Example :
	Response message for REST-API login call when mandatory parameters are missing.
	<pre>{
	"Status": "Failed",
	"Error message": "Input parameter user and/or passwd is Missing or its value is invalid"
	}</pre>

If an invalid value is entered for a mandatory input parameter	For Example :
	"action" json field is mandatory in SSID json payload and it accepts the values "create" and "delete"
	Below is the response when invalid value passed to "action" json field in SSID json payload.
	<pre>{
	"Status-code": 4,
	"message": "Input parameter ssid->action is Missing or its value is invalid"
	}</pre>

In the Action or Monitoring API, the given iap_ip_address is not part of the swarm.	<pre>{
	"Status": "Failed",
	"Status-code": 7,
	"CLI Command executed": "show upgrade
	",
	"IAP IP address": "172.68.104.25",
	"Error message": "Internal communication error; please check input parameters and try again"
	}</pre>

If the Instant AP fails to process the request during configuration API calls.	<pre>{
	"Status-code": 7,
	"message": "Internal communication error; please check input parameters and try again"
	}</pre>

If the Instant CLI fails to parse the show command.	<pre>{
	"Status": "Failed",
	"Status-code": 6,
	"CLI Command executed": "show abcdef\n",
	"IAP IP address": "172.68.104.253",
	"Error message": "cli output: \n\nCOMMAND=show abcdef\n% Parse error.\n"
	}</pre>

When trying to delete a profile which doesn't exist	<pre>{
	"Status-code": 6,
	"message": "CLI0 error: auth-serve12344444r: Profile not found\n"
	}</pre>

Status Codes

The Response Messages in the above table includes a status code (0-8) for each successful or failed response. These status code are explained in the table below:

Table 6: *Status Codes*

Status Code	Meaning
0	Success
1	Invalid or expired sid
2	Invalid API
3	Invalid JSON format
4	Invalid or missing parameters
5	Missing parameters
6	Config module error
7	Internal Communication Error
8	Unknown error

This chapter describes the following REST API types supported by Aruba Instant:

Action API

Action APIs are meant for individual Instant APs, namely, the master, slave, or a standalone Instant AP. The following configurations can be performed using the Action API:

Ensure to prefix escape character (\ ) when including - \n, \r, double quotes, or any other special characters – as part of JSON input parameter values.

Syntax

The following is a sample CURL command used to call Action APIs on a master or slave Instant AP:

```
curl "https://<Master-iap_ip>:4343<API>?sid=<SID>"  -H "Content-Type: application/json" --data @<json_payload_file> --insecure
```

The following is a sample CURL command used to call Action APIs on standalone Instant APs:

```
curl "https://<Standalone-iap_ip>:4343<API>?sid=<SID>"  -H "Content-Type: application/json" --data @<json_payload_file> --insecure
```

Sample Configurations

The following is an example for CURL call to configure the hostname on a slave Instant AP in cluster mode:

```
Master Instant AP IP Address : 172.68.104.253
SID : vrNKiAbgCMIfl8Yrerkq
API  : /rest/hostname
Slave Instant AP IP Address : 172.68.104.252

curl "https://172.68.104.253:4343/rest/hostname?sid=vrNKiAbgCMIfl8Yrerkq" -H "Content-Type: application/json" --data @hostname_add_json_file --       insecure
```

Following is the sample hostname_add_json_file for above .

```
{
        "iap_ip_addr" : "172.68.104.252"
        "hostname_info" : {
                          "hostname" : "slave"
```

```
                        }
}
```

The following is the successful response to the above call:

```
{
        "Status":       0,
        "message":      "Success"
}
```

The following is an example for CURL call to configure or modify the zone name on a standalone Instant AP:

Standalone Instant AP IP address : 172.68.102.252

```
curl "https://172.68.102.252:4343/rest/zone?sid=vrNKiAbgCMIfl8Yrerkq" -H "Content-Type:
application/json" --data @zone_add_json_file --insecure
```

Following is the sample zone_add_json_file for the above curl call:

```
{
        "iap_ip_addr" : "172.68.102.252",
        "zone_info" : {
                        "action" : "create"
                        "zonename" : "arubanetworks_com_office1"
                      }
}
```

The following is an example for a CURL call to delete the zone name on a standalone Instant AP:

```
curl "https://172.68.102.252:4343/rest/zone?sid=vrNKiAbgCMIfl8Yrerkq" -H "Content-Type:
application/json" --data @zone_add_json_file --insecure
```

Following is the sample zone_add_json_file for the above CURL call:

```
{
        "iap_ip_addr" : "172.68.102.252",
        "zone_info" : {
                        "action" : "delete"
                      }
}
```

The following table lists the JSON_Payload for the features that can be configured on an Instant AP using the Action API:

Table 7: *Action API Configuration*

Configuration	API	JSON_Payload

Hostname	/rest/hostname	{
		"iap_ip_addr" : "string",
		"hostname_info" :
		{
		"hostname" : "string"
		}
		}
		iap_ip_addr—Denotes the Instant AP IP address of the master, slave, or standalone Instant AP on which the hostname is to be configured.
		hostname—Specify a name for the Virtual Controller.

Swarm Mode	/rest/swarm-mode	{
		"iap_ip_addr" : "string",
		"swarm-mode" :
		{
		"swarm-mode": "string"
		}
		}

Table 7: *Action API Configuration*

Configuration	API	JSON_Payload
		■ **iap_ip_addr**—Denotes the Instant AP IP address of the master, slave, or standalone Instant AP on which the swarm mode is to be configured. ■ **swarm-mode**—Configures the swam mode. The valid string values for this field are **standalone** or **cluster**.

Static channel and Power	/rest/channel	<pre>{
		"iap_ip_addr" : "string",
		"channel" :
		{
		"a-channel" :
		{
		"channel_name" : "string",
		"tx_power" : "string"
		},
		"g-channel" :
		{
		"channel_name" : "string",
		"tx_power" : "string"
		}
		}
		}</pre> ■ **iap_ip_addr**—Denotes the Instant AP IP address of the master, slave, or standalone Instant AP on which the static channel and power setting is to be configured.
		■ **a-channel**—Configures the specified 5 GHz channel.
		● **channel_name**—Enter a value for the 5 GHz value. The valid channels for a band are determined by the Instant APregulatory domain.
		● **tx_power**—Enter a transmission power value between -51 dBm to 51 dBm.
		■ **g-channel**—Configures the specified 2.4 GHz channel.
		● **channel_name**—Enter a value for the 2.4 GHz value. The valid channels for a band are determined by the Instant APregulatory domain.
		● **tx_power**—Enter a transmission power value between -51 dBm to 51 dBm.
		Below is a sample json payload file to configure radio channels for the 5 GHz band:
		<pre>{
		"iap_ip_addr" : "172.68.104.253",
		"channel" :
		{
		"a-channel" :
		{
		"channel_name" : "44",
		"tx_power" : "18"
		}
		}
		}</pre>

Zone	/rest/zone	{

Table 7: *Action API Configuration*

Configuration	API	JSON_Payload

		<pre>"iap_ip_addr" : "string",
		"zone_info" :
		{
		"action" : "string",
		"zonename" : "string"
		}
		}</pre> ■ **iap_ip_addr**—Denotes the Instant AP IP address of the master, slave, or standalone Instant AP on which the zone is to be configured.
		■ **action**—Use either of the following values:
		● **create**—To add zone configuration.
		● **delete**— to remove zone configuration.
		■ **zonename**—Configures zone on an Instant AP. You can configure up to six SSID zones per AP, and up to 32 SSID zones per ssid-profile. Use comma separators when listing multiple zones.

Antenna gain	/rest/antenna-gain	<pre>{
		"iap_ip_addr" : "string",
		"antenna_gain_info" :
		{
		"a-external-antenna" : "string",
		"g-external-antenna" : "string"
		}
		}</pre> **iap_ip_addr**—Denotes the Instant AP IP address of the master, slave, or standalone Instant AP on which antenna gain is to be configured.
		a-external-antenna—Configures the antenna gain. You can configure a gain value in dBi for the following types of antenna:
		■ 6- Dipole or Omni
		■ 14- Panel
		■ 14 - Sector
		g-external-antenna—Configures the antenna gain. You can configure a gain value in dBi for the following types of antenna:
		■ 6 - Dipole or Omni
		■ 12 - Panel
		■ 12 - Sector

Enabling and disabling radios	rest/radio-state	<pre>{
		"iap_ip_addr" : "string",
		"radio_state" :
		{
		"dot11a-radio-disable" : "string",
		"dot11g-radio-disable" : "string"
		}
		}</pre> ■ **iap_ip_addr**—Denotes the Instant AP IP address of the master, slave, or standalone Instant AP on which radio setting is to be configured.
		■ **dot11a-radio-disable**—Enter any of the following values:
		● **yes**—disables the dot11a radio

Table 7: *Action API Configuration*

Configuration	API	JSON_Payload

		● **no**—enables the dot11a radio
		■ **dot11g-radio-disable**—Enter any of the following values:
		● **yes**—disables the dot11g radio
		● **no**—enables the dot11g radio
		Below is a sample json_payload_file for disabling dot11a radio on an Instant AP:
		`{`
		`"iap_ip_addr" : "172.68.104.253",`
		`"radio_state" :`
		`{`
		`"dot11a-radio-disable" : "yes"`
		`}`
		`}`

Configuration API

Configuration APIs are used to either add new data, or to modify or delete old data . This is done by sending HTTP POST requests using the **curl** command. Instant currently does not support HTTP DELETE and HTTP PUT operations. All configurations are made entirely on the master Instant AP (in case of clusters) or on a standalone Instant AP. The following configurations are currently supported on Instant using REST API:

Syntax

The following is a sample CURL command used to call configuration APIs on a master Instant AP:

```
curl "https://<Master-iap_ip>:4343<API>?sid=<sid>"  -H "Content-Type: application/json" --data @<json_payload_file> --insecure
```

The following is a sample CURL command used to call configuration APIs on a standalone Instant AP:

```
curl "https://<Standalone-iap_ip>:4343/<API>?sid=<sid>"  -H "Content-Type: application/json" --data @<json_payload_file> --insecure
```

NOTE

The **--insecure** option can be used with the curl command if the certificate of the Instant AP cannot be validated.

NOTE

Ensure to prefix escape character (\ ) when including - \n, \r, double quotes, or any other special characters – as part of JSON input parameter values.

Table 8: *Configuration Command Parameters*

Parameters	Description
<Master-iap-ip>	IPv4 address of the master Instant AP where the configuration element should be got from.
<Standalone-iap-ip>	IPv4 address of the standalone Instant AP where the configuration element should be got from.
<API>	The REST API URL associated with the configuration.
<json-payload-file>	File containing the JSON payload that is used in the configuration HTTP POST request.

Adding or Modifying API Configuration

The following section lists the JSON_Payload and the curl call for the features that can be configured on an Instant AP using the Configuration API:

VC Country Code

Table 9: *VC Country Code Configuration*

API	JSON_Payload	Parameters
/rest/country-code	{ "country_code_info" : { "action" : "string", "country-code" : "string" } }	**action**—Enter one of the following values: ■ create—to add the country code ■ delete—to remove the country code **country-code**—Enter the country code.

Syntax

The following is an example for a curl call to configure or modify the VC country code on a master or standalone Instant AP :

```
curl "https://172.68.104.253:4343/rest/country-code?sid=UUDJwDsNjrNRgmTvCeiy" -H "Content-Type: application/json"  --data @vcc_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (vcc_add_json_file) to add the VC country code:

```
{
"country_code_info" :
{
"action" : "create",
"country-code" : "VI"
}
}
```

Below is a sample configuration (vcc_del_json_file) to delete the VC country code:

```
{
"country_code_info" :
{
"action" : "delete ",
"country-code" : "VI"
}
}
```

VC IP address

Table 10: *VC IP address Configuration*

API	JSON_Payload	Parameters
/rest/virtual-controller-ip	`{ "virtual-controller-ip" : { "vc-ip" : "string" } }`	**vc-ip**—Enter the VC IP address.

Syntax

The following is an example for curl call to configure or modify the VC IP address on a master Instant AP :

```
curl "https://172.68.104.253:4343/rest/virtual-controller-ip?sid=UUDJwDsNjrNRgmTvCeiy" -H
"Content-Type: application/json"  --data @vcc_ip_json_file --insecure
```

Sample Configuration

Below is a sample configuration (vcc_ip_json_file) to add or modify the for VC IP address

```
{
"virtual-controller-ip" :
{
"vc-ip" : "10.1.2.3",
}
}
```

NTP Server

Table 11: *NTP Server Configuration*

API	JSON_Payload	Parameters
/rest/ntp-server	`{ "ntp-server" : { "action" :"string", "ntp_server_ip" : "string" }`	**action**—Enter one of the following values: ■ create—add ntp server configuration ■ delete—delete ntp server configuration

Table 11: *NTP Server Configuration*

API	JSON_Payload	Parameters
	}	**ntp_server_ip**—Enter the NTP IP address or domain name.

Syntax

The following is an example for a curl call to configure or modify the NTP Server IP address on masteror standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/ntp-server?sid=UUDJwDsNjrNRgmTvCeiy" -H "Content-Type: application/json"  --data @ntp_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (ntp_add_json_file) to add or modify the ntp server IP address:

```
{
"ntp-server" :
{
"action" : "create",
"ntp_server_ip" : "pool.ntp.org"
}
}
```

Syslocation

Table 12: *Syslocation Configuration*

API	JSON_Payload	Parameters

/rest/syslocation	{
	"syslocation_info" :
	{
	"action" : "string",
	"syslocation" : "string"
	}
	}
		action—Enter one of the following values:
		■ create—add syslocation configuration
		■ delete—delete syslocation configuration
		syslocation—Add the name of the physical location

Syntax

The following is an example for a curl call to configure or modify syslocation on a master Instant AP :

```
curl "https://172.68.104.253:4343/rest/syslocation-code?sid=UUDJwDsNjrNRgmTvCeiy" -H "Content-Type: application/json"  --data @sysloc_add_json_file --insecure
```

Sample Configuration

Below is sample configuration (sysloc_add_json_file) to add or modify the physical location of an Instant:

```
{
"syslocation_info" :
{
"action" : "create",
"syslocation" : "sunnyvale"
}
}
```

Organization

Table 13: *Organization Configuration*

API	JSON_Payload	Parameters

/rest/organization	{
	"organization_info" :
	{
	"action" : "string",
	"organization" : "string"
	}
	}
		action—Enter one of the following values:
		■ create—add organization configuration
		■ delete—delete organization configuration
		organization—Enter the name of your organization

Syntax

The following is an example for curl call to configure/modify organization on Master/Standalone Instant AP :

```
curl "https://172.68.104.253:4343/rest/organization?sid=UUDJwDsNjrNRgmTvCeiy" -H
"Content-Type: application/json"  --data @org_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (org_add_json_file) to add or modify orgnization information on an Instant AP:

```
{
"organization_info" :
{
"action" : "create",
"organization" : "aruba"
}
}
```

Syslog Level

Table 14: *Syslog Level Configuration*

API	JSON_Payload	Parameters

/rest/syslog-level	{
	"syslog-level" :
	{
	"action" : "string",
	"level" : "string",
	"component" : "string"
	}
	}
		action—Enter one of the following values:
		■ create—add syslog-level configuration
		■ delete—delete syslog-level configuration
		level—Configures the Syslog facility level. Enter any of the following logging levels:
		■ Emergency—Panic conditions that occur when the system becomes unusable.
		■ Alert—Any condition requiring immediate attention and correction.
		■ Critical—Any critical conditions such as a hard drive error.
		■ Errors—Error conditions.
		■ Warning—Warning messages.
		■ Notice—Significant events of a noncritical and normal nature. The default value for all Syslog facilities.
		■ Informational—Messages of general interest to system users.

Table 14: *Syslog Level Configuration*

API	JSON_Payload	Parameters
		■ Debug—Messages containing information useful for debugging. **Component**—Enter any of the following components: ■ ap-debug—Generates a log for the Instant AP device for debugging purposes. ■ network—Generates a log when there is a change in the network, for example, when a new Instant AP is added to a network. ■ security—Generates a log for network security, for example, when a client connects using wrong password. ■ system—Generates a log about the system configuration and status. ■ user—Generates a log for the Instant AP clients. ■ user-debug—Generates a detailed log about the clients for debugging purposes. ■ wireless—Generates a log about radio configuration.

Syntax

The following is an example for a curl call to configure or modify the syslog-server on a master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/syslog-server?sid=UUDJwDsNjrNRgmTvCeiy" -H
"Content-
Type: application/json" --data @syslogser_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (syslogser_add_json_file) of the syslog server on the Instant AP :

```
{
"syslog-server" :
{
"action" :
"create" ,
"syslog_server_ip" : "23.5.6.7"
}
}
```

Syslog Server

Table 15: *Syslog Server Configuration*

API	JSON_Payload	Parameters

/rest/syslog-server	`{`
	`"syslog-server" :`
	`{`
	`"action" : "string" ,`
	`"syslog_server_ip" : "string"`
	`}`
		action—This is a mandatory configuration parameter. Enter one of the following values:
		■ create—add syslog-server configuration
		■ delete—delete syslog-server

Table 15: *Syslog Server Configuration*

API	JSON_Payload	Parameters
	}	configuration **syslog_server_ip**—Denotes the IP address of the syslog server.

Syntax

The following is an example for a curl call to configure or modify the syslog-server on a master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/syslog-server?sid=UUDJwDsNjrNRgmTvCeiy" -H
"Content-Type: application/json"  --data @syslogser_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (syslogser_add_json_file) of the syslog server on the Instant AP :

```
{
"syslog-server" :
{
"action" : "create" ,
"syslog_server_ip" : "23.5.6.7"
}
}
```

dot11g Radio Profile

Table 16: *11g Radio Profile Configuration*

API	JSON_Payload	Parameters
/rest/radio-profile-11g	{ "radio-profile-11g" : { "action" : "string", "11g-radio-profile-name" : "string", "40MHZ-intolerance" : "string", "beacon-interval" : integer, "csd-override" : "string", "cell-size-reduction" : { "action" : "string", "value" : integer }, "csa-count" : integer, "max-distance" : integer, "max-tx-power" : integer, "min-tx-power" : integer, "legacy-mode" : "string",) "disable-arm-wids-functions" : { "action" : "string", "value" : "string" }, "dot11h" : "string",true/false, "free-channel-index" : { "action" : "string",	**action**—This is a mandatory parameter. Enter one of the following values: ■ create—add dot11g radio profile ■ delete—delete dot11g radio profile configuration **11g-radio-profile-name**—Denotes the profile name of the 2.4 GHz radio profile. **40MHZ-intolerance**—Controls whether or not Instant APs using this radio profile will advertise intolerance of 40 MHz operation. Select one of the following: ■ enable—Enables the 40 MHz intolerance operation. ■ disable—Disables the 40 MHz intolerance operation **beacon-interval**—Enter the Beacon period for the Instant AP in milliseconds (between 60-500 ms). When enabled, the 802.11 beacon management frames are transmitted by the access point at the specified interval. **cell-size-reduction**—The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an Instant APs receive coverage area. It helps to minimize co-channel interference and optimizes channel reuse.

Table 16: *11g Radio Profile Configuration*

API	JSON_Payload	Parameters

	<pre>"value" : integer
	},
	"honor-40MHZ-intolerance-disable" :
	"string",
	"interference-immunity" : integer,
	"smart-antenna" : "string",
	"spectrum-monitor" : "string",
	"zone" :
	{
	"action" : "string",
	"value" : "string"
	}
	}
	
	}</pre>
		■ **action**—Enter one of the following values:
		● create—add cell-size-reduction configuration
		● delete—remove the cell-size-reduction configuration
		■ **value**—Enter an integer value between 0-55 dB.
		
		NOTE: This value should be changed if the network is experiencing performance issues.
		
		csd-override—Most transmissions to HT stations are sent through multiple antennas using CSD. This option is disabled by default, and should only be enabled under the supervision of Aruba technical support. Use this feature to turn off antenna diversity when the AP must support legacy clients such as Cisco 7921g VoIP phones, or older 802.11g clients (e.g. Intel Centrino clients). Enter one of the following values:
		■ **enable**—When you enable the CSD Override parameter, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n CDD data.
		■ **disable**—Disables the csd override intolerance operation
		csa-count—Specify an integer value between 0-10. This parameter configures the number of channel switching announcements that must be sent before switching to a new channel. This allows associated clients to recover gracefully from a channel change.
		max-distance—Specify an integer value between 600-1000. This parameter configures the maximum distance between a client and an Instant AP or between a mesh point and a mesh portal in meters. This value is used to derive ACK and CTS timeout times.
		max-tx-power—Enter a value between 3 dBm to max. This parameter configures the maximum transmit power value for the 2.4 GHz radio profile.
		min-tx-power—Enter a value between 3 dBm to max. This parameter configures the minimum transmit power value for the 2.4 GHz radio profile.

Table 16: *11g Radio Profile Configuration*

API	JSON_Payload	Parameters
		legacy-mode—Enables the Instant APs to run the radio in non-802.11n mode. Enter one of the following values: ■ **enable**—Enables the legacy-mode feature ■ **disable**—Disables the legacy-mode **disable-arm-wids-functions**—Enter one of the following values: ■ **Dynamic**—By default, WIDS protection is on dynamic mode. If an Instant APis heavily loaded with client traffic and the CPU utilization exceeds the threshold limit, the WIDS processing is suspended. This causes more CPU cycles to handle the client traffic. When the CPU utilization is within the the threshold limit, the WIDS processing is resumed. ■ **On**—When disable-arm-wids-functions is on, the Instant AP will always process frames for WIDS purposes even when it is heavily loaded with client traffic. ■ **Off**—When disable-arm-wids-functions is off, the Instant AP will stop process frames for WIDS purposes regardless of whether the Instant AP is heavily loaded or not. The WIDS functionality will not take effect. **dot11h**—Choose one of the following options: ■ **enable**—Allows the Instant AP to advertise its 802.11d (country information) and 802.11h capabilities ■ **disable**—Disables the dot11h configuration **free-channel-index**—The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25. ■ **action**—Enter one of the following values: ● create—add free-channel-index configuration ● delete—remove the free-channel-index configuration ■ **value**—Enter an integer value between 10-40. **honor-40MHZ-intolerance-disable**—Choose one of the following: ■ **enable**—When this parameter is enabled, the radio will still use the 40 MHz channels even if the 40 MHz intolerance indication is received from another Instant AP or station.

Table 16: *11g Radio Profile Configuration*

API	JSON_Payload	Parameters
		■ **disable**—The radio will not use the 40 MHz channels f the 40 MHz intolerance indication is received from another Instant AP or station. **interference-immunity**—This parameter configures the immunity level to improve performance in high-interference environments. You can specify any of the following immunity levels: ■ **0**— no ANI adaptation. ■ **1**— Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ **2**— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ■ **3**—Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ■ **4**— Level 3 settings, and FIR immunity. At this level, the Instant AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ **5**— The I Instant APcompletely disables PHY error reporting, improving performance by eliminating the time the Instant AP would spend on PHY processing. **NOTE:** Increasing the immunity level makes the Instant AP to lose a small amount of range. **smart-antenna**—Choose one of the following: ■ **enable**—This feature, when enabled, helps optimize the selection of antenna polarization values based on the data collected from the training of polarization pattern combinations. It identifies the clients most likely to benefit from smart antenna polarization, based on the average RSSI of the received frames and the

Table 16: *11g Radio Profile Configuration*

API	JSON_Payload	Parameters
		number of streams. This feature uses frame-based antenna training, which allows the Instant AP to cycle through training combinations and collect statistics without causing any impact on the client. At the end of the training sequence, the Instant AP selects the best antenna polarization based on these collected statistics. The smart antenna feature does not support optimized antenna polarization for clients using SU or MU transmit beamforming, and will use default polarization values for these clients. ■ **disable**—disables the smart-antenna configuration. **spectrum-monitor**—Choose one of the following: ■ **enable**—Allows the Instant APs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring Instant APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients. ■ **disable**—Disables spectrum monitor. **zone**—Configures a zone name for the radio profile. **NOTE:** NOTE: This parameter cannot be configured on a default radio profile. Following are the zone configuration parameters: ■ **action**—Choose one of the following: ● create—add the zone configuration on the Instant AP. ● delete—remove the zone configuration. ■ **value**—Enter a string value.

Syntax

The following is an example for curl call to configure/modify dot11g-radio-profile on Master/Standalone Instant AP :

```
curl "https://172.68.104.253:4343/rest/radio-profile-11g?sid=UUDJwDsNjrNRgmTvCeiy" -H
"Content-Type: application/json"  --data @11gprofile_add_json_file --insecure
```

Sample Configuration

Below is sample 11gprofile_add_json_file to configure dot11g radio profile on Instant AP:

```
{
"radio-profile-11g" :
{
"action" : "create",
"11g-radio-profile-name" : "dot11g-radio",
```

```
"40MHZ-intolerance" : "enable",
"beacon-interval" : 500,
"csd-override" : "enable",
"cell-size-reduction" :
{
"action" : "create",
"value" : 5
},
"csa-count"  : 1,
"max-distance" : 2,
"max-tx-power" : 18,
"min-tx-power" : 12,
"legacy-mode" : "disable",
"disable-arm-wids-functions" :
{
"action" : "create",
"value" : "dynamic"
},
"dot11h" : "enable",
"free-channel-index" :
{
"action" : "create",
"value" : 40
},
"honor-40MHZ-intolerance-disable" : "enable",
"interference-immunity" : 5,
"smart-antenna" : "enable",
"spectrum-monitor" : "enable",
"zone" :
{
"action" : "create",
"value" : "radio-outdoor"
}
}
}
```

ARM

Table 17: *ARM Configuration*

API	JSON_Payload	Parameters

/rest/arm	`{`
	`"arm" :`
	`{`
	`"action" : "string",`
	`"a-channels" :`
	`{`
	`"action" : "string",`
	`"a-channel" : "string"`
	`},`
	`"g-channels" :`
	`{`
	`"action" : "string",`
	`"g-channel" : "string"`
	`},`
	`"air-time-fairness-mode" :`
	`{`
	`"action" : "string",`
	`"value" : "string"`
		action—This is a mandatory configuration parameter. Enter one of the following values:
		■ **create**—add arm configuration
		■ **delete**—delete arm configuration
		a-channels—Configures 5 GHz channels.
		■ **action**—Enter one of the following values:
		● create—add a 5 GHz channel
		● delete—delete the 5 GHz channel
		■ **g-channel**—Enter a valid channel number determined by the Instant AP regulatory domain.
		air-time-fairness-mode—Allows equal access to all clients on the wireless medium, regardless of client type, capability, or operating system and prevents the clients from monopolizing resources.
		■ **action**—Enter one of the following

Table 17: *ARM Configuration*

API	JSON_Payload	Parameters

	<pre>},
	"band-steering-mode" :
	{
	"action" : "string",
	"value" : "string"
	},
	"min-tx-power" :
	{
	"action" : "string",
	"power" : "string"
	},
	"max-tx-power" :
	{
	"action" : "string",
	"power" : "string"
	},
	"client-aware" : "string",
	"wide-bands" : "string",
	"80mhz-support" : "string",
	"scanning" : "string",
	"client-match" :
	{
	"enable" : "string",
	"calc-interval" :
	{
	"action" :
	"value" : <INT:interval>
	},
	"nb-matching" :
	{
	"action" : "string",
	"value" : <INT:pct>
	},
	"calc-threshold" :
	{
	"action" : "string",
	"value" : <INT:thresh>
	},
	"slb-mode" :
	{
	"action" : "string",
	"value" : <INT:mode>
	},
	"max-request" :
	{
	"action" : "string",
	"value" : <INT:req>
	},
	"max-adoption" :
	{
	"action" : "string",
	"value" : <INT:adopt>
	},
	"holdtime" :
	{</pre>
		values:
		● create—configure air-time-fairness-mode
		● delete—delete air-time-fairness-mode configuration
		■ **value**—Enter one of the following modes:
		● default-access—To provide access based on client requests. When this mode is configured, the per user and per SSID bandwidth limits are not enforced.
		● fair-access—To allocate Airtime evenly across all the clients.
		● preferred-access—To set a preference where 802.11n clients are assigned more airtime than 802.11a or 802.11g. The 802.11a or 802.11g clients get more airtime than 802.11b. The ratio is 16:4:1.
		band-steering-mode—Assigns the dual-band capable clients to the 5 GHz band on dual-band. It reduces co-channel interference and increases available bandwidth for dual band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band.
		■ **action**—Enter one of the following values:
		● create—configure band-steering-mode
		● delete—delete band-steering-mode configuration
		■ **value**—Enter one of the following band steering modes:
		● prefer-5ghz—To allow the Instant AP to steer the client to 5 GHz band (if the client is 5 GHz capable). However, the Instant AP allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
		● force-5ghz—To enforce 5 GHz band steering mode on the Instant APs, so that the 5 GHz capable clients are allowed to use only the 5 GHz channels.
		● balance-bands—To allow the Instant APs to balance the clients across the two 2.4 GHz and 5 GHz radio and to utilize the available bandwidth.
		● disable—To allow the clients to select the bands.
		min-tx-power—This parameter sets the minimum transmission power. This indicates the minimum EIRP. If the minimum transmission EIRP setting configured on an Instant AP is not supported by the Instant AP model, this value is reduced to the highest supported power setting.

Table 17: *ARM Configuration*

API	JSON_Payload	Parameters

	<pre>"action" : "string",
	"value" : <INT:adopt>
	},
	"good-snr" :
	{
	"action" : "string",
	"value" : <INT:snr>
	},
	"key" :
	{
	"action" : "string",
	"value" : <STRING:key>
	},
	"bad-snr" :
	{
	"action" : "string",
	"value" : <INT:interval>
	},
	"snr-thresh" :
	{
	"action" : "string",
	"value" : <INT:snr>
	},
	"client-thresh" :
	{
	"action" : "string",
	"value" : <INT:thresh>
	},
	"report-interval" :
	{
	"action" : "string",
	"value" : <INT:interval>
	},
	"vbr-entry-age" :
	{
	"action" : "string",
	"value" : <INT:age>
	},
	"sta-entry-age" :
	{
	"action" : "string",
	"value" : <INT:age>
	},
	"restriction-timeout" :
	{
	"action" : "string",
	"value" : <INT:time>
	},
	"debug" :
	{
	"action" : "string",
	"value" : <INT:level>
	}
	}
	}</pre>
		■ **action**—Enter one of the following values:
		● create—configure minimum transmission power on the Instant AP.
		● delete—delete minimum transmission power configuration
		■ **power**—Enter a value between 0-127 dBm.
		max-tx-power—Sets the highest transmit power levels for the Instant AP. If the maximum transmission EIRP configured on an Instant AP is not supported by the Instant AP model, the value is reduced to the highest supported power setting.
		■ **action**—Enter one of the following values:
		● create—configure maximum transmission power on the Instant AP.
		● delete—delete maximum transmission power configuration
		■ **power**—Enter a value between 0-127 dBm.
		
		NOTE: Higher power level settings may be constrained by local regulatory requirements and Instant AP capabilities.
		
		client-aware—This parameter is enabled by default. Following are the configuration options:
		■ **enable**—Enables the client aware feature. When enabled, the Instant AP will not change channels for the Access Points when clients are active, except for high priority events such as radar or excessive noise. The client aware feature must be enabled in most deployments for a stable WLAN.
		■ **disable**—Disables the client aware feature.
		wide-bands—Allows administrators to configure 40 MHz. channels in the 2.4 GHz and 5 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. The 40 MHz channels double the frequency bandwidth available for data transmission. For high performance, enter 5 GHz. If the Instant AP density is low, enter 2.4 GHz. Choose one of the following:
		■ none
		■ all
		■ 2.4 GHz
		■ 5 GHz
		80mhz-support—Only the Instant APs that support 802.11ac can be configured with 80 MHz channels. Choose one of the following options:

Table 17: *ARM Configuration*

API	JSON_Payload	Parameters
	} ■ **action**—Enter one of the following values: ● create—add ARM configuration ● delete—delete ARM configuration	■ **enable**—Enables the use of 80 MHz channels on Instant APs with 5 GHz radios, which support a VHT. ■ **disable**—Disables the 80 MHz channel **scanning**—This option is enabled by default. ■ **enable**—Allows the Instant APs to scan other channels for RF Management and WIPS enforcement. ■ **disable**—Disables the channel scan operation **client-match**—When the client match feature is enabled on an Instant AP, the Instant AP measures the RF health of its associated clients. If the client's RSSI is less than 18dB but has a good RSSI with another Instant AP having an RSSI of more than 30db or atleast 10db more than its current RSSI, the client will be moved to the Instant AP with the higher RSSI for better performance and client experience. In the current release, the client match feature is supported only within the Instant APs within the swarm. ■ **action**—Enter one of the following values: ● enable—enables client match on the Instant AP. ● disable—disables the client match configuration **calc-interval**—Configures an interval at which client match is calculated. ■ **action**—Enter one of the following values: ● enable—enables cal-interval function on the Instant AP. ● disable—disables the cal-interval configuration ■ **value**—Enter a value between 1-600 seconds. The default value is 3. **nb-matching**—Configures a percentage value to be considered in the same virtual RF neighborhood of Client match. ■ **action**—Enter one of the following values: ● enable—enables nb-matching function on the Instant AP. ● disable—disables the nb-matching configuration ■ **value**—Enter a percentage value between 20-100%. The default value is 60%. **calc-threshold**—Configures a threshold that takes acceptance client count difference among all the channels of Client match into account. When the client load on an Instant AP reaches or exceeds the threshold in comparison, client match is enabled on that Instant AP. ■ **action**—Enter one of the following

Table 17: *ARM Configuration*

API	JSON_Payload	Parameters
		values: ● enable—enables calc-threshold configuration on the Instant AP. ● disable—disables the calc-threshold configuration ■ **value**—Enter a threshold value between 1-255. The default value is 5. **slb-mode**—Configures a balancing strategy for client match. ■ **action**—Enter one of the following values: ● enable—enables slb-mode on the Instant AP. ● disable—disables the slb-mode configuration ■ **value**—Enter one of the following values: ● 1—Channel-based ● 2—Radio-based ● 3—Channel and Radio based **max-request**—Configures the maximum number of requests for client match. ■ **action**—Enter one of the following values: ● enable—enables max-request configuration on the Instant AP. ● disable—disables the max-request configuration ■ **value**—Enter a value for the maximum number of requests between 0-100. The default value is 10. **max-adoption**—Configure a maximum number for adopting clients. ■ **action**—Enter one of the following values: ● enable—enables max-adoption configuration on the Instant AP. ● disable—disables the max-adoption configuration ■ **value**—Enter a value for the maximum number of requests between 0-100. The default value is 10. **holdtime**—Configures the hold time for the next client match action on the same client. ■ **action**—Enter one of the following values: ● enable—enables the holdtime configuration on the Instant AP. ● disable—disables the holdtime configuration ■ **value**—Enter a value for the holdtime between 1-1800. The default value is 300. **good-snr**—The Instant APs with a RSSI higher than the specified good-snr value will be considered as a potential target Instant AP. ■ **action**—Enter one of the following values: ● enable—enables the good-snr

Table 17: *ARM Configuration*

API	JSON_Payload	Parameters
		configuration on the Instant AP. ● disable—disables the good-snr configuration ■ **value**—Enter a value for the good-snr between 1-100. The default value is 30. **key**—Configures the client match key of an Instant AP. ■ **action**—Enter one of the following values: ● enable—enables the key configuration on the Instant AP. ● disable—disables the key configuration ■ **value**—Enter a value for the key between 1–2147483646. **bad-snr**—The clients with an SNR value below the threshold value will be moved to a potential target Instant AP. ■ **action**—Enter one of the following values: ● enable—enables the bad-snr configuration on the Instant AP. ● disable—disables the bad-snr configuration ■ **value**—Enter a value for the bad-snr between 0-100. The default value is 18. **client-thresh**—When the number of clients on a radio exceeds the value, SLB algorithm will be triggered. ■ **action**—Enter one of the following values: ● enable—enables the client-thresh configuration on the Instant AP. ● disable—disables the client-thresh configuration ■ **value**—Enter a value for the client-thresh between 0-255. The default value is 30. **report-interval**—Configures the report interval of VBR on each Instant AP. ■ **action**—Enter one of the following values: ● enable—enables the report interval configuration on the Instant AP. ● disable—disables the report interval configuration ■ **value**—Enter a value for the report interval between 0-3600. The default value is 30. **vbr-entry-age**—Denotes the aging time for stable VBR entries. ■ **action**—Enter one of the following values: ● enable—enables the vbr-entry-age configuration on the Instant AP. ● disable—disables the vbr-entry-age configuration ■ **value**—Enter a value for the vbr-entry-

Table 17: *ARM Configuration*

API	JSON_Payload	Parameters
		age between 1-3600. The default value is 30. **sta-entry-age**—Denotes the aging time of stale STA entries. ■ **action**—Enter one of the following values: ● enable—enables the sta-entry-age configuration on the Instant AP. ● disable—disables the sta-entry-age configuration ■ **value**—Enter a value for the sta-entry-age between 1-3600. The default value is 1000. **restriction-timeout**—Configures the timeout interval during which non-target Instant AP will not respond to a specific client. ■ **action**—Enter one of the following values: ● enable—enables the restriction-timeout configuration on the Instant AP. ● disable—disables the restriction-timeout configuration ■ **value**—Enter a value for the sta-entry-age between 1-255. The default value is 10. **debug**—Displays information required for debugging client match issues. ■ **action**—Enter one of the following values: ● enable—enables the debug configuration on the Instant AP. ● disable—disables the debug configuration ■ **value**—Enter a value from 0-4 for the debug level: ● 0—none ● 1—error ● 2—information ● 3—debug ● 4—dump

Syntax

The following is an example for a curl call to configure or modify ARM on a master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/arm?sid=UUDJwDsNjrNRgmTvCeiy" -H "Content-Type:
application/json"  --data @arm_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (arm_add_json_file) to create or modify an ARM profile on the Instant AP:

```
{
"arm" :
{
"action" : "create",
"min-tx-power" :
{
"action" : "create",
```

```
"power" : "18"
},
"max-tx-power" :
{
"action" : "create",
"power" : "127"
},
"client-aware" :  "enable",
"80mhz-support" : "enable",
"scanning" : "disable",
"wide-bands" : "5ghz",
"a-channels" :
{
"action" : "create",
"a-channel" : "44"
},
"air-time-fairness-mode" :
{
"action" : "create",
"value" : "fair-access"
},
"band-steering-mode" :
{
"action" : "create",
"value" : "balance-bands"
},
"wide-bands" : "5ghz",
"client-match" :
{
"enable" : "no",
"bad-snr" :
{
"action" : "enable",
"value" : 13
},
"calc-threshold" :
{
"action" : "enable",
"value" : 3
},
"slb-mode" :
{
"action" : "enable",
"value" : 1
},
"max-request" :
{
"action" : "enable",
"value" :  3
},
"sta-entry-age" :
{
"action" : "enable",
"value" : 30
},
"restriction-timeout" :
{
"action" : "enable",
"value" : 3
},
"debug" :
```

```
{
"action" : "enable",
"value" : 2
},
"client-thresh" :
{
"action" : "enable",
"value" : 3
},
"report-interval" :
{
"action" : "enable",
"value" : 3
},
"vbr-entry-age" :
{
"action" : "enable",
"value" : 39
},
"bad-snr" :
{
"action" : "enable",
"value" : 3
},
"snr-thresh" : {
"action" : "enable",
"value" : 3
},
"key" : {
"action" : "enable",
"value" : "2147483646"
},
"max-adoption" : {
"action" : "enable",
"value" : 3
},
"holdtime" : {
"action" : "enable",
"value" : 3
},
"good-snr" : {
"action" : "enable",
"value" : 3
},
"calc-interval" : {
"action" : "enable",
"value" : 3
},
"nb-matching" : {
"action" : "enable",
"value" : 30
}
}
}
}
```


dot11a Radio Profile

Table 18: *11a Radio Profile Configuration*

API	JSON_Payload	Parameters

/rest/radio-profile-11a	<pre>{
	"radio-profile-11a" :
	{
	"action" : "string",
	"11a-radio-profile-name" : "string",
	"40MHZ-intolerance" : "string",
	"beacon-interval" : integer,
	"csd-override" : "string",
	"cell-size-reduction" : {
	"action" : "string",
	"value" : integer
	},
	"csa-count" : integer,
	"max-distance" : integer,
	"max-tx-power" : integer,
	"min-tx-power" : integer,
	"legacy-mode" : "string",
	"disable-arm-wids-functions" :
	{
	"action" : "string",
	"value" : "string"
	},
	"dot11h" : "string",
	"free-channel-index" :
	{
	"action" : "string",
	"value" : integer
	},
	"honor-40MHZ-intolerance-disable" :
	"string",
	"interference-immunity" : integer,
	"smart-antenna" : "string",
	"spectrum-band" : "string",
	"spectrum-monitor" : "string",
	"very-high-throughput-disable" :
	"string",
	"zone" :
	{
	"action" : "string",
	"value" : "string"
	}
	}
	
	}</pre> ■ **action**—Enter one of the following values:
	● create—add a dot11a radio profile
	● delete—delete dot11a radio profile configuration
		action—This is a mandatory configuration parameter.. Enter one of the following values:
		■ create—add dot11a radio profile
		■ delete—delete dot11a radio profile configuration
		11a-radio-profile-name—Denotes the profile name of the 5 GHz radio profile.
		40MHZ-intolerance—Controls whether or not Instant APs using this radio profile will advertise intolerance of 40 MHz operation. Select one of the following:
		■ enable—Enables the 40 MHz intolerance operation.
		■ disable—Disables the 40 MHz intolerance operation
		beacon-interval—Enter the Beacon period for the Instant AP in milliseconds (between 60-500 ms). When enabled, the 802.11 beacon management frames are transmitted by the access point at the specified interval.
		cell-size-reduction—The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an Instant APs receive coverage area. It helps to minimize co-channel interference and optimizes channel reuse.
		■ **action**—Enter one of the following values:
		● create—add cell-size-reduction configuration
		● delete—remove the cell-size-reduction configuration
		■ **value**—Enter an integer value between 0-55 dB.
		
		NOTE: This value should be changed if the network is experiencing performance issues.

Table 18: *11a Radio Profile Configuration*

API	JSON_Payload	Parameters
		csd-override—Most transmissions to HT stations are sent through multiple antennas using CSD. This option is disabled by default, and should only be enabled under the supervision of Aruba technical support. Use this feature to turn off antenna diversity when the AP must support legacy clients such as Cisco 7921g VoIP phones, or older 802.11a clients (e.g. Intel Centrino clients). Enter one of the following values: ■ **enable**—When you enable the CSD Override parameter, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n CDD data. ■ **disable**—Disables the csd override intolerance operation **csa-count**—Specify an integer value between 0-10. This parameter configures the number of channel switching announcements that must be sent before switching to a new channel. This allows associated clients to recover gracefully from a channel change. **max-distance**—Specify an integer value between 600-1000. This parameter configures the maximum distance between a client and an Instant AP or between a mesh point and a mesh portal in meters. This value is used to derive ACK and CTS timeout times. **max-tx-power**—Enter a value between 3 dBm to max. This parameter configures the maximum transmit power value for the 5 GHz radio profile. **min-tx-power**—Enter a value between 3 dBm to max. This parameter configures the minimum transmit power value for the 5 GHz radio profile. **legacy-mode**—Enables the Instant APs to run the radio in non-802.11n mode. Enter one of the following values: ■ **enable**—Enables the legacy-

Table 18: *11a Radio Profile Configuration*

API	JSON_Payload	Parameters
		mode feature ■ **disable**—Disables the legacy-mode **disable-arm-wids-functions**—Enter one of the following values: ■ **Dynamic**—By default, WIDS protection is on dynamic mode. If an Instant APis heavily loaded with client traffic and the CPU utilization exceeds the threshold limit, the WIDS processing is suspended. This causes more CPU cycles to handle the client traffic. When the CPU utilization is within the the threshold limit, the WIDS processing is resumed. ■ **On**—When disable-arm-wids-functions is on, the Instant AP will always process frames for WIDS purposes even when it is heavily loaded with client traffic. ■ **Off**—When disable-arm-wids-functions is off, the Instant AP will stop process frames for WIDS purposes regardless of whether the Instant AP is heavily loaded or not. The WIDS functionality will not take effect. **dot11h**—Choose one of the following options: ■ **enable**—Allows the Instant AP to advertise its 802.11d (country information) and 802.11h capabilities ■ **disable**—Disables the dot11h configuration **free-channel-index**—The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25. ■ **action**—Enter one of the following values: ● create—add free-channel-index configuration ● delete—remove the free-channel-index configuration ■ **value**—Enter an integer value between 10-40. **honor-40MHZ-intolerance-disable**—Choose one of the following:

Table 18: *11a Radio Profile Configuration*

API	JSON_Payload	Parameters
		■ **enable**—When this parameter is enabled, the radio will still use the 40 MHz channels even if the 40 MHz intolerance indication is received from another Instant AP or station. ■ **disable**—The radio will not use the 40 MHz channels f the 40 MHz intolerance indication is received from another Instant AP or station. **interference-immunity**—This parameter configures the immunity level to improve performance in high-interference environments. You can specify any of the following immunity levels: ■ **0**— no ANI adaptation. ■ **1**— Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ **2**— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ■ **3**—Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 5 GHz appliances such as cordless phones. ■ **4**— Level 3 settings, and FIR immunity. At this level, the Instant AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ **5**— The I Instant APcompletely disables PHY error reporting, improving performance by eliminating the time the Instant AP would spend on PHY processing.

Table 18: *11a Radio Profile Configuration*

API	JSON_Payload	Parameters
		NOTE: Increasing the immunity level makes the Instant AP to lose a small amount of range. **smart-antenna**—Choose one of the following: ■ **enable**—This feature, when enabled, helps optimize the selection of antenna polarization values based on the data collected from the training of polarization pattern combinations. It identifies the clients most likely to benefit from smart antenna polarization, based on the average RSSI of the received frames and the number of streams. This feature uses frame-based antenna training, which allows the Instant AP to cycle through training combinations and collect statistics without causing any impact on the client. At the end of the training sequence, the Instant AP selects the best antenna polarization based on these collected statistics. The smart antenna feature does not support optimized antenna polarization for clients using SU or MU transmit beamforming, and will use default polarization values for these clients. ■ **disable**—disables the smart-antenna configuration. **spectrum-band**—Allows you to specify the portion of the channel to monitor for 5 GHz configuration. **spectrum-monitor**—Choose one of the following: ■ **enable**—Allows the Instant APs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring Instant APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients. ■ **disable**—Disables spectrum monitor. **very-high-throughput-disable**—Select one of the following:

Table 18: *11a Radio Profile Configuration*

API	JSON_Payload	Parameters
		■ **enable**—Disables VHT for clients connecting on the 5 GHz band. ■ **disable**—enables the VHT for clients connecting on the 5 GHz band. **zone**—Configures a zone name for the radio profile. **NOTE:** This parameter cannot be configured on a default radio profile. Following are the zone configuration parameters: ■ **action**—Choose one of the following: ● create—add the zone configuration on the Instant AP. ● delete—remove the zone configuration. ■ **value**—Enter a string value.

Syntax

The following is an example for a curl call to configure or modify a dot11a-radio-profile on a master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/radio-profile-11a?sid=UUDJwDsNjrNRgmTvCeiy" -H
"Content-Type: application/json"  --data @11aprofile_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (11aprofile_add_json_file) to create or modify a dot11a radio profile on an Instant AP:

```
{
"radio-profile-11a" : {
"action" : "create",
"11a-radio-profile-name" : "dot11a-radio",
"40MHZ-intolerance" : "enable",
"beacon-interval" : 500,
"csd-override" : "enable",
"cell-size-reduction" : {
"action" : "create",
"value" : 5
},
"csa-count"  : 1,
"max-distance" : 2,
"max-tx-power" : 18,
"min-tx-power" : 12,
"legacy-mode" : "disable",
"disable-arm-wids-functions" : {
"action" : "create",
"value" : "dynamic"
},
"dot11h" : "enable",
"free-channel-index" : {
"action" : "create",
```

```
"value" : 40
},
"honor-40MHZ-intolerance-disable" : "enable",
"interference-immunity" : 5,
"smart-antenna" : "enable",
"spectrum-band" : "5ghz-middle",
"very-high-throughput-disable" : "enable",
"spectrum-monitor" : "enable",
"zone" : {
"action" : "create",
"value" : "radio-outdoor"
}
}
}
```

SSID Profile

Table 19: *SSID Profile Configuration*

API	JSON_Payload	Parameters

/rest/ssid	<pre>{
	"ssid-profile" :
	{
	"action" : "string",
	"ssid-profile" : "string",
	"essid":
	{
	"action" : "string",
	"value" : "string"
	},
	"type": "string",
	"opmode" : "string",
	"wpa-passphrase": "string",
	"vlan":
	{
	"action" : "string",
	"value" : "string"
	},
	"rf-band": "string",
	"enable": "string",
	"disable" : "string",
	"captive-portal":
	{
	"external" : "string",
	"profile" : "string",
	"profile_name" : "string",
	"exclude-uplink" : "string",
	"exclude-uplink-types" : "string",
	"captive-portal-type" : "string"
	},
	"hide-ssid": "string",
	"dtim-period":
	{
	"action" : "string",
	"value" : integer
	},
	"broadcast-filter":
	{
	"action" : "string",</pre>
		action—This is a mandatory configuration parameter. Enter one of the following values:
		■ create—add an SSID Profile
		■ delete—delete SSID profile configuration
		essid—Defines a variable for each Instant AP that identifies a WLAN network.
		■ **action**—Enter one of the following values:
		● create—add an ESSID
		● delete—delete ESSID
		■ **value**—Specify an ESSID name of your choice.
		type—Choose the type of network (Employee, Voice, or Guest)
		opmode—Select a type of opmode (opensystem, wpa2-aes, wpa2-psk-aes, wpa-tkip, wpa-psktkip, wpa-tkip wpa2-aes, wpa-psk-tkip, wpa2-psk-aes, static-wep, dynamicwep, mpsk-aes, wpa3-open, wpa3-sae-aes)
		wpa-passphrase—Specify a WPA passphrase of your choice.
		vlan—Allows you to assign a unique VLAN ID or a VLAN name to a specified SSID user.
		■ **action**—Enter one of the following values:
		● create—add a VLAN ID
		● delete—delete VLAN ID
		■ **value**—Specify a VLAN ID between 1-4095.
		rf-band—Specify a radio frequency band:
		■ 2.4—configures the 2.4 GHz radio profile
		■ 5.0—configures the 5 GHz radio profile
		■ all—configures both 2.4 GHz and 5 GHz radio profile

Table 19: *SSID Profile Configuration*

API	JSON_Payload	Parameters

	<pre>"value" : "string"
	},
	"g-min-tx-rate": "string",
	"a-min-tx-rate": "string",
	"a-basic-rates":
	{
	"action" : "string",
	"value" : "string"
	},
	"g-basic-rates": {
	"action" : "string",
	"value" : "string"
	},
	"dmo-channel-utilization-threshold":
	integer,
	"local-probe-req-thresh": integer,
	"max-clients-threshold": integer,
	"dot11k": "string",
	"dot11r": "string",
	"dot11v": "string",
	"mdid" :
	{
	"action" : "string",
	"value" : integer
	},
	"auth-server" :
	{
	"action" : "string",
	"value" : "string"
	},
	"deny-inter-user-bridging" :
	"string",
	"deny-local-routing" : "string",
	"max-authentication-failures" :
	integer
	
	}
	}</pre>
		enable—Select **Yes** to re-enable the deactivated SSIDs.
		disable—Select **Yes** to disable the SSID.
		captive portal—Configures captive portal authentication for the SSID.
		■ external—Select **Yes**
		■ profile—Select **Yes**
		■ profile_name—Enter a profile name.
		■ exclude-uplink—Select **Yes**
		hide-ssid—Hides the SSID. When enabled, the SSID will not be visible for the users. Select **Enabled** or **Disabled**.
		dtim-period—Configures the DTIM interval for the SSID profile
		■ **action**—Enter one of the following values:
		● create—add a DTIM period
		● delete—delete DTIM period configuration
		■ **value**—Choose a value between 1-10 beacons.
		broadcast-filter—Configures broadcast filtering parameters.
		■ **action**—Enter one of the following values:
		● create—add a broadcast filter
		● delete—delete broadcast filter configuration
		■ **value**—Choose a value (All, ARP, Unicast-ARP-Only, or Disabled)
		g-min-tx-rate—Choose a minimum transmit rate for the 2.4 GHz band (1, 2, 5, 6,9,11,12,18, 2, 4, 36, 48, 54 in Mbps).
		a-min-tx-rate—Choose a minimum transmission rate for the 5 GHz band (6,9,12,18,24,36,48,54 in Mbps)
		a-basic-rates—Allows you to define a set of modulation rates to use for the clients on the 5 GHz radio band.
		■ **action**—Enter one of the following values:
		● create—add modulation rates
		● delete—delete modulation rates configuration
		■ **value**—Choose a value for the 5 GHz band (6,9,12,18,24,36,48,5,4 in Mbps).
		g-basic-rates—Allows you to define a set of modulation rates to use for the clients on the 2.4 GHz radio band.
		■ **action**—Enter one of the following values:
		● create—add modulation rates
		● delete—delete modulation rates configuration
		■ **value**—Choose a value for the 2.4 GHz band (1,2,5,6,9,11,12,18,2,4,36,48,54 in Mbps).

Table 19: *SSID Profile Configuration*

API	JSON_Payload	Parameters
		dmo-channel-utilization-threshold—Select a value between 1-100 for DMO channel utilization. **local-probe-req-thresh**—Enter a RSSI threshold value between 0-100 dB to limit the number of incoming probe requests. **max-clients-threshold**—Enter a value between 0-100 for max clients threshold limit. **dot11k**—Select **enable** or **disable** **dot11r**—Select **enable** or **disable** **dot11v**—Select **enable** or **disable** mdid—Denotes the mobility domain identifier. ■ **action**—Enter one of the following values: ● create—add MDID ● delete—delete MDID configuration ■ **value**—Choose a value between 1–65535. **auth-server**—Configures an authentication server for the SSID users. ■ **action**—Enter one of the following values: ● create—add auth-server ● delete—delete auth-server configuration ■ **value**—Specify a name for the authentication server. **deny-inter-user-bridging**—Select **enable** to disable the bridging traffic between two clients connected to the same SSID. **deny-local-routing**—Select **enable** or **disable** **max-authentication-failures**—Specify an integer value to configure the maximum number of authentication failures to dynamically blacklist the users.

Syntax

The following is an example for a curl call to configure or modify the ssid profile on Instant AP :

```
curl "https://172.68.104.253:4343/rest/ssid?sid=Gmr6BQ9QW7qAaMWw0kbT" -H "Content-Type:
application/json"  --data @ssid_json_file -insecure
```

Sample Configuration

The following is a sample configuration to create or modify an SSID profile on an Instant AP:

```
{
"ssid-profile" :
{
"action" : "create",
"ssid-profile" : "AA-Cabin123",
"essid": {
"action" : "create",
"value" : "AA-Cabin123"
},
"type": "employee",
"opmode" : "wpa2-psk-aes",
```

```
"wpa-passphrase": "abcefgg@123",
"vlan": {
"action" : "create",
"value" : "102"
},
"rf-band": "5.0",
"enable": "yes",
"dtim-period": {
"action" : "create",
"value" : 1
},
"broadcast-filter": {
"action" : "create",
"value" : "arp"
},
"g-min-tx-rate": "1",
"a-min-tx-rate": "6",
"a-basic-rates":{
"action" : "create",
"value" : "6,9"
},
"g-basic-rates": {
"action" : "create",
"value" : "11"
},
"dmo-channel-utilization-threshold": 90,
"local-probe-req-thresh": 0,
"max-clients-threshold": 64,
"dot11k": "enable",
"dot11r": "enable",
"dot11v": "enable",
"mdid" : {
"action" : "create",
"value" : 65535
},
"auth-server" : {
"action" : "create",
"value" : "auth_server"
},
"deny-inter-user-bridging" : "enable",
"deny-local-routing" : "enable",
"max-authentication-failures" : 0
}
}
```

RF Band

Table 20: *RF Band Configuration*

API	JSON_Payload	Parameters

/rest/rf-band	`{`
	`"rf_band_info" :`
	`{`
	`"rf-band" : "string"`
	`}`
	`}`
		■ **rf-band**—Enter one of the following values:
		● 2.4—configures the 2.4 GHz radio profile
		● 5.0—configures the 5 GHz radio profile
		● all—configures both 2.4 GHz and 5 GHz radio profile

Syntax

The following is an example for a curl call to configure or modify the rf-band on an Instant AP:

```
curl "https://172.68.104.253:4343/rest/rf-band?sid=Gmr6BQ9QW7qAaMWw0kbT" -H "Content-Type: application/json"  --data @rf_band.json_file -insecure
```

Sample Configuration

Below is a sample configuration (rf_band_json_file) to configure a 5 GHz rf-band on an Instant AP:

```
{
"rf_band_info" :
{
"rf-band" : "5"
}
}
```

Authentication Server Profile

Table 21: *Authentication Server Profile Configuration*

API	JSON_Payload	Parameters

/rest/auth-server	<pre>{
	"auth-server-config" :
	{
	"action": string
	"auth-profile-name": string,
	"port": integer,
	"acctport" :
	{
	"action": string
	"value": integer,
	},
	"deadtime" :
	{
	"action": string,
	"value": integer,
	},
	"timeout" :
	{
	"action": string,
	"value": integer
	},
	"retry-count" :
	{
	"action": string
	"value": integer
	},
	"ip": string
	"key": string,
	
	"nas-id" :
	{
	"action": string
	"value": string
	},
	"nas-ip" :
	{
	"action": string],
	"value": string
	}
	}</pre>
		action—This is a mandatory configuration parameter. Enter one of the following values:
		■ create—configure an authentication server profile
		■ delete—delete authentication server profile configuration
		auth-profile-name—Specify a name for the authentication server profile.
		port—Configure the authorization port number of the external RADIUS server.
		acctport—Configures the accounting port number used for sending accounting records to the RADIUS server.
		■ **action**—Enter one of the following values:
		● create—configure an accounting port for the auth-server profile
		● delete—delete accounting port configuration
		■ value—Enter the accounting port number.
		deadtime—Configures a dead time interval for the authentication server.
		■ **action**—Enter one of the following values:
		● create—add a new deadtime for the auth-server profile
		● delete—delete deadtime configuration
		■ **value**—Enter a value for the deadtime between 1-1440 minutes.
		timeout—Configures a timeout value in seconds to determine when a RADIUS request must expire.
		■ **action**—Enter one of the following values:
		● create—add a timeout for the auth-server profile
		● delete—delete timeout configuration

Table 21: *Authentication Server Profile Configuration*

API	JSON_Payload	Parameters
	<pre>}</pre>	■ **value**—Enter a value for the timeoutbetween 1-30 seconds. **retry-count**—Configures the maximum number of authentication requests that can be sent to the server group. ■ **action**—Enter one of the following values: ● create—add retry count. ● delete—delete retry count ■ **value**—Enter a value for the retry count between 1-5. **ip**—Specify the IP address or the host name of the RADIUS server. **key**—Specify the shared key communicating with the external RADIUS server. **nas-ip**—Configures the Virtual Controller IP address as the NAS address which is sent in data packets. ■ **action**—Enter one of the following values: ● create—add NAS IP configuration ● delete—delete NAS IP configuration ■ **value**—Enter the IP address for the NAS IP.

Syntax

The following is an example for curl call to configure/modify auth-server on Instant AP

```
curl "https://172.68.104.253:4343/rest/auth-server?sid=ry9okDtURmxiU6NxqaMN" -H "Content-Type: application/json"  --data @auth_cfg_add_json_file –insecure
```

Sample Configuration

Below is a sample configuration (auth_cfg_add_json_file) to configure an authentication server profile on an Instant AP:

```
{
"auth-server-config" :
{
"action": "create" ,
"auth-profile-name": "auth-server",
"port": 1812,
"acctport" :
{
"action": "create",
"value": 1813
},
"deadtime" :
{
"action": "create",
"value": 360
},
"timeout" :
{
"action": "create",
"value": 60
```

```
},
"retry-count" :
{
"action": "create",
"value": 4
},
"ip": "10.2.3.4",
"key": "itsabug",
"nas-id" :
{
"action": "create",
"value": "abcdefgh"
},
"nas-ip" :
{
"action": "create",
"value": "10.2.3.0"
}
}
}
```

ACL Profile

Table 22: *ACL Profile Configuration*

API	JSON_Payload	Parameters

/rest/acl-rules	`{`
	`"acl-config" :`
	
	`{`
	`"action": "string",`
	`"acl_name": "string",`
	`"bandwidth_limit":`
	`{`
	`"upstream" :`
	`{`
	`"action": "string",`
	`"per-user": "string",`
	`"limit": integer`
	`},`
	`"downstream" : {`
	`"action": "string",`
	`"per-user": "string",`
	`"limit": integer`
	`}`
	`},`
	`"captive-portal":`
	`{`
	`"action": "string",`
	`"type": "string",`
	`"external_profile_name": "string"`
	`},`
	`"vlan-info":`
	`{`
	`"set" : "string",`
	`"vlan" : "string"`
	`},`
	`"rules" : [`
	`{`
		action—This is a mandatory configuration parameter. Enter one of the following values:
		■ create—configure an ACL profile
		■ delete—delete ACL profile configuration
		acl_name—Enter a name for the ACL rule.
		bandwidth_limit—Assign bandwidth contracts to user roles.
		■ **upstream**—Configures the upstream bandwidth contract.
		● **action**—Enter one of the following values:
		● create—add upstream bandwidth contract
		● delete—delete upstream bandwidth contract
		● **per-user**—Assign a upstream bandwidth limit for each user between 1–65535 Kbps.
		■ **downstream**—Configures the downstream bandwidth contract.
		● **action**—Enter one of the following values:
		● create—add downstream bandwidth contract
		● delete—delete downstream bandwidth contract
		● **per-user**—Assign a downstream bandwidth limit for each user between 1–65535 Kbps.

Table 22: *ACL Profile Configuration*

API	JSON_Payload	Parameters

	<pre>"action" : "string",
	"service-type" : "string",
	"protocol-info" : {
	"protocol": "string",
	"sport" : "string",
	"dport" : "string"
	},
	"destination-type" : "string",
	"rule-action" : "string"
	"options" : {
	"log": string,
	"blacklist": string,
	"disable-scanning": string
	}
	},
	]
	}
	}</pre>
		captive-portal—Configures a captive-portal role, to assign to the users role after a successful authentication.
		■ **action**—Enter one of the following values:
		● create—add captive portal role
		● delete—delete captive portal role
		■ **type**—Select **internal** or **external**
		■ **external_profile_name**—Choose **default** if you want to use the default external-cp-profile
		vlan-info—Configures a VLAN in the derivation role.
		■ **set**—Enter **Yes** to set a VLAN.
		■ **vlan**—Enter a VLAN name or a VLAN ID.
		rules—Creates an access rule. You can create up to 128 ACEs in an ACL for a user role. However, it is recommended to delete any existing configuration and apply changes at regular intervals.
		■ **action**—Enter one of the following values:
		● create—add an ACL rule
		● delete—delete ACL rule
		■ **service-type**—Enter a service type.
		■ **protocol-info**—Configures a protocol for the ACL rule.
		● **protocol**—Enter one of the following:
		● A protocol number between 0-255.
		● any—any protocol
		● tcp—transmission control protocol
		● udp—User Datagram Protocol
		■ **sport**—This parameter specifies the starting port number from which the rule applies. Enter an integer value between 1–65534.
		■ **dport**—This parameter specifies the ending port number until which the rule applies. Enter an integer value between 1–65534.
		■ **destination-type**—Enter one of the following values for the destination type:
		● all-destinations
		● to-a-server
		● except-to-a-server
		● to-a-network
		● except-to-a-network
		● to-a-domain

Table 22: *ACL Profile Configuration*

API	JSON_Payload	Parameters
		NOTE: When destination-type is set to any of the above values except for all-destinations, view the mandatory destination-info to be entered in below sample configuration. **rule-action**—Specify **permit** or **deny** **options**—Allows you to specify up to 10 options for network ACLs and up to 12 options for DPI ACLs. You can configure any of the following options: ■ **log**—Type **enable**. This creates a log entry when this rule is triggered. ■ **blacklist**—Type **enable**. This blacklists the client when this rule is triggered. ■ **disable-scanning**—Type **enable**. This disables ARM scanning when this rule is triggered.

Syntax

The following is an example for a curl call to configure or modify access-rules on an Instant AP:

```
curl "https://172.68.104.253:4343/rest/acl-rules?sid=oa8xnOcAsz2dqGywrt6B" -H "Content-Type: application/json"  --data @acl_json_file -insecure
```

The following is an example for curl call to configure/modify access-rules on Instant AP

```
curl "https://172.68.104.253:4343/rest/acl-rules?sid=oa8xnOcAsz2dqGywrt6B" -H "Content-Type: application/json"  --data @acl_json_file -insecure
```

Sample Configuration

Below is a sample (acl_json_file) to configure an acl-profile on an Instant AP:

```
{
"acl-config" : {
"action": "create",
"acl_name": "test1234",
"bandwidth_limit": {
"upstream" : {
"action": "enable",
"per-user": "yes",
"limit": 20
},
"downstream" : {
"action": "enable",
"per-user": "no",
"limit": 30
}
},
"captive-portal": {
"action": "enable",
"type": "external",
"external_profile_name": "abcdefgh"
},
"vlan-info": {
"set" : "yes",
"vlan" : "103"
},
"rules" : [
```

```
{
"action" : "create",
"service-type" : "protocol",
"protocol-info" : {
"protocol": "udp",
"sport" : "67",
"dport" : "68"
},
"destination-type" : "all-destinations",
"rule-action" : "permit"
},
]
}
}
```

Below is a sample configuration when the destination-type is set **to-a-server**:

```
destination-type" : "to-a-server",
"destination-info" :  {
                "ip-addr": "10.17.148.100"
                       }
```

Below is a sample configuration when the destination-type is set **to-a-network**:

```
"destination-type" : "to-a-network",
"destination-info" :  {
                "ip-addr": "10.17.148.100",
                "mask": "255.255.0.0"
                       },
```

Below is a sample configuration when the destination-type is set **to-a-domain**:

```
"destination-type" : "to-a-domain",
"destination-info" :  {
                "domain-name": "mydomain.com"
                       }
```

External Captive Portal

Table 23: *External Captive Portal Configuration*

API	JSON_Payload	Parameters
/rest/ext-captive-portal-profile	{ "external_captive_portal_profile_info" : { "action": "string", "name": "string", "auto-whitelist-disable": "string", "https": "string", "prevent-frame-overlay" : "string", "server-fail-through": "string", "server-offload": "string", "switch-ip": "string", "redirect-url": { "action": "string", "value": "string" }, "out-of-service-page": { "action": "string", "value": "string" },	**action**—This is a mandatory configuration parameter. Enter one of the following values: ■ create—add external captive profile configuration ■ delete—delete the external captive portal profile configuration **name**—This is a mandatory configuration parameter. Specify a name for the external captive portal profile. To use the default captive portal profile, specify **default**. **auto-whitelist-disable**—Select **enable** or **disable** **https**—Select **enable** or **disable** **prevent-frame-overlay**—Select **enable** or **disable** **server-fail-through**—Select **enable** or **disable** **server-offload**—Select **enable** or **disable**

Table 23: *External Captive Portal Configuration*

API	JSON_Payload	Parameters

	`"url": "string",`
	`"server": "string",`
	`"auth-text": "string",`
	`"port": integer`
	`}`
		switch-ip—Select **enable** or **disable**
		redirect-url—Configures a URL to redirect the users after a successful authentication.
		
		NOTE: By default, after entering the requested info at the splash page, the users are redirected to the URL that was originally requested. When a URL is configured for redirection, it overrides the user's original request and redirects them to URL configured for redirection.
		
		■ **action**—This is a mandatory configuration parameter. Enter one of the following values:
		● create—add redirect-url configuration
		● delete—delete the redirect-url configuration
		out-of-service-page—Configures a URL to redirect the users when the internet uplink is down.
		■ **action**—This is a mandatory configuration parameter. Enter one of the following values:
		● create—add out-of-service-page configuration
		● delete—delete the out-of-service-page configuration
		■ **value**—Enter the URL.
		url—Configure the URL of the external captive portal server.
		server—Specify the captive portal server
		auth-text—Configure the authentication text to be returned by the external server. The authentication text command configuration is required only for the External - Authentication Text splash mode.
		port—Specify the port to use for communication with the external captive portal server.

Syntax

The following is an example for a curl call to configure or modify an external-captive-portal profile on an Instant AP

```
curl "https://172.68.104.253:4343/rest/external-captive-portal-
profile?sid=oa8xnOcAsz2dqGywrt6B" -H "Content-Type: application/json"  --data @ecp_json_
file –insecure
```

Sample Configuration

Below is a sample configuration (ecp_json_file) to configure an external-captive-portal-profile on an Instant AP:

```
{
```

```
"external_captive_portal_profile_info" :
{
"action": "create",
"name": "default",
"auto-whitelist-disable": "enable",
"https": "enable",
"server-fail-through": "enable",
"server-offload": "enable",
"switch-ip": "disable",
"redirect-url": {
"action": "create",
"value":
"http://sjmlisboa.sharpmotion.com.hk/wifi/?v=205&vr=eae27d77ca20db309e056e3d2dcd7d69d1c48
0f2398e0b606b882bfc361566fb"
},
"out-of-service-page":{
"action": "create",
"value": "<a href='http://www.163.com'>163.com</a> "
},
"url" : "/aruba.php",
"server": "localhost",
"auth-text": "Authenticated",
"port": 80
}
}
```

IDS

Table 24: *IDS Configuration*

API	JSON_Payload	Parameters

/rest/ids	`{`
	`"ids-config" :`
	`{`
	`"action": "string",`
	`"infrastructure-detection":`
	`{`
	`"level": "string",`
	`"custom-policies" :`
	`{`
	`"detect-ap-spoofing" : "string",`
	`"detect-windows-bridge" : "string",`
	`"signature-deauth-broadcast" : "string",`
	`"signature-deassociation-broadcast" : "string",`
	`"detect-chan-based-mitm" : "string",`
	`"detect-adhoc-using-valid-ssid" : "string",`
	`"detect-malformed-large-duration" : "string",`
	`"detect-ap-impersonation" : "string",`
	`"detect-adhoc-network" : "string",`
	`"detect-valid-ssid-misuse" : "string"`
	`"detect-wireless-bridge" : "string",`
	`"detect-ht-40mhz-intolerance" : "string",`
	`"detect-ht-greenfield" : "string",`
	`"detect-ap-flood" : "string",`
	`"detect-client-flood" : "string",`
	`"detect-bad-wep" : "string",`
	`"detect-cts-rate-anomaly" : "string",`
	`"detect-rts-rate-anomaly" : "string",`
	`"detect-invalid-addresscombination" : "string",`
		action—This is a mandatory configuration parameter. Enter one of the following values:
		■ enable—enables IDS policy on the Instant AP
		■ Disable—disables IDS policy on the Instant AP
		■ **level**—This is a mandatory configuration parameter. Enter the client detection level type:
		● off
		● low
		● medium
		● high
		● custom
		detect-ap-spoofing—Select **enable** or **disable**
		detect-windows-bridge—Select **enable** or **disable**
		signature-deauth-broadcast—Select **enable** or **disable**

Table 24: *IDS Configuration*

API	JSON_Payload	Parameters

	<pre>"detect-malformed-htie" : "string",
	"detect-malformed-assoc-req" : "string",
	"detect-malformed-frame-auth" : "string",
	"detect-overflow-ie" : "string",
	"detect-overflow-eapol-key" : "string",
	"detect-beacon-wrong-channel" : "string",
	"detect-invalid-mac-oui": "string"
	}
	},
	"client-detection":
	{
	"level": "string",
	"custom-policies" :
	"detect-valid-clientmisassociation" : "string",
	"detect-disconnect-sta" : "string",
	"detect-omerta-attack" : "string",
	"detect-fatajack" : "string",
	"detect-block-ack-attack" : "string",
	"detect-hotspotter-attack" : "string",
	"detect-unencrypted-valid" : "string",
	"detect-power-save-dos-attack" : "string",
	"detect-eap-rate-anomaly" : "string",
	"detect-rate-anomalies" : "string",
	"detect-chopchop-attack" : "string"
	"detect-tkip-replay-attack" : "string",
	"signature-airjack" : "string",
	"signature-asleap" : "string",
	"detect-wpa-ft-attack": "string"
	}
	},
	"infrastructure-protection":
	{
	"level": "string",
	"custom-policies" :
	{
	"protect-ssid" : "string",
	"rogue-containment" : "string",
	"protect-adhoc-network" : "string",
	"protect-ap-impersonation" : "string"
	}
	},
	"client-protection":
	{
	"level": "string",
	"custom-policies" :
	{
	"protect-valid-sta": "string",
	"protect-windows-bridge": "string"
	}
	},
	"wired-containment": "string",
	"wired-containment-ap-adj-mac": "string",
	"wired-containment-susp-l3-rogue": "string",
	"wireless-containment": "string"
	}</pre>
		signature-deassociation-broadcast—Select **enable** or **disable**
		detect-chan-based-mitm—Select **enable** or **disable**
		detect-adhoc-using-valid-ssid—Select **enable** or **disable**
		detect-malformed-large-duration—Select **enable** or **disable**
		detect-ap-impersonation—Select **enable** or **disable**
		detect-adhoc-network—Select **enable** or **disable**
		detect-valid-ssid-misuse—Select **enable** or **disable**
		detect-ht-40mhz-intolerance—Select **enable** or **disable**
		detect-ht-greenfield—Select **enable** or **disable**
		detect-ap-flood—Select **enable** or **disable**
		detect-client-flood—Select **enable** or **disable**
		detect-bad-wep—Select **enable** or **disable**
		detect-cts-rate-anomaly—Select **enable** or **disable**
		detect-rts-rate-anomaly—Select **enable** or **disable**
		detect-invalid-addresscombination—Select **enable** or **disable**
		detect-malformed-htie—Select **enable** or **disable**
		detect-malformed-assoc-req—Select **enable** or **disable**
		detect-malformed-frame-auth—Select **enable** or **disable**
		detect-overflow-ie—Select **enable** or **disable**
		detect-overflow-eapol-key—Select **enable** or **disable**
		detect-beacon-wrong-channel—Select **enable** or **disable**
		detect-invalid-mac-oui—Select **enable** or **disable**

Table 24: *IDS Configuration*

API	JSON_Payload	Parameters
	<pre>}</pre>	**detect-valid-clientmisassociation**—Select **enable** or **disable** **detect-disconnect-sta**—Select **enable** or **disable** **detect-omerta-attack**—Select **enable** or **disable** **detect-fatajack**—Select **enable** or **disable** **detect-block-ack-attack**—Select **enable** or **disable** **detect-hotspotter-attack**—Select **enable** or **disable** **detect-unencrypted-valid**—Select **enable** or **disable** **detect-power-save-dos-attack**—Select **enable** or **disable** **detect-eap-rate-anomaly**—Select **enable** or **disable** **detect-rate-anomalies**—Select **enable** or **disable** **detect-chopchop-attack**—Select **enable** or **disable** **detect-tkip-replay-attack**—Select **enable** or **disable** **signature-airjack**—Select **enable** or **disable** **signature-asleap**—Select **enable** or **disable** **detect-wpa-ft-attack**—Select **enable** or **disable** **infrastructure-protection**—Sets the infrastructure protection level. ■ **level**—This is a mandatory configuration parameter. Enter the client detection level type: ● off ● low ● high ● custom **protect-ssid**—Select **enable** or **disable**

Table 24: *IDS Configuration*

API	JSON_Payload	Parameters
		rogue-containment—Select **enable** or **disable** **protect-adhoc-network**—Select **enable** or **disable** **protect-ap-impersonation**—Select **enable** or **disable** **client-protection**—Sets the client protection level. ■ **level**—This is a mandatory configuration parameter. Enter the client detection level type: ● off ● low ● high ● custom **protect-valid-sta**—Select **enable** or **disable** **protect-windows-bridge**—Select **enable** or **disable** **wired-containment**—Select **enable** or **disable** **wired-containment-ap-adj-mac**—Select **enable** or **disable** **wired-containment-susp-l3-rogue**—Select **enable** or **disable** **wireless-containment**—Enter one of the following values: ■ none ■ deauth-only ■ tarpit-all-sta ■ tarpit-non-valid-sta

Syntax

The following is an example for a curl call to configure or modify ids on an Instant AP :

```
curl "https://172.68.104.253:4343/rest/ids?sid=Gmr6BQ9QW7qAaMWw0kbT" -H "Content-Type:
application/json"  --data @ids_json_file -insecure
```

Sample Configuration

Below is a sample configuration (ids_json_file) to configure ids on an Instant AP:

```
{
"ids-config" :
{
"action": "enable",
"infrastructure-detection":
{
"level": "custom",
"custom-policies" :
```

```
{
"detect-ap-spoofing" : "enable",
"detect-windows-bridge" : "enable",
"signature-deauth-broadcast" : "enable",
"signature-deassociation-broadcast" : "enable",
"detect-chan-based-mitm" : "enable",
"detect-adhoc-using-valid-ssid" : "enable",
"detect-malformed-large-duration" : "enable",
"detect-ap-impersonation" : "enable",
"detect-adhoc-network" : "enable",
"detect-valid-ssid-misuse" : "enable",
"detect-wireless-bridge" : "enable",
"detect-ht-40mhz-intolerance" : "enable",
"detect-ht-greenfield" : "enable",
"detect-ap-flood" : "enable",
"detect-client-flood" : "enable",
"detect-bad-wep" : "enable",
"detect-cts-rate-anomaly" : "enable",
"detect-rts-rate-anomaly" : "enable",
"detect-invalid-addresscombination" : "enable",
"detect-malformed-htie" : "enable",
"detect-malformed-assoc-req" : "enable",
"detect-malformed-frame-auth" : "enable",
"detect-overflow-ie" : "enable",
"detect-overflow-eapol-key" : "enable",
"detect-beacon-wrong-channel" : "enable",
"detect-invalid-mac-oui": "enable"
}
},
"client-detection": {
"level": "custom",
"custom-policies" :
{
"detect-valid-clientmisassociation" : "disable",
"detect-disconnect-sta" : "disable",
"detect-omerta-attack" : "disable",
"detect-fatajack" : "disable",
"detect-block-ack-attack" : "disable",
"detect-hotspotter-attack" : "disable",
"detect-unencrypted-valid" : "disable",
"detect-power-save-dos-attack" : "disable",
"detect-eap-rate-anomaly" : "disable",
"detect-rate-anomalies" : "disable",
"detect-chopchop-attack" : "disable",
"detect-tkip-replay-attack" : "disable",
"signature-airjack" : "disable",
"signature-asleap" : "disable",
"detect-wpa-ft-attack": "disable"
}
},
"infrastructure-protection": {
"level": "custom",
"custom-policies" :
{
"protect-ssid" : "disable",
"rogue-containment" : "disable",
"protect-adhoc-network" : "disable",
"protect-ap-impersonation" : "disable"
}
},
"client-protection": {
```

```
"level": "custom",
"custom-policies" :
{
"protect-valid-sta": "disable",
"protect-windows-bridge": "disable"
}
},
"wired-containment": "disable",
"wired-containment-ap-adj-mac": "disable",
"wired-containment-susp-l3-rogue": "disable",
"wireless-containment": "deauth-only"
}
}
```

Software Upgrade

Table 25: *Software Upgrade Configuration*

API	JSON_Payload	Parameters

/rest/os-upgrade	`{`
	`"upgrade-info" :`
	`{`
	`"auto-reboot": true`
	`"Centaurus-url": "string"`
	`"Lupus-url": "string"`
	`"Gemini-url": "string"`
	`"Hercules-url": "string"`
	`"Vela-url": "string"`
	`"Draco-url": "string"`
	`"Ursa-url": "string"`
	`"Aries-url": "string"`
	`"Scorpio-url": "string"`
	`}`
	`}`
		auto-reboot—This is a mandatory configuration parameter. **auto-reboot**—Choose one of the following values:
		■ yes—enables auto reboot
		■ no—disables auto reboot
		Centaurus-url—enter the upgrade URL.
		Lupus-url—enter the upgrade URL.
		Gemini-url—enter the upgrade URL.
		Hercules-url—enter the upgrade URL.
		Vela-url—enter the upgrade URL.
		Draco-url—enter the upgrade URL.
		Ursa-url—enter the upgrade URL.
		Aries-url—enter the upgrade URL.
		Scorpio-url—enter the upgrade URL.

Syntax

The following is an example for a curl call to upgrade image on a master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/os-upgrade?sid=UUDJwDsNjrNRgmTvCeiy" -H "Content-Type: application/json"  --data @upgrade_json_file --insecure
```

Sample Configuration

Below is sample configuration (upgrade_json_file) to upgrade an image on a multi-class Instant AP cluster:

```
{
"upgrade-info" :
{
"auto-reboot": "yes",
"Centaurus-url": "ftp://10.1.1.41/ArubaInstant_Centaurus_8.8.0.0_79697",
"Hercules-url": "ftp://10.1.1.41/ArubaInstant_Hercules_8.8.0.0_79697",
"Gemini-url": "http://192.168.3.102/ArubaInstant_Gemini_8.8.0.0_79697"
}
}
```

Time Zone

Table 26: *Time Zone Configuration*

API	JSON_Payload	Parameters

/rest/clock	{
	"clock_info" :
	{
	"timezone" :
	{
	"action" : "string"
	"name" : "string"
	"hour_offset" : integer
	"minute_offset" : integer
	}
	}
	}
		action—Enter one of the following values:
		■ create—add time zone configuration
		■ delete—delete time zone configuration
		name—Specify a name for the timezone configuration
		hour_offset—Specify the hours offset from the UTC.
		minute_offset—Specify the minutes offset from the UTC.

Syntax

The following is an example for a curl call to configure or modify the timezone on a master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/clock?sid=UUDJwDsNjrNRgmTvCeiy" -H "Content-Type:
application/json"  --data @tz_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (tz_add_json_file) to configure a timezone on the Instant AP:

```
{
"clock_info" :
{
"timezone" :
{
"action" : "create",
"name" : "Coordinated-Universal-Time"
"hour_offset" : 0
"minute_offset" : 0
}
}
}
```

AP Reboot

Table 27: *AP Reboot Configuration*

API	JSON_Payload	Parameters

/rest/reboot	{
	"iap_ip_addr": "string",
	"reboot-info" :
	{
	"target": "string"
	}
	}
		iap-ip-addr—Denotes the IP address of the Instant AP to be rebooted.
		target—Enter one of the following values:
		■ single—reboots a single Instant AP.
		■ all—Reboots all the Instant APs in the cluster.

Syntax

The following is an example for a curl call to reboot the master, slave, standalone Instant AP or all Instant APs in cluster mode:

```
curl "https://172.68.104.253:4343/rest/reboot?sid=UUDJwDsNjrNRgmTvCeiy" -H "Content-Type:
application/json"  --data @reboot_json_file --insecure
```

Sample Configuration

Below is a sample configuration (reboot_json_file) to reboot all Instant APs in cluster:

```
{
"iap_ip_addr": "172.68.104.253",
"reboot-info" :
{
"target": "single"
}
}
```

Below is a sample configuration (reboot_json_file) to reboot a slave Instant AP in the cluster:

```
{
"iap_ip_addr": "172.68.104.252",
"reboot-info" :
{
"target": "single"
}
}
```

Wired Port Profile

Table 28: *Wired Port Profile Configuration*

API	JSON_Payload	Parameters
/rest/wired-port-profile	{ "wired-port-profile" : { "profile-name" : "string", "action" : "string", "access-rule-name" : "string", <name> "allowed-vlan" : { "action" : "string", "value" : "string" <vlan> } "captive-portal": { "external" : "string", "profile" : "string", "profile_name" : "string", "exclude-uplink" : "string", "exclude-uplink-types" : "string", "captive-portal-type" : "string" }, "native-vlan" : "string", "poe" : "string", "speed" : "string", <speed> "switchport-mode" : "string", <mode> "trusted" : "string", "type" : "string", "uplink-enable" : "string", "mac-authentication" : "string", "shutdown" : "string", "dot1x" : "string", "duplex" : "string" "auth-server" : { "action" : "string",	**profile-name**—This is a mandatory configuration parameter. Enter a profile name for the wired port profile. **action**—This is a mandatory configuration parameter. Enter one of the following values: ■ create—add the wired-port-profile configuration ■ delete—delete the wired-port-profile configuration **access-rule-name**—Enter the access rule to which the wired-port-profile is to be mapped to. allowed-vlan—Configures a list of allowed VLANs. The Allowed VLAN refers to the VLANs carried by the port in Access mode. ■ **action**— Enter one of the following values: ● create—add the access-rule name ● delete—delete the access-rule name ■ value—Configure the list of comma separated digits or ranges **1,2,5** or **1-4,** or **all**. **captive-portal**—Enables internal or external captive portal authentication for the wired profile users. Configure the following values: ■ **external**—Select **Yes** ■ **profile**—Select **Yes** ■ **profile_name**—Enter a profile name for the captive

Table 28: *Wired Port Profile Configuration*

API	JSON_Payload	Parameters
	"value" : "string" <name> } } }	portal profile ■ **exclude-uplink**—Select **Yes** ■ **exclude-uplink-types**—Enter the type of uplink to be excluded ■ **captive-portal-type**—Enter the type. **native-vlan**—Enter a string value for the VLAN ID. **poe**—Select **enable** or **disable**. **speed**—Assign a speed value (10, 100, 200, auto). switchport-mode—switchport mode for the wired profile. You can specify any of the following modes ■ **Access**— Use this mode to allow the port to carry a single VLAN specified as the native VLAN. ■ **Trunk**—Use this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs. **trusted**—Select **enable** or **disable**. **type**—Select **employee** or guest **uplink-enable**—Select **enable** or **disable**. **mac-authentication**—Select **enable** or **disable**. **shutdown**—Select **enable** or **disable**. **dot1x**—Select **enable** or **disable**. **duplex**—Select any one of these (**full**, **half**, or **auto**). **auth-server**—Configures the authentication server for the wired profile. ■ **action**— Enter one of the following values: ● create—add the auth-server ● delete—delete the auth-server configuration ■ **value**—Configure the auth-server name.

Syntax

The following is an example for a curl call to configure or modify the wired-port-profile on the master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/wired-port-profile?sid=UUDJwDsNjrNRgmTvCeiy" -H
"Content-Type: application/json"  --data @wired_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (wired_add_json_file) to configure wired-port mode to access and enable uplink on Instant AP:

```
{
"wired-port-profile" :
{
"profile-name" : "wired12345678",
"action" : "create",
"switchport-mode" : "access",
"native-vlan" : "guest",
"type" : "guest",
"shutdown" : "disable",
"uplink-enable" : "enable",
"captive-portal":
{
"external" : "yes",
"profile" : "yes",
"profile_name" : "abcdefgh",
"exclude-uplink" : "yes",
"exclude-uplink-types" : "Ethernet"
}
}
}
```

Below is a sample configuration (wired_add_json_file) to configure wired-port mode to trunk and enable dot1x on Instant AP:

```
{
"wired-port-profile" : {
"profile-name" : "abcdefg",
"action" : "create",
"allowed-vlan" : {
"action" : "create",
"value" : "100,110,111,112,113,114,115,116"
},
"shutdown" : "disable",
"dot1x" : "enable",
"duplex" : "auto",
"auth-server" : {
"action" : "create",
"value" : "auth_server1234"
}
}
}
```

Wired Profile Map

Table 29: *Wired Profile Map Configuration*

API	JSON_Payload	Parameters
/rest/wired-profile-map	{ "wired-profile-map" : { "enet0-port-profile" : "string", "enet1-port-profile" : { "action" : "string", "value" : "string" }, "enet2-port-profile" : {	**enet0-port-profile**—Specify a name for the enet0 port profile **enet1-port-profile**-Configures the enet1 port profile. ■ **action**—This is a mandatory configuration parameter. Enter one of the following values: ● create—configures a enet1 port profile. ● delete—deletes the enet1 port profile configuration,

Table 29: *Wired Profile Map Configuration*

API	JSON_Payload	Parameters

	<pre>"action" : "string",
	"value" : "string"
	},
	"enet3-port-profile" :
	{
	"action" : "string",
	"value" : "string"
	},
	"enet4-port-profile" :
	{
	"action" : "string",
	"value" : "string"
	}
	}
	}</pre>
		■ **value**—Enter the wired port profile name to associate with enet1.
		enet2-port-profile—Configures the enet2 port profile.
		■ **action**—This is a mandatory configuration parameter. Enter one of the following values:
		● create—configures a enet2 port profile.
		● delete—deletes the enet2 port profile configuration,
		■ **value**—Enter the wired port profile name to associate with enet2.
		enet3-port-profile—Configures the enet3 port profile.
		■ **action**—This is a mandatory configuration parameter. Enter one of the following values:
		● create—configures a enet3 port profile.
		● delete—deletes the enet3 port profile configuration,
		■ **value**—Enter the wired port profile name to associate with enet3.
		enet4-port-profile—Configures the enet4 port profile.
		■ **action**—This is a mandatory configuration parameter. Enter one of the following values:
		● create—configures a enet4 port profile.
		● delete—deletes the enet4 port profile configuration,
		■ **value**—Enter the wired port profile name to associate with enet4.

Syntax

The following is an example for a curl call to configure or modify the wired-profile-map on a master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/wired-profile-map?sid=UUDJwDsNjrNRgmTvCeiy" -H
"Content-Type: application/json"  --data @wired_prof_map_add_json_file --insecure
```

Sample Configuration

Below is a sample configuration (wired_prof_map_add_json_file) to configure wired-porifle-map on an Instant AP:

```
{
"wired-profile-map" : {
"enet0-port-profile" : {
"action" : "create",
"value" : "wired123"
}
}
}
```

Management User

Table 30: *Management User Configuration*

API	JSON_Payload	Parameters

/rest/mgmt-user	{
	"mgmt-user" :
	{
	"action" : "string",
	"username" : "string",
	"cleartext_password" : "string",
	"usertype" : "string",
	"hash_password" : "string",
	"read-only" : "string",
	"guest-mgmt" : "string",
	"local" : "string"
	}
	}
		mgmt-user—Configures administrator credentials.
		■ **action**—This is a mandatory configuration parameter. Enter one of the following values:
		● create—Add management user configuration
		● delete—delete management user configuration
		■ **username**—Enter the username.
		■ **cleartext_password**—Enter the password. cleartext Indicates if a user will enable clear text as the password input format.
		■ **usertype**—Enter the type of the user (**read-only**, **guest-mgmt**, or **local**).
		■ **hash_password**—Enter the password in hash format.
		■ **read-only**—**Yes** is the only valid input and should be specified only when action is to delete the read-only user.
		■ **guest-mgmt**—**Yes** is the only valid input and should be specified only when action is to delete the guest-mgmt user.
		■ **local**—**Yes** is the only valid input and should be specified only when action is to delete the local user.
		
		NOTE: read-only, guest-mgmt, and local parameters are to be specified in case of action being **delete** only.

Syntax

The following is an example for a curl call to configure or modify the mgmt-user settings on a master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/mgmt-user?sid=29pUMtJzz3FnN60Xuxj2" -H "Content-Type: application/json"  --data @user_cfg_add_json -insecure
```

The following is an example for a curl call to delete the mgmt-user settings on a master or standalone Instant AP:

```
curl "https://172.68.104.253:4343/rest/mgmt-user?sid=29pUMtJzz3FnN60Xuxj2" -H "Content-Type: application/json"  --data @user_cfg_del_json -insecure
```

Sample Configuration

Below is a sample (use_cfg_add_json_file) to configure guest mgmt-user on an Instant AP:

```
{
"mgmt-user" : {
"action" : "create",
"username" : "abcdefg",
```

```
"hash_password" :
"5e5762aa023236f391f7c47f540948b80212f3b8feb1e832e79e377e248ba4b220fba89d14",
"usertype" : "guest-mgmt"
}
}
```

Below is a sample to delete the guest mgmt-user configuration on an Instant AP:

```
{
"mgmt-user" : {
"action" : "delete",
"guest-mgmt" : "yes"
}
}
```

Below is a sample (use_cfg_add_json_file) to configure read only mgmt-user on an Instant AP:

```
{
"mgmt-user" : {
"action" : "create",
"username" : "abcdefg",
"cleartext_password" : "aruba23456",
"usertype" : "read-only"
}
}
```

Below is a sample to delete the read only mgmt-user configuration on an Instant AP:

```
{
"mgmt-user" : {
"action" : "delete",
"read-only" : "yes"
}
}
```

Below is a sample (use_cfg_add_json_file) to configure local mgmt-user on an Instant AP:

```
{
"mgmt-user" : {
"action" : "create",
"username" : "abcdefg",
"cleartext_password" : "aruba23456",
"usertype" : "local"
}
}
```

Below is a sample to delete the local mgmt-user configuration on an Instant AP:

```
{
"mgmt-user" : {
"action" : "delete",
"local" : "yes"
}
}
```

Monitoring API

Monitoring API is used to get the state, statistics, and logs from individual Instant APs, namely master, slave, or standalone Instant APs.

Ensure to prefix an escape character (\ ) when including - \n, \r, double quotes, or any other special characters – as part of JSON input parameter values.

Syntax

The following is a sample CURL command used to call monitoring APIs on a master Instant AP:

```
curl "https://<Master-IAP_ip>:4343/rest/show-cmd?iap_ip_addr=<Master-IAP_ip_
address>&cmd=<show_command>&sid=<sid>"  --insecure | sed 's/\\n/\n/g'
```

The following is a sample CURL command used to call monitoring APIs on a slave Instant AP:

```
curl "https://<Master/Standalone-IAP_ip>:4343/rest/show-cmd?iap_ip_addr=<SLAVE-IAP_ip_
address>&cmd=<show_command>&sid=<sid>"  --insecure | sed 's/\\n/\n/g'
```

The following is a sample CURL command used to call monitoring APIs on a standalone Instant AP:

```
curl "https://<Standalone-IAP_ip>:4343/rest/show-cmd?iap_ip_addr=<Standalone-IAP_ip_
address>&cmd=<show_command>&sid=<sid>"  --insecure | sed 's/\\n/\n/g'
```

Table 31: *Login Command Parameters*

Parameters	Description
<username>	Username of the user.
<password>	Password of the user.
<show_command>	The API syntax of the show commands. Refer to API Syntax.
<sid>	A unique string that the server generates and returns to the user when a login authentication is successful. User has to include this SID in all API calls of this session. It is valid until the user explicitly logs out, or, until the inactivity timeout expires.
<Master-iap-ip>	IPv4 address of the master Instant AP.
<Standalone-iap-ip>	IPv4 address of the standalone Instant AP.

The monitoring API takes the Instant show commands as its input. However, when using a show command in the monitoring API, user has to replace spaces with "%20".

For Example :

- For CLI command **show aps** corresponding REST-API command is **show%20aps**.
- For CLI command **show stats ap 2.3.4.5** corresponding REST-API command is **show%20stats%20ap%202.3.4.5**.

The following show commands are currently supported through the REST API. For a detailed description of these commands and their usage guidelines, see the *Aruba Instant CLI Reference Guide*.

Table 32: *Supported List of Show Commands*

CLI Syntax	API Syntax
show clients	show%20clients
show aps	show%20aps
show running-config	show%20running-config
show stats ap <IP-address>	show%20stats%20ap%20<IP-address>
show version	show%20version
show summary	show%20summary
show wired-port-settings	show%20wired-port-settings
show port status	show%20port%20status

Table 32: *Supported List of Show Commands*

CLI Syntax	API Syntax
show network	show%20network
show client debug	show%20client%20debug
show network <name>	show%20network%20<name>
show ap-env	show%20ap-env
show log iap-bootup	show%20log%20iap-bootup
show client status <mac>	show%20client%20status%20<mac>

Sample Configuration

The following is an example for a curl call to execute the command **show aps** on a master Instant AP:

```
curl "https://172.68.104.253:4343/rest/show-cmd?iap_ip_
addr=172.68.104.253&cmd=show%20aps&sid=cHvOFgLGyfATrKBJgQTh" -H "Content-Type:
application/json"  --insecure| sed 's/\\n/\n/g'
```

The following is the successful response to the above curl call:

```
{
"Status":       "Success",
"Status-code":  0,
"CLI Command executed": "show aps
",
"IAP IP address":       "172.68.104.253",
"Command output":       "cli output:
COMMAND=show aps
\r
2 Access Points
---------------
Name  IP Address      Mode    Spectrum  Clients  Type         IPv6 Address  Mesh Role
Zone  Serial #   radio0 Channel  radio0 Power (dB)  radio0 Utilization (%)  radio0 Noise
Floor (dBm)  radio1 Channel  radio1 Power (dB)  radio1 Utilization (%)  radio1 Noise
Floor (dBm)  Need Antenna Config  From Port  Config Id  Config Csum  Ext SSID Active
Link Local IP Address
----  ----------      ----    --------  -------  ----         ------------  ---------  --
--  --------   --------------  -----------------  ----------------------  ---------------
---------  --------------  -----------------  ----------------------  -------------------
-----  -------------------  ---------  ---------  -----------  ---------------  ---------
------------
a     172.68.104.253  access  disable   0        225(indoor)  --            N/A        -
   CT0841843  161             23                 20(good)               -96(good)
         6               23                64(ok)                  -96(good)
    No                   none       66         45054        enable           --
as    172.68.104.252  access  disable   0        225(indoor)  --            N/A        -
   CT0841902  -               -                  -                      -
         -               -                 -                       -
    No                   none       66         45054        enable           --"
}
```

The following is a failed response to an invalid show command:

```
$ curl "https://<master-ip>:4343/rest/show-cmd?iap_ip_addr=<iap-
ip>&cmd=show%20apsss&sid=KT27GmukHnyqGdrZzv7N"  --insecure
{
"Status":       "Failed",
"Status-code":  6,
"CLI Command executed": "show apsss\n",
"IAP IP address":       "<iap-ip>",
```

```
"Error message":        "cli output: \n\nCOMMAND=show apsss\n% Parse error.\n"
}
```

The following is a failed response to an invalid show command:

```
$ curl "https://<master-ip>:4343/rest/show-cmd?iap_ip_addr=<iap_
ip>&cmd=sssshow%20apsss&sid=KT27GmukHnyqGdrZzv7N"  --insecure
{
"Status":       "Failed",
"Status-code":  4,
"IAP IP address":       "<iap-ip>",
"Error message":        "Input parameter cmd is invalid"
}
```

The text in bold highlights the invalid syntax. Ensure to use the correct show command syntax in the curl commands.