

---

**CloudAxis :: Applications :: Rest API Document**  
**v. 1.7.0**  
**Project Documentation**

---



## Table Of Content

1. Table Of Content .....	i
2. Home .....	1
3. Contact Management .....	3
4. User Authentication .....	10
5. Conference Management .....	13
6. Participant Management .....	32
7. Social Connectors .....	39
8. Global Address Book (GAB) .....	43
9. VMR Management .....	46
10. One Time Token .....	48
11. SMTP and Server Settings .....	50
12. User Management .....	54
13. Role Management .....	63
14. LDAP Configuration .....	66
15. RP Core Service .....	69
16. Access Point Service .....	76
17. DMA Configuration Service .....	81
18. Policy Management .....	90
19. Certificate Management .....	94
20. Product Version Management .....	108
21. License Management .....	109
22. NTP Configuration Management .....	128
23. Logging Management .....	132
24. Conference Settings .....	136
25. Localization Management .....	139
26. Proxy Configuration .....	144
26. Template Customization .....	146
26. Single Sign-On (SSO) Configuration .....	154
26. White Label Configuration .....	161
26. Notification Message Configuration .....	168
26. Test Features Activation and Deactivation .....	170
26. SNMP Management .....	174



# 1 Home

---

## 1.1 CloudAXIS Web Services Portal API Specification Documentation Site

This site describes the Representational State Transfer (REST) APIs for CloudAxis WSP Platform.

The APIs provide software developers and system administrators with better control over their CloudAxis environment outside of the standard web interface. The REST APIs are useful for developers and administrators who aim to integrate the functionality of a CloudAxis environment with custom scripts or external applications that access the APIs via the standard Hypertext Transfer Protocol (HTTP).

### 1.1.1 The benefits of the REST APIs are:

**Broad client support** - Any programming language, framework, or system with support for HTTP protocol can use the APIs.

**Self descriptive** - Client applications require minimal knowledge of the infrastructure as many details are discovered at runtime.

**Resource-based model** - The resource-based REST model provides a natural way to manage a platform.

This site acts as a reference to the CloudAxis REST APIs. It aims to provide developers and administrators with instructions and examples to help harness the functionality of their CloudAxis environment through the REST APIs.

### 1.1.2 List of APIs:

Name of API	Brief Description
<a href="#">SMTP and Server Settings Configuration</a>	Provides steps to configure SMTP and Server settings
<a href="#">User Management</a>	Provides interfaces to create, retrieve, modify, delete and search user accounts
<a href="#">Role Management</a>	Provides interfaces to create, update, delete and list CloudAxis supported roles
<a href="#">Contact Management</a>	Provides interfaces to create, retrieve, modify and delete a user's contacts details
<a href="#">LDAP Configuration</a>	Provides interfaces to configure LDAP settings
<a href="#">User Authentication</a>	Provides interfaces to login/logout user and validate token
<a href="#">Conference Management</a>	Provides interfaces to create, retrieve, modify, join, cancel and end a conference
<a href="#">Participant Management</a>	Provides interfaces to add,remove and retrieve participant details for a conference
<a href="#">Rp Core Service</a>	Provides interfaces to store and retrieve core parameters (Like AD configuration)
<a href="#">Access Point Service</a>	Provides interfaces to create, retrieve, modify and delete access point details
<a href="#">DMA Configuration Service</a>	Provides interfaces to create, retrieve, modify and delete a DMA configuration from WSP

Policy Management	Provides interfaces to update and retrieve Social Connector Policies.
Certificate Management	Provides interfaces to implement Certificate Management operations like Certificate/CSR generation, Certificate list, upload Certificate etc.
Product Version Management	Provides interfaces to retrieve the product version number.
License Management	Provides interface for license management like Activate/Deactivate Licenses, Generate/Download/Delete Activation Requests and Configure System for MEA for product/(s) and feature/(s)
NTP Management	Provides interfaces to perform NTP related task
Logging Management	Provides interfaces to perform logging related task
One Time Token	Provides interfaces to generate One Time Token
Conference Settings	Provides interfaces to control the conference settings
Localization	Provides interfaces for Localization feature
Proxy Configuration	Provides interfaces for Proxy Configuration feature
Template Customization	Provides interfaces for customizing E-mail Templates
Social Connector Configuration	Provides interfaces to configure the social connectors
GAB listing	Provides interfaces to retrieve the social contacts
Single Sign-On (SSO) Configuration	Provides interfaces to configure SSO
White Label Configuration	Provides interfaces to configure white-labelling
VMR Management	Provides interfaces to manage personal VMR
Notification Message Configuration	Provides interfaces to configure notification message
Test Features Activation and Deactivation	Provides interfaces to activate & deactivate the test feature
SNMP Management	Provides interfaces to configure SNMP and Notification Agent

## 2 Contact Management

---

### 2.1 Contact Management

Provides API to perform CRUD operations for Contacts.

Contact resource stores the details of a users contacts.

#### Properties:

- *name*: Full name of the contact
- *providerUserId*: Unique identifier of the contact
- *providerId*: Source of the contact information
- *imageUrl*: Contact's image url if applicable.
- *profileUrl*: Contact's profile url if applicable.
- *firstName*: First name of contact
- *lastName*: Last name of contact
- *email*: Email address of contact
- *phoneNumber*: Phone number of contact
- *presenceStatus*: Presence status of the contact. Possible values are AVAILABLE, BUSY, AWAY, UNAVAILABLE, UNKNOWN.

**Mandatory Properties:** providerUserId, firstName, lastName, email

The supported REST APIs are:

#### 2.1.1 List all contacts

##### Roles allowed:

- ROLE\_ADMIN
- ROLE\_USER

##### Request:

```
GET: http://<WSP IP Address>/wsp/users/<username>/contacts
HEADER DETAILS:
X-CA-UserName: <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
X-CA-Token: <Auth token obtained after authentication>
Accept: application/vnd.com.polycom.cloudAxis.contactcollection+json
```

##### Query Parameters:

- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0

##### Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.contactcollection+json
{
  "contacts":[
    {
      "self":"http://<WSP IP Address>/users/<username>/contacts/1",
      "name":"Bob Mickey",
      "firstName":"Bob",
      "lastName":"Mickey",
      "providerUserId":"bob.mickey@xyz.com",
      "providerId":"LOCAL",
      "email":"bMickey@xyz.com",
      "phoneNumber":"+0123456789",
      "imageUrl":null,
      "profileUrl":null,
      "presenceStatus":"UNKNOWN"
    }
  ],
  "prev":null,
  "statistics":{
    "currentPage":0,
    "totalPages":1,
    "pageSize":1
  },
  "next":null,
  "self":"http://<WSP IP Address>/wsp/<username>/contacts?pageSize=5&currentPage=0"
}
```

**Status codes:**

- 200: Successful read
- 404: If user not found
- 500: Internal Server Error

**2.1.2 Create Contact****Roles allowed:**

- ROLE\_ADMIN
- ROLE\_USER

**Request:**



```

POST: http://<WSP IP Address>/wsp/users/jMickey/contacts
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.contact+json
    Content-type:       application/vnd.com.polycom.cloudAxis.contact+json

Body:
{
    "firstName": "Bob",
    "lastName": "Mickey",
    "providerUserId": "bob.mickey@xyz.com",
    "providerId": "LOCAL",
    "email": "bMickey@xyz.com",
    "phoneNumber": "+0123456789",
    "imageUrl": null,
    "profileUrl": null,
    "presenceStatus": "UNKNOWN"
}

```

**Response :**

```

HTTP/1.1 201 Created
Location: https://<WSP IP Address>/users/<username>/contacts/1
Content-Type: application/vnd.com.polycom.cloudAxis.contact+json
{
    "self": "http://<WSP IP Address>/users/<username>/contacts/1",
    "name": "Bob Mickey",
    "firstName": "Bob",
    "lastName": "Mickey",
    "providerUserId": "bob.mickey@xyz.com",
    "providerId": "LOCAL",
    "email": "bMickey@xyz.com",
    "phoneNumber": "+0123456789",
    "imageUrl": null,
    "profileUrl": null,
}

```

**Status codes:**

- 201: Successful contact creation
- 404: User not found
- 400: Invalid request
- 500: Internal server error

**2.1.3 Modify Contact****Roles allowed:**

- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```

PUT: http://<WSP IP Address>/wsp/users/jMickey/contacts/1
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.contact+json
Body:
{
    "firstName":"Bob",
    "lastName":"Mickey",
    "providerUserId":"bob.mickey@xyz.com",
    "providerId":"LOCAL",
    "email":"bMickey@xyz.com",
    "phoneNumber":"+0123456789",
    "imageUrl":null,
    "profileUrl":null,
    "presenceStatus":"UNKNOWN"
}

```

### Properties:

- *firstName*: First name of contact
- *lastName*: Last name of contact
- *email*: Email address of contact
- *phoneNumber*: Phone number of contact

### Response :

```
HTTP/1.1 204 No Content
```

### Status codes:

- 201: Successful contact creation
- 404: User not found
- 400: Invalid request
- 500: Internal server error

#### 2.1.4 Get Contact

##### Roles allowed:

- ROLE\_ADMIN
- ROLE\_USER

##### Request:

```

GET: http://<WSP IP Address>/wsp/users/<username>/contacts/1
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.contact+json

```

### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.contact+json
{
    "self": "http://<WSP IP Address>/users/<username>/contacts/1",
    "name": "Bob Mickey",
    "firstName": "Bob",
    "lastName": "Mickey",
    "providerUserId": "bob.mickey@xyz.com",
    "providerId": "LOCAL",
    "email": "bMickey@xyz.com",
    "phoneNumber": "+0123456789",
    "imageUrl": null,
    "profileUrl": null,
    "presenceStatus": "UNKNOWN"
}

```

**Status codes:**

- 200: Successful read
- 404: Username or contact does not exist
- 500: Internal Server Error

**2.1.5 Delete contact****Roles allowed:**

- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```

DELETE: http://<WSP IP Address>/wsp/users/<username>/contacts/1
HEADER DETAILS:
    X-CA-UserName          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token             <Auth token obtained after authentication>

```

**Response :**

```

HTTP/1.1 204 NO CONTENT

```

**Status codes:**

- 204: Successful delete
- 404: User or contact does not exist
- 500: Internal Server Error

**2.1.6 Import Contacts from CSV file****Roles allowed:**

- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```

POST: http://<WSP IP Address>/wsp/users/<username>/contacts/import

HEADER DETAILS:

    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.contactcollection+json
    Content-Type:       multipart/form-data

FORM PARAMETERS:

    file                <One CSV file of supported type>
    type                <gmail/yahoo/outlook/hotmail>

```

**Response :**

```

HTTP/1.1 200 OK

```

**Status codes:**

- 200: Successful read
- 500: Internal Server Error

**2.1.7 List frequent contacts for a user**

It returns Frequent Contact group with contacts

**Roles allowed:**

- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```

GET: http://<WSP IP Address>/wsp/contact-groups/Frequent%20Contact?type=name

HEADER DETAILS:

    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.contactgroup+json

```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.contactgroup+json
{
  "self": "https://wsp-dev-newflow.cloudax.is:443/wsp/contact-groups/402",
  "name": "Frequent Contact",
  "description": "Frequent Contact",
  "system": true,
  "id": 402,
  "contacts": [
    {
      "name": "1234",
      "providerUserId": "SP1Z8ZL56",
      "providerId": "LINKEDIN",
      "email": null,
      "firstName": "1234",
      "lastName": "1234",
      "imageUrl": "http://m.c.lnkd.licdn.com/mpr/mprx/0_JqFQX6X_i8KSX7xyjf94cLZIiEcgBfR",
      "presenceStatus": "UNKNOWN",
      "self": "http://<WSP IP Address>/wsp/contacts/SP1Z8ZL56"
    }
  ]
}
```

**Status codes:**

- 200: Successful read
- 404: If user not found
- 500: Internal Server Error

## 3 User Authentication

---

### 3.1 User Authentication

Provides APIs to perform User Login, User Logout and Token Validation:

#### Properties:

- *userName*: User may be an enterprise Active-Directory user or locally created Service-Portal user. In case of enterprise user, userName can be in either of the following 3 formats. In case of enterprise user, irrespective of what userName format is provided in the request, the response will always be in the corresponding UPN form of the user. After authentication is done, all subsequent API calls are required to send UPN format of the userName.
  - sAMAccountName (When default domain is not enabled): NETBIOSNAME \sam\_username
  - sAMAccountName (When default domain is enabled): sam\_username
  - userPrincipalName ie UPN: upn\_username@domain.com
- *password*: Password of the User's userName. The password of the user will not be sent back in the response for security reasons and it will be null.
- *tokenId*: The tokenId issued to the user. Token's length is of 64 characters.
- *displayName*: The display name of the logged-in user.
- *enabled*: User account's enabled status.
- *locked*: User account's locked status.
- *wspLicense*: WSP license status.
- *meaLicense*: MEA license status.
- *role*: The role assigned to the user.
- *changePassword*: Number of times the user's password is changed.

#### 3.1.1 User Login

User authentication and login API.

#### Request:

```
POST: http://<WSP IP Address>/wsp/auth/login
HEADER DETAILS:
    Accept: application/vnd.com.polycom.cloudaxis.userauth+json
    Content-type: application/vnd.com.polycom.cloudaxis.userauth+json
Body:
{
  "userName": "NETBIOSNAME\\sam_username",
  "password": "secret"
}
```

**Mandatory Properties:** userName, password

**Response :**

```

HTTP/1.1 200 OK - Authenticated
Content-Type: application/vnd.com.polycom.cloudaxis.userauth+json
{
  "userName": "upn_username@domain.com",
  "password": null,
  "tokenId": "63D1F5D9191E3CAC-558DB400-90517BF1-E09229AA-54E0BA70B7F85186FCA23E23",
  "displayName": "Display Name",
  "enabled": null,
  "locked": null,
  "meaLicense": "ACTIVATED",
  "wspLicense": "ACTIVATED",
  "role": {
    "self": "http://localhost:8080/wsp/roles/ROLE_SUPER_ADMIN",
    "name": "ROLE_SUPER_ADMIN"
  },
  "changePassword": "2"
}

```

### Status Codes:

- 200: OK - Authentication Successful
- 400: Bad Request
- 401: Unauthorized
- 500: Internal server error

### 3.1.2 Token Validation

Token validation API.

#### Request:

```

POST: http://<WSP IP Address>/wsp/auth/validate
HEADER DETAILS:
    Accept:          application/vnd.com.polycom.cloudaxis.userauth+json
    Content-type:    application/vnd.com.polycom.cloudaxis.userauth+json
Body:
{
  "userName": "upn_username@domain.com",
  "tokenId": "3D1F5D9191E3CAC-558DB400-90517BF1-E09229AA-54E0BA70B7F85186FCA23E23"
}

```

#### Properties:

- *userName*: User may be an enterprise Active-Directory user or locally created Service-Portal user. In case of enterprise user, userName must be in UPN format.
  - UPN format userName: upn\_username@domain.com
- *tokenId*: Token Id generated from user authentication API which is described above.

**Mandatory Properties:** userName, tokenId

#### Response :

```

HTTP/1.1 200 OK - Authenticated
Content-Type: application/vnd.com.polycom.cloudaxis.userauth+json
{
  "userName": "upn_username@domain.com",
  "password": null,
  "tokenId": "63D1F5D9191E3CAC-558DB400-90517BF1-E09229AA-54E0BA70B7F85186FCA23E23",
  "displayName": "Display Name",
  "enabled": null,
  "locked": null,
  "meaLicense": "ACTIVATED",
  "wspLicense": "ACTIVATED",
  "role": {
    "self": "http://localhost:8080/wsp/roles/ROLE_SUPER_ADMIN",
    "name": "ROLE_SUPER_ADMIN"
  },
  "changePassword": "2"
}

```

**Status Codes:**

- 200: OK - Authentication Successful
- 400: Bad request
- 401: Unauthorized
- 500: Internal server error

**3.1.3 User Logout**

User logout API.

**Request:**

```

POST: http://<WSP IP Address>/wsp/auth/logout
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain.com>
    X-CA-Token:         <tokenId obtained after authentication>

```

**Properties:**

- *userName*: User may be an enterprise Active-Directory user or locally created Service-Portal user. In case of enterprise user, userName must be in UPN format.
  - UPN format userName: upn\_username@domain.com
- *tokenId*: Token Id generated from user authentication API which is described above.

**Response :**

```

HTTP/1.1 200 OK - Successful

```

**Status Codes:**

- 200: OK - Logout Successful



## 4 Conference Management

### 4.1 Conference Management

Provides APIs to perform CRUD operations for Conference.

Conference resource is critical in storing the metadata for a conference in WSP.

The Conference status can have the below values:

ON_GOING	Meeting is in Progress.
FUTURE	Meeting is scheduled for a future date.
COMPLETED	Meeting has been completed.
CANCELLED	Meeting has been cancelled.

The Conference Type can have the below values:

AD_HOC	Ad Hoc Meeting
SCHEDULED	Scheduled meeting for future date.

**NOTE : At least 1 DMA needs to be configured before these API's can be used.**

#### Properties:

- *id*: Internal id for conference (Should not be passed for updation or creation)
- *presentedId*: User friendly id for conference (Should not be passed for updation or creation)
- *type*: The type of meeting is passed only during creation (see table above for more details). For ad-hoc meeting use 'AD\_HOC', for future meeting use 'SCHEDULED'.
- *status*: Should not be passed for updation or creation (see table above for more details).
- *authRequired*: Boolean value that specifies whether authentication is required for a meeting.
- *createdTime*: This is generated internally, should not be passed.
- *allowMultipleChairperson*: Boolean value that specifies whether meeting can have multiple chairperson. Default value is false.
- *sendMailInvite*: Boolean value to opt for sending meeting related mails.
- *vmrNumber*: This field is supplied if user wants to use personal VMR. Or else this should be null. Should not be supplied for updation. (Can be alphanumeric, DMA can in future use alphanumeric room numbers)
- *participantPasscode*: Passcode for Attendee. Can be alphanumeric.
- *hostPasscode*: Passcode for Host. Can be alphanumeric
- *name*: Name/Title for the Conference being scheduled
- *description*: Description of the meeting
- *startTime*: Start Time of the conference ( **Format**: YYYY-MM-DDTHH:MM:SS) (Please note the time zone is UTC) For an AD\_HOC meeting, this should be sent while scheduling a meeting.
- *endTime*: End Time of the conference
- *createdBy*: username of the person creating the conference. Should be supplied for creation and should not be supplied for updation.

- *recordingAllowed*: This is obtained from the conference template and indicates whether recording is allowed or not in the meeting.
- *userParticipants*: List of all the participants for the conference. An Active Directory user is added as "userName":"name\_of\_the\_user" while other participants are added as "userName":"mailId","email":"mailId"
- *dmaUsed*: Suggests the DMA used for this conference.
- *duration*: Duration of the meeting that is calculated internally.
- *createdByPersVmr*: Boolean flag which is true if meeting is created by using personal VMR. Default value is false.
- *participants*: List of all the participants for the conference. Refer to the below examples.

**Mandatory Properties:** type, name, startTime, endTime, createdBy

The supported REST APIs are:

#### 4.1.1 List all conferences

Lists all the conferences that have been setup.

##### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

##### Request:

```
GET: http://<WSP IP Address>/wsp/conferences
```

##### HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.portal.rest.ConferenceCollection+json

##### Query Parameters:

- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0

##### Response :

HTTP/1.1 200 OK

Content-Type: application/vnd.com.polycom.cloudaxis.portal.rest.conferencecollection+json

```
{
  "conferences": [
    {
      "self": "https://<WSP IP Address>/conferences/1687",
      "id": "1687",
      "presentedId": "JlmiNlLdi5",
      "name": "API doc review",
      "description": "Agenda",
      "startTime": "2015-01-14T07:30:00.000+0000",
      "participantPasscode": "1234",
      "hostPasscode": null,
      "recordingAllowed": false,
      "duration": null,
      "endTime": "2015-01-14T08:30:00.000+0000",
      "vmrNumber": "811054",
      "type": "SCHEDULED",
      "status": "FUTURE",
      "allowMultipleChairperson": false,
      "sendMailInvite": true,
      "createdBy": {
        "self": "https://<WSP IP Address>/wsp/users/sabhat@polycom.com",
        "userName": "sabhat@polycom.com",
        "id": "sabhat@polycom.com",
        "email": "sahana.bhat@polycom.com",
        "domain": null,
        "firstName": "Sahana",
        "lastName": "Bhat",
        "title": null,
        "department": null,
        "phoneNumber": null,
        "city": null,
        "enabled": true,
        "role": {
          "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
          "name": "ROLE_USER"
        }
      },
      "externalDirectory": true
    },
    {
      "createdTime": "2015-01-14T04:11:28.331+0000",
      "userParticipants": [
        {
          "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
          "userName": "sabhat@polycom.com",
          "id": "sabhat@polycom.com",
          "email": "sahana.bhat@polycom.com",
          "domain": null,
          "firstName": "Sahana",
          "lastName": "Bhat",
          "title": null,
          "department": null,
          "phoneNumber": null,
          "city": null,
          "enabled": true,
          "role": {
            "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
            "name": "ROLE_USER"
          }
        },
        {
          "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
          "name": "ROLE_USER"
        }
      ],
      "externalDirectory": true
    }
  ]
}
```

**Status codes:**

- 200: Successful read
- 500: Internal Server Error

**4.1.2 Create Conference**

Creates a conference in the DMA via WSP.

The following fields should not be entered during conference creation

- **duration**
- **status**
- **presentedId**
- **created Time**

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```

POST: http://<WSP IP Address>/wsp/conferences
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.conference+json
    Content-type:       application/vnd.com.polycom.cloudAxis.conference+json
Body:
{
  "name": "API doc review",
  "description": "Agenda",
  "startTime": "2015-01-14T07:30:00.000+0000",
  "participantPasscode": "1234",
  "hostPasscode": null,
  "recordingAllowed": false,
  "endTime": "2015-01-14T08:30:00.000+0000",
  "vmrNumber": null,
  "type": "SCHEDULED",
  "status": "FUTURE",
  "allowMultipleChairperson": false,
  "sendMailInvite": true,
  "createdBy": {
    "userName": "sabhat@polycom.com"
  },
  "createdTime": "",
  "userParticipants": null,
  "guestParticipants": null,
  "createdByPersVmr": false,
  "participants": [
    {
      "contactId": "baskar.palanisamy@polycom.com",
      "source": "LOCAL",
      "fullName": "baskar.palanisamy@polycom.com"
    },
    {
      "contactId": "atul.singh@polycom.com",
      "source": "LOCAL",
      "fullName": "Atul Singh"
    }
  ],
  "authRequired": false
}

```

**Response :**

```

HTTP/1.1 201 Created
Location: https://<WSP IP Address>/conferences/1687
Content-Type: application/vnd.com.polycom.cloudaxis.conference+json
{
  "self": "https://<WSP IP Address>/conferences/1687",
  "id": "1687",
  "presentedId": "JlmiNlLdi5",
  "name": "API doc review",
  "description": "Agenda",
  "startTime": "2015-01-14T07:30:00.000+0000",
  "participantPasscode": "1234",
  "hostPasscode": null,
  "recordingAllowed": false,
  "duration": null,
  "endTime": "2015-01-14T08:30:00.000+0000",
  "vmrNumber": "811054",
  "type": "SCHEDULED",
  "status": "FUTURE",
  "allowMultipleChairperson": false,
  "sendMailInvite": true,
  "createdBy": {
    "self": "https://<WSP IP Address>/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  "externalDirectory": true
},
"createdTime": "2015-01-14T04:11:28.331+0000",
"userParticipants": [
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  }
],

```

**Status codes:**

- 201: Successful conference creation
- 400: Bad request
- 500: Internal server error

**4.1.3 Get conference Details by Id**

Get details of a specific conference.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
GET: http://<WSP IP Address>/wsp/conferences/<CONF_ID>      (Example - http://<WSP IP Address>/wsp/conferences/1687)
```

**HEADER DETAILS:**

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.conference+json

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.conference+json
{
  "self": "https://<WSP IP Address>/conferences/1687",
  "id": "1687",
  "presentedId": "JlmiNlLdi5",
  "name": "API doc review",
  "description": "Agenda",
  "startTime": "2015-01-14T07:30:00.000+0000",
  "participantPasscode": "1234",
  "hostPasscode": null,
  "recordingAllowed": false,
  "duration": null,
  "endTime": "2015-01-14T08:30:00.000+0000",
  "vmrNumber": "811054",
  "type": "SCHEDULED",
  "status": "FUTURE",
  "allowMultipleChairperson": false,
  "sendMailInvite": true,
  "createdBy": {
    "self": "https://<WSP IP Address>/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  "externalDirectory": true
},
"createdTime": "2015-01-14T04:11:28.331+0000",
"userParticipants": [
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  }
],
"guestParticipants": [

```



**Status codes:**

- 200: Successful read
- 404: Not Found
- 500: Internal Server Error

**4.1.4 Get conference Details by Conference Presented ID**

Get details of the conference by presented id

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
GET: http://<WSP IP Address>/wsp/conferences/confid?confid=<CONFID>      (Example - http://<WSP IP Address>/wsp/conferences/confid?confid=Jlmi)
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:              application/vnd.com.polycom.cloudAxis.conference+json
```

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.conference+json
{
  "self": "https://<WSP IP Address>/conferences/1687",
  "id": "1687",
  "presentedId": "JlmiNlLdi5",
  "name": "API doc review",
  "description": "Agenda",
  "startTime": "2015-01-14T07:30:00.000+0000",
  "participantPasscode": "1234",
  "hostPasscode": null,
  "recordingAllowed": false,
  "duration": null,
  "endTime": "2015-01-14T08:30:00.000+0000",
  "vmrNumber": "811054",
  "type": "SCHEDULED",
  "status": "FUTURE",
  "allowMultipleChairperson": false,
  "sendMailInvite": true,
  "createdBy": {
    "self": "https://<WSP IP Address>/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  "externalDirectory": true
},
"createdTime": "2015-01-14T04:11:28.331+0000",
"userParticipants": [
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  }
],
"guestParticipants": [

```

**Status codes:**

- 200: Successful read
- 404: Not Found
- 500: Internal Server Error

**4.1.5 Update conference**

Modify the details of a scheduled conference

The following fields cannot be modified:

- **createdBy**
- **duration**
- **status**
- **presentedId**
- **created Time**

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

PUT: http://<WSP IP Address>/wsp/conferences/<CONF\_ID> (Example - http://<WSP IP Address>/wsp/conferences/1687)

#### HEADER DETAILS:

X-CA-UserName: <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn\_username>  
 X-CA-Token: <Auth token obtained after authentication>  
 Content-Type: application/vnd.com.polycom.cloudAxis.conference+json

#### Body:

```
{
  "id":1687,
  "name":"API doc review",
  "description":"Agenda",
  "startTime":"2015-01-15T07:30:00.000+0000",
  "participantPasscode":"12345",
  "hostPasscode":null,
  "recordingAllowed":false,
  "duration":null,
  "endTime":"2015-01-16T08:30:00.000+0000",
  "vmrNumber":null,
  "allowMultipleChairperson":false,
  "sendMailInvite":true,
  "createdBy":{
    "userName":"sabhat@polycom.com"
  },
  "createdTime":"",
  "userParticipants":null,
  "guestParticipants":null,
  "createdByPersVmr":false,
  "participants":[
    {
      "contactId":"baskar.palanisamy@polycom.com",
      "source":"LOCAL",
      "fullName":"baskar.palanisamy@polycom.com"
    },
    {
      "contactId":"atul.singh@polycom.com",
      "source":"LOCAL",
      "fullName":"Atul Singh"
    }
  ],
  "authRequired":false
}
```

### Response :

HTTP/1.1 204 No Content

### Status codes:

- 204: Successful update of Conference
- 500: Internal server error

#### 4.1.6 Cancel conference

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
POST: http://<WSP IP Address>/wsp/conferences/<CONF_ID>/cancel   (Example - http://<WSP IP Address>/wsp/conferences/1687/cancel)
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.conference+json
```

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.conference+json
{
  "self": "https://<WSP IP Address>/conferences/1687",
  "id": "1687",
  "presentedId": "JlmiNlLdi5",
  "name": "API doc review",
  "description": "Agenda",
  "startTime": "2015-01-14T07:30:00.000+0000",
  "participantPasscode": "1234",
  "hostPasscode": null,
  "recordingAllowed": false,
  "duration": null,
  "endTime": "2015-01-14T08:30:00.000+0000",
  "vmrNumber": "811054",
  "type": "SCHEDULED",
  "status": "CANCELLED",
  "allowMultipleChairperson": false,
  "sendMailInvite": true,
  "createdBy": {
    "self": "https://<WSP IP Address>/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  "externalDirectory": true
},
"createdTime": "2015-01-14T04:11:28.331+0000",
"userParticipants": [
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  }
],
"guestParticipants": [

```

**Status codes:**

- 200: Successful cancel
- 400: Bad Request
- 500: Internal Server Error

**4.1.7 End conference****Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
POST: http://<WSP IP Address>/wsp/conferences/<CONF_ID>/end (Example - http://<WSP IP Address>/wsp/conferences/1687/cancel)
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.conference+json
```

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.conference+json
{
  "self": "https://<WSP IP Address>/conferences/1687",
  "id": "1687",
  "presentedId": "JlmiNlLdi5",
  "name": "API doc review",
  "description": "Agenda",
  "startTime": "2015-01-14T07:30:00.000+0000",
  "participantPasscode": "1234",
  "hostPasscode": null,
  "recordingAllowed": false,
  "duration": null,
  "endTime": "2015-01-14T08:30:00.000+0000",
  "vmrNumber": "811054",
  "type": "SCHEDULED",
  "status": "COMPLETED",
  "allowMultipleChairperson": false,
  "sendMailInvite": true,
  "createdBy": {
    "self": "https://<WSP IP Address>/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  "externalDirectory": true
},
"createdTime": "2015-01-14T04:11:28.331+0000",
"userParticipants": [
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  },
  {
    "self": "https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
    "userName": "sabhat@polycom.com",
    "id": "sabhat@polycom.com",
    "email": "sahana.bhat@polycom.com",
    "domain": null,
    "firstName": "Sahana",
    "lastName": "Bhat",
    "title": null,
    "department": null,
    "phoneNumber": null,
    "city": null,
    "enabled": true,
    "role": {
      "self": "https://<WSP IP Address>:443/wsp/roles/role_user",
      "name": "ROLE_USER"
    }
  }
],
"guestParticipants": [

```



**Status codes:**

- 200: Successful end
- 400: Bad Request
- 500: Internal Server Error

**4.1.8 Applying Filters on Conference**

The following filters are accepted:

- **createdBy**: Filter conferences by the user who had created the conference
- **participantId**: Filter conferences by the participant who attended the conference
- **status**: Filter conferences by status (FUTURE/CANCELLED/ON\_GOING/COMPLETED)
- **type**: Filter conferences by its type (AD\_HOC/SCHEDULED)
- **startTime** and **endTime**: Filter conferences whose start time is after **startTime** and end time is before **endTime**. ( **Format**: YYYY-MM-DDTHH:MM:SS) (Please note the time zone is UTC and both startTime & endTime needs to be specified)

**Example:****Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
GET: http://<WSP IP Address>/wsp/conferences?status=COMPLETED&createdBy=sabhat&type=SCHEDULED
```

**HEADER DETAILS:**

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.portal.rest.ConferenceCollection+json

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.portal.rest.conferencecollection+json
{
  "conferences":[
    {
      "self":"https://<WSP IP Address>/conferences/1687",
      "id":"1687",
      "presentedId":"JlmiNlLdi5",
      "name":"API doc review",
      "description":"Agenda",
      "startTime":"2015-01-14T07:30:00.000+0000",
      "participantPasscode":"1234",
      "hostPasscode":null,
      "recordingAllowed":false,
      "duration":null,
      "endTime":"2015-01-14T08:30:00.000+0000",
      "vmrNumber":"811054",
      "type":"SCHEDULED",
      "status":"COMPLETED",
      "allowMultipleChairperson":false,
      "sendMailInvite":true,
      "createdBy":{
        "self":"https://<WSP IP Address>/wsp/users/sabhat@polycom.com",
        "userName":"sabhat@polycom.com",
        "id":"sabhat@polycom.com",
        "email":"sahana.bhat@polycom.com",
        "domain":null,
        "firstName":"Sahana",
        "lastName":"Bhat",
        "title":null,
        "department":null,
        "phoneNumber":null,
        "city":null,
        "enabled":true,
        "role":{
          "self":"https://<WSP IP Address>:443/wsp/roles/role_user",
          "name":"ROLE_USER"
        }
      },
      "externalDirectory":true
    },
    {
      "createdTime":"2015-01-14T04:11:28.331+0000",
      "userParticipants":[
        {
          "self":"https://<WSP IP Address>:443/wsp/users/sabhat@polycom.com",
          "userName":"sabhat@polycom.com",
          "id":"sabhat@polycom.com",
          "email":"sahana.bhat@polycom.com",
          "domain":null,
          "firstName":"Sahana",
          "lastName":"Bhat",
          "title":null,
          "department":null,
          "phoneNumber":null,
          "city":null,
          "enabled":true,
          "role":{
            "self":"https://<WSP IP Address>:443/wsp/roles/role_user",
            "name":"ROLE_USER"
          }
        },
        {
          "self":"https://<WSP IP Address>:443/wsp/roles/role_user",
          "name":"ROLE_USER"
        }
      ],
      "externalDirectory":true
    }
  ]
}

```

**Status codes:**

- 200: Successful read
- 400: Bad Request
- 500: Internal Server Error

**4.1.9 Get a Link to Join a conference****Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
GET: http://<WSP IP Address>/wsp/conferences/<CONF_ID>/join (Example - http://<WSP IP Address>/wsp/conferences/1687/join)
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             text/plain
```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: text/plain
    https://server.polycom.com/JlmiNlLdi5
```

**Status codes:**

- 200: Successful
- 400: Bad Request
- 500: Internal Server Error

## 5 Participant Management

---

### 5.1 Participant Management

Provides APIs to add/remove participants from conference.

#### Properties:

- *fullName*: Full name of the participant.
- *firstName*: First name of the participant.
- *lastName*: Last name of the participant.
- *contactId*: Identifier of user.
- *source*: Connector information: Local,facebook,google,etc. It is an optional value. Default: Local or LDAP User

The supported REST APIs are:

#### 5.1.1 List all participants of a conference

##### Roles allowed:

- ROLE\_USER
- ROLE\_ADMIN

##### Request:

```
GET: http://<WSP IP Address>/wsp/conferences/{id}/participants
```

##### HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
X-CA-Token:	<Auth token obtained after authentication>
ACCEPT:	application/vnd.com.polycom.cloudAxis.participantcollection+json

##### Query Parameters:

- *pageSize*: Size of the current page request. Default: 10
- *currentPage*: Current page number of the request. Default: 0

##### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.participantcollection+json
{
  "participants": [
    {
      "self": "http://localhost:8080/wsp/conferences/771/participants/112",
      "id": 112,
      "contactId": "abc",
      "source": "facebook",
      "fullName": "abc def",
      "firstName": "abc",
      "lastName": "def"
    },
    {
      "self": "http://localhost:8080/wsp/conferences/771/participants/113",
      "id": 113,
      "contactId": "xyz",
      "source": "google",
      "fullName": "abc def",
      "firstName": "abc",
      "lastName": "def"
    }
  ],
  "prev": null,
  "statistics": {
    "currentPage": 0,
    "totalPages": 1,
    "pageSize": 1
  },
  "next": null,
  "self": "http://<WSP IP Address>/wsp/conferences/771/participants?pageSize=5&currentPage=0"
}

```

**Status codes:**

- 200: Successful read
- 500: Internal Server Error

**5.1.2 Add Participant to Conference****Roles allowed:**

- ROLE\_USER
- ROLE\_ADMIN

**Request:**

```

POST: http://<WSP IP Address>/wsp/conferences/771/participants
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:        application/vnd.com.polycom.cloudAxis.participant+json
Body:
{
    "contactId": "xyz",
    "source": "google",
    "fullName": "abc def",
    "firstName": "abc",
    "lastName": "def"
}

```

**Response :**

```

HTTP/1.1 201 Created
Location: http://localhost:8080/wsp/conferences/771/participants/113
Content-Type: application/vnd.com.polycom.cloudAxis.participant+json
{
    "self": "http://localhost:8080/wsp/conferences/771/participants/113",
    "id": 113,
    "contactId": "xyz",
    "source": "google",
    "fullName": "abc def",
    "firstName": "abc",
    "lastName": "def"
}

```

**Status codes:**

- 201: Successful participant creation
- 500: Internal server error

**5.1.3 Add Participants to Conference****Roles allowed:**

- ROLE\_USER
- ROLE\_ADMIN

**Request:**

```
POST: http://<WSP IP Address>/wsp/conferences/771/participants

HEADER DETAILS:

    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:             <Auth token obtained after authentication>
    Content-type:           application/vnd.com.polycom.cloudAxis.participantcollection+json

Body:
{
  "participants": [
    {
      "contactId": "xyz",
      "source": "google",
      "fullName": "abc def",
      "firstName": "abc",
      "lastName": "def"
    },
    {
      "contactId": "abc",
      "source": "facebook",
      "fullName": "abc def",
      "firstName": "abc",
      "lastName": "def"
    }
  ]
}
```

**Response :**

```

HTTP/1.1 201 Created
Location: http://localhost:8080/wsp/conferences/771/participants
Content-Type: application/vnd.com.polycom.cloudAxis.participantcollection+json
{
  "participants": [
    {
      "self": "http://localhost:8080/wsp/conferences/771/participants/112",
      "id": 112,
      "contactId": "abc",
      "source": "facebook",
      "fullName": "abc def",
      "firstName": "abc",
      "lastName": "def"
    },
    {
      "self": "http://localhost:8080/wsp/conferences/771/participants/113",
      "id": 113,
      "contactId": "xyz",
      "source": "google",
      "fullName": "abc def",
      "firstName": "abc",
      "lastName": "def"
    }
  ],
  "self": "http://<WSP IP Address>/wsp/conferences/771/participants"
}

```

**Status codes:**

- 201: Successful participant creation
- 500: Internal server error

**5.1.4 Get Participant details****Roles allowed:**

- ROLE\_USER
- ROLE\_ADMIN

**Request:**

```

GET: http://<WSP IP Address>/wsp/conferences/771/participants/113
HEADER DETAILS:
  X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
  X-CA-Token:         <Auth token obtained after authentication>
  Accept:             application/vnd.com.polycom.cloudAxis.participant+json

```

**Response :**



```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.participant+json
{
  "self": "http://localhost:8080/wsp/conferences/771/participants/113",
  "id": 113,
  "contactId": "xyz",
  "source": "google"
}
```

**Status codes:**

- 200: Successful read
- 404: Participant not found
- 500: Internal Server Error

**5.1.5 Remove Participant from conference****Roles allowed:**

- ROLE\_USER

**Request:**

```
DELETE: http://localhost:8080/wsp/conferences/771/participants/113
HEADER DETAILS:
X-CA-UserName: <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token: <Auth token obtained after authentication>
```

**Response :**

```
HTTP/1.1 204 NO CONTENT
```

**Status codes:**

- 204: Successful delete
- 404: Participant is not found
- 500: Internal Server Error

**5.1.6 Remove Participants from conference****Roles allowed:**

- ROLE\_USER
- ROLE\_ADMIN

**Request:**

```
DELETE: http://localhost:8080/wsp/conferences/771/participants?ids=id1,id2,id3,id4
HEADER DETAILS:
X-CA-UserName: <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token: <Auth token obtained after authentication>
```

**Response :**

```
HTTP/1.1 204 NO CONTENT
```

**Status codes:**

- 204: Successful delete
- 404: Participant is not found
- 500: Internal Server Error

## 6 Social Connectors

### 6.1 Contact Sources Connector Configuration

Provides services for listing and configuring contact provider connectors.

#### Properties:

- *sourceName*: The name of the social connector.
- *imageUrl*: url pointing to the logo of the connector if available.
- *authenticationUrl*: The url to be used for authenticating for the connector. This value cannot be updated.
- *authScope*: The scope of the authorization for the social connector.
- *presence*: True or false based on whether presence information is supported for the connector. This value cannot be updated.
- *enabled*: True or false based on whether the connector is enabled for the user by the admin.
- *authenticated*: True or false based on whether the connector is authenticated.

The supported REST API's are :

#### 6.1.1 List all Connectors

List all configured and supported contact provider connectors

#### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

#### Request:

```
GET: http://<WSP IP Address>/wsp/contact-sources
HEADER DETAILS:
X-CA-UserName: <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token: <Auth token obtained after authentication>
Accept: application/vnd.com.polycom.cloudAxis.contactsourcecollection+json
```

#### Query Parameters:

- *enabled*: Takes value as true/false and list enabled/disabled connector. If no value is provided all connectors are listed.

#### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.contactsourcecollection+json

{
  "statistics": null,
  "prev": null,
  "next": null,
  "sources": [
    {
      "self": "http://<WSP IP Address>/wsp/contact-sources/107",
      "id": "107",
      "sourceName": "LINKEDIN",
      "imageUrl": null,
      "authenticationUrl": null,
      "authScope": "r_basicprofile r_emailaddress r_network r_fullprofile rw_nus w_messages r_contactinfo",
      "presence": true,
      "enabled": true,
      "authenticated": false,
      "redirectUri": "/wsp/wspconnect/connect/linkedin",
      "refreshInterval": 0
    },
    {
      "self": "http://<WSP IP Address>/wsp/contact-sources/106",
      "id": "106",
      "sourceName": "GOOGLE",
      "imageUrl": null,
      "authenticationUrl": null,
      "authScope": "https://www.googleapis.com/auth/googletalk https://www.googleapis.com/auth/userinfo.profile https://www.googleapis.com/auth/contacts",
      "presence": true,
      "enabled": true,
      "authenticated": false,
      "redirectUri": "/wsp/wspconnect/connect/google",
      "refreshInterval": 0
    }
  ]
}

```

### Status codes:

- 200: Successful listing
- 400: Bad request
- 500: Internal Server Error

### 6.1.2 Configure the connectors

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```

PUT: http://<WSP IP Address>/wsp/contact-sources
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.contactsourcecollection+json
Body:
{
  "sources": [
    {
      "sourceName": "LINKEDIN",
      "imageUrl": null,
      "authenticationUrl": null,
      "authScope": "r_basicprofile r_emailaddress r_network r_fullprofile rw_nus w_messages r_contactinfo",
      "presence": true,
      "enabled": true,
      "authenticated": false,
      "redirectUri": "/wsp/wspconnect/connect/linkedin",
      "refreshInterval": 5
    },
    {
      "sourceName": "GOOGLE",
      "imageUrl": null,
      "authenticationUrl": null,
      "authScope": "https://www.googleapis.com/auth/googletalk https://www.googleapis.com/auth/userinfo.profile https://www.googleapis.com/auth/contacts",
      "presence": true,
      "enabled": true,
      "authenticated": false,
      "redirectUri": "/wsp/wspconnect/connect/google",
      "refreshInterval": 5
    }
  ]
}

```

**Response :**

```
HTTP/1.1 201 No-Content
```

**Status codes:**

- 201: Successful updation
- 404: Not Found
- 500: Internal server error

**6.1.3 Disconnect connector****Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```

POST: http://<WSP IP Address>/wsp/contact-sources/{providerId}/disconnect
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
Body:
{
}

```

### Supported path parameters:

- *providerId* : This specifies the provider Id of connector such as LINKEDIN,LOCAL,GOOGLE

### Response :

```
HTTP/1.1 201 No-Content
```

### Status codes:

- 201: Successful updation
- 404: Not Found
- 500: Internal server error

## 7 Global Address Book (GAB)

---

### 7.1 Global Address Book(GAB) API's

Provides api's for getting the contacts from various connectors.

The Supported REST API's are :

#### 7.1.1 Get Contacts

List contacts of the user based on the filter criteria

**Roles allowed:**

- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
GET: http://<WSP IP Address>/wsp/contacts
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.contactcollection+json
```

**Query Parameters:**

- *source*: This query param specifies the connector from which the contacts need to be fetched. If nothing is specified all the contacts will be listed. Eg. GOOGLE, LOCAL, LINKEDIN
- *search*: If search is provided, the result is a search result among the contacts based on the value provided with search. If not provided it is normal listing.

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.contactcollection+json

{
  "statistics": null,
  "prev": null,
  "next": null,
  "contacts": [
    {
      "name": "1234",
      "providerUserId": "SP1Z8ZL56",
      "providerId": "LINKEDIN",
      "email": null,
      "firstName": "1234",
      "lastName": "1234",
      "imageUrl": "http://m.c.lnkd.licdn.com/mpr/mprx/0_JqFQX6X_i8KSX7xyjf94cLZiEcgbFR",
      "presenceStatus": null,
      "phoneNumber": null,
      "profileUrl": null,
      "self": "http://<WSP IP Address>/wsp/contacts/SP1Z8ZL56"
    },
    {
      "name": "XYZ",
      "providerUserId": "xyz@gmail.com",
      "providerId": "GOOGLE",
      "email": "xyz@gmail.com",
      "firstName": "xyz",
      "lastName": "xyz",
      "imageUrl": "https://www.google.com/m8/feeds/photos/media/default/xyz@gmail.com",
      "presenceStatus": "AVAILABLE",
      "phoneNumber": null,
      "profileUrl": null,
      "self": "http://<WSP IP Address>/wsp/contacts/xyz@gmail.com"
    }
  ]
}

```

**Status codes:**

- 200: Successful listing
- 400: Bad request
- 500: Internal Server Error

**7.1.2 Get Synchronized Contacts**

Synchronized contacts from contact providers and returns the contacts

**Roles allowed:**

- ROLE\_ADMIN
- ROLE\_USER

**Request:**



```
GET: http://<WSP IP Address>/wsp/contacts/sync
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.contactcollection+json
```

## Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.contactcollection+json

{
  "statistics": null,
  "prev": null,
  "next": null,
  "contacts": [
    {
      "name": "1234",
      "providerUserId": "SP1Z8ZL56",
      "providerId": "LINKEDIN",
      "email": null,
      "firstName": "1234",
      "lastName": "1234",
      "imageUrl": "http://m.c.lnkd.licdn.com/mpr/mprx/0_JqFQX6X_i8KSX7xyjf94cLZIiEcgbFR",
      "presenceStatus": null,
      "phoneNumber": null,
      "profileUrl": null,
      "self": "http://<WSP IP Address>/wsp/contacts/SP1Z8ZL56"
    },
    {
      "name": "XYZ",
      "providerUserId": "xyz@gmail.com",
      "providerId": "GOOGLE",
      "email": "xyz@gmail.com",
      "firstName": "xyz",
      "lastName": "xyz",
      "imageUrl": "https://www.google.com/m8/feeds/photos/media/default/xyz@gmail.com",
      "presenceStatus": "AVAILABLE",
      "phoneNumber": null,
      "profileUrl": null,
      "self": "http://<WSP IP Address>/wsp/contacts/xyz@gmail.com"
    }
  ]
}
```

## Status codes:

- 200: Successful listing
- 400: Bad request
- 500: Internal Server Error

## 8 VMR Management

### 8.1 VMR (Virtual Meeting Room) Management

Provides API to fetch personal VMR from DMA and ability to store VMR's.

**Properties:** \* *vmr*: The VMR number pulled from DMA.

- *dma*: The DMA related to the VMR.
- *owned*: Boolean that suggests if the VMR is owned by the user or if it is system-generated.
- *name*: name associated with VMR

The supported REST APIs are:

#### 8.1.1 Fetch personal VMR from configured DMA.

**Roles allowed:**

- ROLE\_USER
- ROLE\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/wsp/vmr
HEADER DETAILS:
      X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
      X-CA-Token:         <Auth token obtained after authentication>
      Accept:             application/vnd.com.polycom.cloudaxis.VmrCollectionRepresentation+json
```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.VmrCollectionRepresentation+json
{
  "vmrs": [
    {
      "self": "https://wsp-dev1.cloudax.is:443/wsp/vmr/11321980",
      "vmr": "11321980",
      "dma": "10.250.88.113",
      "owned": true,
      "name": "Vmr 1"
    },
    {
      "self": "https://wsp-dev1.cloudax.is:443/wsp/vmr/11395280",
      "vmr": "11395280",
      "dma": "10.250.88.113",
      "owned": true,
      "name": "Vmr 2"
    }
  ]
}
```

**Status codes:**

- 200: Successful listing
- 500: Internal Server Error

## 9 One Time Token

### 9.1 OneTimeToken APIs

It provides APIs to generate OneTimeToken and is used it along with other REST APIs to do a single successful API call:

#### Properties:

- *userName*: Username for which the OneTimeToken is requested.
- *password*: Password of the User's userName. The password of the user will not be sent back in the response for security reasons and it will be null.
- *tokenId*: The OneTimeToken ie OTT issued to the user to do a single successful transaction. Token's length is of 64 characters.
- *enabled*: User account's enabled status.
- *locked*: User account's locked status.
- *role*: The role assigned to the user.

The supported REST APIS are:

#### 9.1.1 Generate One Time Token

This API is used to generate OneTimeToken which is required to do a single successful transaction in specific cases.

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/platformManagement/ott
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <tokenId obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudaxis.userauth+json
```

#### Response :

```
HTTP/1.1 200 OK
{
  "userName": "admin",
  "password": null,
  "tokenId": "63D1F5D9191E3CAC-558DB400-90517BF1-E09229AA-54E0BA70B7F85186FCA23E23",
  "enabled": null,
  "locked": null,
  "role": null
}
```

#### Status Codes:

- 200: Request is successful
- 401 : Unauthorized if CA-Token is invalid

- 500: Internal Server Error

## 10 SMTP and Server Settings

---

### 10.1 SMTP and Server Settings Configuration

#### Properties:

- *key* : key for the SMTP or Server configuration.
- *value*: value for the key.

#### 10.1.1 SMTP Configuration.

SMTP configuration is required for sending emails.

#### Properties:

- The keys for SMTP are as below:
  - SMTP\_SERVER: SMTP Server name. (eg - corprelayint1.polycom, smtp.gmail.com, etc)
  - SMTP\_PORT: Port at which the SMTP\_SERVER listens. (25 - insecure (SMTP), 465/587 - secure (SMTPS))
  - SMTP\_SECURE: true/false. (Set to false when the SMTP\_PORT is 25, else set to true)
  - SMTP\_LOGIN: login ID to be used to contact the SMTP\_SERVER. (eg - john.Mickey)
  - SMTP\_PASSWORD: password for the login ID. (eg - Mickey@123)
  - SMTP\_SENDER\_MAIL: Mail ID by which the participants would get the mails from the WSP. (eg - noreply-cloudAxis@polycom.com)

**Mandatory keys :** SMTP\_SERVER, SMTP\_SENDER\_MAIL

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```

POST: http://<WSP IP Address>/wsp/cores/list
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.rpinfracollection+json
Body:
{
    "rpCoreDetails":
    [
        {"key": "SMTP_SERVER", "value": "corprelayintl.polycom.com"},
        {"key": "SMTP_PORT", "value": "25"},
        {"key": "SMTP_SECURE", "value": "false"},
        {"key": "SMTP_LOGIN", "value": "login_name"},
        {"key": "SMTP_PASSWORD", "value": "login_passwd"},
        {"key": "SMTP_SENDER_MAIL", "value": "noreply-cloudAxis@polycom.com"}
    ]
}

For configuring a GMail account:
    {"key": "SMTP_SERVER", "value": "smtp.gmail.com"},
    {"key": "SMTP_PORT", "value": "587"},
    {"key": "SMTP_SECURE", "value": "true"},
    {"key": "SMTP_LOGIN", "value": "login_name"},
    {"key": "SMTP_PASSWORD", "value": "login_passwd"},
    {"key": "SMTP_SENDER_MAIL", "value": "login_name@gmail.com"}

```

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.rpinfracollection+json
{
  "self": null,
  "statistics": null,
  "prev": null,
  "next": null,
  "rpCoreDetails": [
    {
      "self": null,
      "name": null
    },
    {
      "self": null,
      "name": null
    },
    {
      "self": null,
      "name": null
    },
    {
      "self": null,
      "name": null
    },
    {
      "self": null,
      "name": null
    }
  ]
}

```

**Status codes:**

- 200: OK - Successful
- 500: Internal Server Error

**10.1.2 Network Configuration.**

This is required for MEA and WSP to find each others addresses.

**Properties:**

- *NETWORK\_HTTP\_SERVER*: This is the FQDN of the MEA server.
- *NETWORK\_WSP\_SERVER*: This is the FQDN of WSP portal.

**Mandatory keys:** NETWORK\_HTTP\_SERVER, NETWORK\_WSP\_SERVER

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**



```

POST: http://<WSP IP Address>/wsp/cores/list
HEADER DETAILS:
    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:             <Auth token obtained after authentication>
    Content-type:           application/vnd.com.polycom.cloudAxis.rpinfracollection+json
Body:
{
    "rpCoreDetails":
    [
        { "key": "NETWORK_HTTP_SERVER", "value": "10.250.88.112" },
        { "key": "NETWORK_WSP_SERVER", "value": "10.250.88.112" }
    ]
}

```

### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.rpinfracollection+json
{
    "self": null,
    "statistics": null,
    "prev": null,
    "next": null,
    "rpCoreDetails": [
        {
            "self": null,
            "name": null
        },
        {
            "self": null,
            "name": null
        }
    ]
}

```

### Status codes:

- 200: OK - Successful
- 500: Internal Server Error

# 11 User Management

## 11.1 User Management

Provides API to perform CRUD operations for User Accounts.

This resource has details for a CloudAxis user and is also related to the roles associated with that user.

### Properties:

- *userName*: User name for the account and it must be unique across the directory.
- *password*: Password for the account.
- *firstName*: First name for the account.
- *lastName*: Last name for the account.
- *title*: Title name for the account.
- *department*: Department to which user belongs to.
- *email*: Email Id for the account.
- *phoneNumber* : Phone number for the account.
- *city*: City to which user belongs to.
- *externalDirectory*: Specify whether account belongs to external directory system or local DB.Default: false.
- *domain*: Domain to which user belongs to.
- *enabled*: Enabled accounts are able to log in to system. Default: true
- *role*: Defined role of the User. Can have values ROLE\_USER,ROLE\_ADMIN & ROLE\_SUPER\_ADMIN.

**Mandatory Properties:** userName, password, firstName, lastName, email, externalDirectory, domain, enabled, role

The supported REST APIs are:

### 11.1.1 List all user accounts

#### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/users
```

HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.usercollection+json

#### Query Parameters:

- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0

#### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.user+json
{
  "users":[
    {
      "self":"http://<WSP IP Address>:8080/wsp/users/jmickey",
      "userName":"jmickey",
      "firstName":"John",
      "lastName":"mickey",
      "title":"J mickey",
      "department":"Cloud Axis",
      "email":"jmickey@domain.com",
      "phoneNumber":"+1-123-456789",
      "city":"San Jose",
      "externalDirectory":false,
      "domain":"domain",
      "enabled":true,
      "role":{
        "self":"http://<WSP IP Address>:8080/wsp/roles/ROLE_USER",
        "name":"ROLE_USER"
      }
    }
  ],
  "prev":null,
  "statistics":{
    "currentPage":0,
    "totalPages":1,
    "pageSize":1
  },
  "next":null,
  "self":"http://<WSP IP Address>:8080/wsp/users?pageSize=5&currentPage=0"
}

```

**Status codes:**

- 200: Successful read
- 500: Internal Server Error

**11.1.2 Create User Account**

**NOTE :** Please take care while passing the externalDirectory flag. To add local user ,use "externalDirectory":false

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

**Request:**

```

POST: http://<WSP IP Address>/wsp/users
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.user+json
    Accept:             application/vnd.com.polycom.cloudAxis.user+json
Body:
{
  "userName": "jmickey",
  "password": "jmickeypwd",
  "firstName": "John",
  "lastName": "mickey",
  "title": "J mickey",
  "department": "Cloud Axis",
  "email": "jmickey@domain.com",
  "phoneNumber": "+1-123-456789",
  "city": "San Jose",
  "externalDirectory": false,
  "domain": "domain",
  "enabled": true,
  "role": {
    "name": "ROLE_USER"
  }
}

```

## Response :role

```

HTTP/1.1 201 Created
Location: https://<WSP IP Address>/wsp/users/jmickey
Content-Type: application/vnd.com.polycom.cloudAxis.user+json
{
  "self": "http://<WSP IP Address>/wsp/users/jmickey",
  "userName": "jmickey",
  "firstName": "John",
  "lastName": "mickey",
  "title": "J mickey",
  "department": "Cloud Axis",
  "email": "jmickey@domain.com",
  "phoneNumber": "+1-123-456789",
  "city": "San Jose",
  "externalDirectory": false,
  "domain": "domain",
  "enabled": true,
  "role": {
    "self": "http://<WSP IP Address>/wsp/roles/ROLE_USER",
    "name": "ROLE_USER"
  }
}

```

## Status codes:

- 201: Successful user account creation

- 500: Internal server error

### 11.1.3 Modify User Account

#### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

#### Request:

```
PUT: http://<WSP IP Address>/wsp/users/jmickey
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.user+json
Body:
{
  "firstName": "John",
  "lastName": "mickey",
  "title": "J mickey",
  "department": "Cloud Axis",
  "email": "jmickey@domain.com",
  "phoneNumber": "+1-123-456789",
  "city": "San Jose",
  "externalDirectory": false,
  "domain": "domain",
  "enabled": false,
  "role": {
    "name": "ROLE_USER"
  }
}
```

#### Response :

```
HTTP/1.1 204 No Content
```

#### Status codes:

- 204: Successful user account modification
- 500: Internal server error

### 11.1.4 Change User Account password

#### 11.1.5 Resource Description

##### Properties:

- *oldPassword*: current password for the user account.
- *newPassword*: new password for the user account.

##### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

- ROLE\_USER

### Request:

```
POST: http://<WSP IP Address>/wsp/users/jmickey/changepassword

HEADER DETAILS:

    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:             <Auth token obtained after authentication>
    Content-type:           application/vnd.com.polycom.cloudaxis.changepassword+json

Body:
{
  "oldPassword": "jmickeypwd",
  "newPassword": "newjmickeypwd"
}
```

### Response :

```
HTTP/1.1 204 No Content
```

### Status codes:

- 204: Successful user account password modification
- 400: If oldPasword is null or not matching with existing password
- 500: Internal server error

#### 11.1.6 Reset User Account password

### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

### Request:

```
POST: http://<WSP IP Address>/wsp/users/jmickey/resetpassword

HEADER DETAILS:

    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:             <Auth token obtained after authentication>
    Content-type:           application/vnd.com.polycom.cloudaxis.changepassword+json

Body:
{
  "newPassword": "newpasswd"
}
```

**Description:** If you need to specify a password while reset send "newPassword": " *new password*"

If you need the system to generate a new password send "newPassword": null

### Response :

```
HTTP/1.1 204 No Content
```

### Description:

- 204: Successful user account password modification
- 404: User account is not found
- 500: Internal server error

### 11.1.7 Read User Account

#### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/users/jmickey

HEADER DETAILS:

X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:             <Auth token obtained after authentication>
Accept:                 application/vnd.com.polycom.cloudAxis.user+json
```

#### Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.user+json
{
  "self": "http://<WSP IP Address>/wsp/users/jmickey",
  "userName": "jmickey",
  "firstName": "John",
  "lastName": "mickey",
  "title": "J mickey",
  "department": "Cloud Axis",
  "email": "jmickey@domain.com",
  "phoneNumber": "+1-123-456789",
  "city": "San Jose",
  "externalDirectory": false,
  "domain": "domain",
  "enabled": true,
  "role": {
    "self": "http://<WSP IP Address>/wsp/roles/ROLE_USER",
    "name": "ROLE_USER"
  }
}
```

#### Description:

- 200: Successful read
- 404: User account is not found
- 500: Internal Server Error

### 11.1.8 Search user by Email or UserName

#### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/users/search?name=test1@a.b
```

#### HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.usercollection+json

## Response :

```
HTTP/1.1 200 OK
```

```
Content-Type: application/vnd.com.polycom.cloudAxis.usercollection+json
```

```
{
  "self": "http://<WSP IP Address>/wsp/users",
  "statistics": {
    "pageSize": 2,
    "currentPage": 0,
    "totalPages": 1
  },
  "prev": null,
  "next": null,
  "users": [
    {
      "self": "http://<WSP IP Address>/wsp/users/abcd",
      "userName": "abcd",
      "email": "test1@a.b",
      "domain": null,
      "firstName": "Deep",
      "lastName": "S",
      "title": null,
      "department": null,
      "phoneNumber": null,
      "city": null,
      "enabled": true,
      "role": null,
      "externalDirectory": false
    },
    {
      "self": "http://<WSP IP Address>/wsp/users/test11",
      "userName": "test11",
      "email": "test1@a.b",
      "domain": null,
      "firstName": "Deep",
      "lastName": "S",
      "title": null,
      "department": null,
      "phoneNumber": null,
      "city": null,
      "enabled": true,
      "role": null,
      "externalDirectory": false
    }
  ]
}
```



**Description:**

- 200: Successful read
- 404: User account is not found
- 500: Internal Server Error

**11.1.9 Delete User Account****Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

**Request:**

```
DELETE: http://<WSP IP Address>/wsp/users/jmickey
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
```

**Response :**

```
HTTP/1.1 204 NO CONTENT
```

**Description:**

- 204: Successful delete
- 404: User account is not found
- 500: Internal Server Error

**11.1.10 Read assigned user role****Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/wsp/users/jmickey/role
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.role+json
```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.role+json
{
  "self": "http://<WSP IP Address>/wsp/roles/ROLE_USER",
  "name": "ROLE_USER"
}
```

**Description:**

- 200: Successful read
- 404: User account is not found
- 500: Internal Server Error

#### 11.1.11 Modify user role

##### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

##### Request:

```
PUT: http://<WSP IP Address>/wsp/users/jmickey/role
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-Type:       application/vnd.com.polycom.cloudAxis.role+json
{
  "name": "ROLE_USER"
}
```

##### Response :

```
HTTP/1.1 204 NO CONTENT
```

##### Description:

- 200: Successful read
- 404: User account is not found
- 500: Internal Server Error

## 12 Role Management

### 12.1 Role Management

It provides API to perform CRUD operations for Role.

The supported REST APIs are:

#### 12.1.1 List all roles

##### Request:

```
GET: http://<WSP IP Address>/wsp/roles
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.rolecollection+json
```

##### Query Parameters:

- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0

##### Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.rolecollection+json
{
  "roles":[
    {
      "self":"http://<WSP IP Address>/wsp/roles/ROLE_USER",
      "name":"ROLE_USER"
    }
  ],
  "prev":null,
  "statistics":{
    "currentPage":0,
    "totalPages":1,
    "pageSize":1
  },
  "next":null,
  "self":"http://<WSP IP Address>/wsp/roles?pageSize=5&currentPage=0"
}
```

##### Description:

- *roles*: List of roles
- 200: Successful read
- 500: Internal Server Error

### 12.1.2 Create Role

#### Request:

```
POST: http://<WSP IP Address>/wsp/roles

HEADER DETAILS:

    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:             <Auth token obtained after authentication>
    Content-type:           application/vnd.com.polycom.cloudAxis.role+json

Body:
{
    "name": "ROLE_USER"
}
```

#### Description:

- *name*: Name of role

#### Response :

```
HTTP/1.1 201 Created
Location: https://<WSP IP Address>/roles/ROLE_USER
Content-Type: application/vnd.com.polycom.cloudAxis.role+json
{
    "self": "http://<WSP IP Address>/wsp/roles/ROLE_USER",
    "name": "ROLE_USER"
}
```

#### Status Codes:

- 201: Successful role creation
- 500: Internal server error

### 12.1.3 Read role

#### Request:

```
GET: http://<WSP IP Address>/wsp/roles/ROLE_USER

HEADER DETAILS:

    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:             <Auth token obtained after authentication>
    Accept:                 application/vnd.com.polycom.cloudAxis.role+json
```

#### Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.role+json
{
    "self": "http://<WSP IP Address>/wsp/roles/ROLE_USER",
    "name": "ROLE_USER"
}
```

**Status Codes:**

- 200: Successful read
- 404: Role is not found
- 500: Internal Server Error

**12.1.4 Delete role****Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
DELETE: http://<WSP IP Address>/wsp/roles/ROLE_USER
```

**HEADER DETAILS:**

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:	<Auth token obtained after authentication>

**Response :**

```
HTTP/1.1 204 NO CONTENT
```

**Status Codes:**

- 204: Successful delete
- 404: Role is not found
- 500: Internal Server Error

## 13 LDAP Configuration

### 13.1 LDAP Configuration and Search

It provides API to configure LDAP and search user in LDAP:

#### 13.1.1 Get LDAP Configuration

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/platform/ldapconfig
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.platform.ldapsetting+json
```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.platform.ldapsetting+json
{
  "port": 389,
  "defaultDomain": "POLYCOM",
  "enableSubDomainSearch": false,
  "enableDefaultDomain": false,
  "domain": "polycom.com",
  "siteName": "India",
  "secure": false,
  "password": null,
  "userName": "polycom\\username",
  "server": "tcydcprd01.polycom.com",
  "enableStaticServer": "false"
}
```

**Status codes:**

- 200: OK - Successful
- 500: Internal Server Error

#### 13.1.2 LDAP Configuration

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```

POST: http://<WSP IP Address>/platform/ldapconfig
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.platform.ldapsetting+json
Body:
{
    "domain": "polycom.com",
    "siteName": "India",
    "userName": "polycom\\username",
    "password": "password",
    "secure": false,
    "port": 389,
    "enableSubDomainSearch": false,
    "enableDefaultDomain": true,
    "defaultDomain": "POLYCOM",
    "server": "tcydcprd01.polycom.com",
    "enableStaticServer": "false"
}

```

### Properties:

- *domain*: Forest Root Domain or SubDomain.
- *siteName*: Site name of the Active Directory where the WSP is planned to be configured. It can be sent as null. Keeping it null will make LDAP configuration without site.
- *userName*: Any Active Directory username. Generally it will be of Admin's.
- *password*: Password of above AD Username.
- *secure*: true if LDAPs is supported.
- *port*: Default port is 389 for LDAP and 636 for LDAPs.
- *enableSubDomainSearch*: true if sub-domain search needs to be enabled
- *enableDefaultDomain*: true if default-domain needs to be enabled.
- *defaultDomain*: Name of the default domain. (If enableDefaultDomain is set true and defaultDomain="POLYCOM" then the users need not login as "polycom\\username". Instead they can enter as "username".
- *server*: Name of the AD server (domain controller). Admin can hard code domain controller if he wants followed by flag enableStaticServer=true.
- *enableStaticServer*: If true then domain controller name provided in server field will be configured. Also enableSubDomainSearch will be considered false and siteName will be ignored though it is provided. If false, server field value will be ignored.

### Response :

```
HTTP/1.1 200 OK
```

### Status codes:

- 200: OK - Successful
- 500: Internal Server Error

### 13.1.3 Find User in Active Directory

#### Roles allowed:

- **ROLE\_SUPER\_ADMIN**

### Request:

```
GET: http://<WSP IP Address>/wsp/users/searchad?filter=user_upn

HEADER DETAILS:

X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudaxis.usercollection+json
```

### Query Parameters:

- **filter:** The filter can be firstname(e.g. chirag) or lastname(e.g. katudia) or username(e.g. ckatudia). The filter is case insensitive.

### Response :

```
HTTP/1.1 200 OK

Content-Type: application/vnd.com.polycom.cloudaxis.usercollection+json

{
  "self": null,
  "statistics": null,
  "prev": null,
  "next": null,
  "users": [
    {
      "self": "http://localhost:8080/users/user_upn@domain.com",
      "userName": "user_upn@domain.com",
      "email": "user.email@domain.com",
      "domain": null,
      "firstName": "First",
      "lastName": " Last",
      "title": null,
      "department": null,
      "phoneNumber": null,
      "city": null,
      "enabled": true,
      "role": null,
      "externalDirectory": false
    }
  ]
}
```

### Status codes:

- 200: OK - If user found or not found. If not found, it will return empty list.
- 500: Internal server error



## 14 RP Core Service

---

### 14.1 RP Core Service

Provides CRUD services for Core parameters: SMTP, MEA and WSP server settings.

The Supported API's are :

#### 14.1.1 List all parameters

List of all stored parameters in the database

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
GET: http://<WSP IP Address>/wsp/cores
```

HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.rpinfracollection+json

**Query Parameters:**

- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.rpinfracollection+json
{
  "rpCoreDetails": [
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_LOGIN",
      "key": "SMTP_LOGIN",
      "value": null
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_PASSWORD",
      "key": "SMTP_PASSWORD",
      "value": null
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_PORT",
      "key": "SMTP_PORT",
      "value": "25"
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_SECURE",
      "key": "SMTP_SECURE",
      "value": "false"
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_SENDER_MAIL",
      "key": "SMTP_SENDER_MAIL",
      "value": "no-reply@polycom.com"
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_SERVER",
      "key": "SMTP_SERVER",
      "value": "xyz.polycom.com"
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/NETWORK_MEA_SERVER",
      "key": "NETWORK_MEA_SERVER",
      "value": "https://mea-server.xyz.is"
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/NETWORK_WSP_SERVER",
      "key": "NETWORK_WSP_SERVER",
      "value": "https://wsp-server.xyz.is"
    }
  ],
  "next": null,
  "prev": null,
  "statistics": {
    "pageSize": 2,
    "currentPage": 0,
    "totalPages": 1
  },
  "self": "http://<WSP_IP_Address>/wsp/cores"
}

```

**Status codes:**

- 200: Successful listing
- 500: Internal Server Error

**14.1.2 List parameters by type query****Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
GET: http://<WSP IP Address>/wsp/cores/type?type=SMTP
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.rpinfracollection+json
```

**Query Parameters:**

- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0
  - *type*: SMTP or NETWORK

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.rpinfracollection+json
{
  "rpCoreDetails": [
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_LOGIN",
      "key": "SMTP_LOGIN",
      "value": null
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_PASSWORD",
      "key": "SMTP_PASSWORD",
      "value": null
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_PORT",
      "key": "SMTP_PORT",
      "value": "25"
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_SECURE",
      "key": "SMTP_SECURE",
      "value": "false"
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_SENDER_MAIL",
      "key": "SMTP_SENDER_MAIL",
      "value": "no-reply@polycom.com"
    },
    {
      "self": "https://<WSP_IP_ADDRESS>/wsp/cores/SMTP_SERVER",
      "key": "SMTP_SERVER",
      "value": "xyz.polycom.com"
    }
  ],
  "next": null,
  "prev": null,
  "statistics": {
    "pageSize": 2,
    "currentPage": 0,
    "totalPages": 1
  },
  "self": "http://<WSP_IP_Address>/wsp/cores"
}

```

### Status codes:

- 200: Successful listing
- 500: Internal Server Error

### 14.1.3 List a Parameter details

#### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

**Request:**

```
GET: http://<WSP IP Address>/wsp/cores/KEY (Example - http://<WSP IP Address>/cores/NETWORK_WSP_SERVER)
HEADER DETAILS:
X-CA-UserName: <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token: <Auth token obtained after authentication>
Accept: application/vnd.com.polycom.cloudAxis.rpinfra+json
```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.rpinfra+json
{
  "self": "https://<WSP_IP_ADDRESS>/wsp/cores/NETWORK_WSP_SERVER",
  "key": "NETWORK_WSP_SERVER",
  "value": "https://wsp-server.xyz.is"
}
```

**Status codes:**

- 200: Successful listing
- 404: Not Found
- 500: Internal Server Error

**14.1.4 Update Parameter value****Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
PUT: http://<WSP IP Address>/wsp/cores/KEY (Example - http://<WSP IP Address>/wsp/cores/NETWORK_WSP_SERVER)
HEADER DETAILS:
X-CA-UserName: <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token: <Auth token obtained after authentication>
Content-Type: application/vnd.com.polycom.cloudAxis.rpinfra+json
Body:
{
  "value": "https://wsp-server1.xyz.is"
}
```

**Response :**

```
HTTP/1.1 204 No Content
```

**Status codes:**

- 204: Successful Update
- 400: Bad Request
- 500: Internal Server Error

### 14.1.5 Update Multiple values

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
POST: http://<WSP IP Address>/wsp/cores/list (Example - http://<WSP IP Address>/wsp/cores/list)
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-Type:       application/vnd.com.polycom.cloudAxis.rpinfracollection+json
Body:
{
    "rpCoreDetails":
    [
        {
            {key: "SMTP_LOGIN", value: ""},
            {key: "SMTP_PASSWORD", value: ""},
            {key: "SMTP_PORT", value: "25"},
            {key: "SMTP_SECURE", value: false},
            {key: "SMTP_SENDER_MAIL", value: "cloudaxis-wspdev1@polycom.com"},
            {key: "SMTP_SERVER", value: "mailrelay.polycom.com"}
        }
    ]
}
```

#### Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.rpinfracollection+json
{
  "self": null,
  "statistics": null,
  "prev": null,
  "next": null,
  "rpCoreDetails": [
    {
      "self": null,
      "name": null
    },
    {
      "self": null,
      "name": null
    },
    {
      "self": null,
      "name": null
    },
    {
      "self": null,
      "name": null
    },
    {
      "self": null,
      "name": null
    }
  ]
}
```

**Status codes:**

- 204: Successful Update
- 500: Internal Server Error
- 400: Bad Request

## 15 Access Point Service

### 15.1 Access Point Service

Provides APIs to perform CRUD operations for Access Point.

An access point is a network location that is routed directly or indirectly to the DMA from where clients or endpoints can connect to participate in a conference.

#### Properties:

- *hostname*: IP Address/domain or the dialstring of Access point
- *geoZone*: Geo Zone such Asia, EU, US, etc
- *transport*: sip, h.323, pstn, isdn, tunnel are the possible values
- *authenticationMode*: Defines the characteristics of the port provided in dial string (if provided). Possible values are auth, noauth and shared.
- *nonAuthenticatedPrefix*: The dial prefix which will get appended to the VMR by MEA or RPAD.
- *priority*: The priority of the accesspoint.

**Mandatory Properties:** hostname, geoZone, transport, authenticationMode

The supported REST APIs are:

#### 15.1.1 List all Access points

Gets the list of accesspoints.

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/accesspoints
HEADER DETAILS:
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.accesspointcollection+json
```

#### Query Parameters:

- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0

#### Response :



```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.accesspointcollection+json
{
  "accessPoints": [
    {
      "self": "http://localhost:8080/wsp/accesspoints/771",
      "id": 771,
      "geoZone": "EU",
      "transport": "sip",
      "hostname": "10.0.0.1",
      "authenticationMode": "AUTO",
      "nonAuthenticatedPrefix": 34,
      "priority": 1
    },
    {
      "self": "http://localhost:8080/wsp/accesspoints/772",
      "id": 772,
      "geoZone": "US",
      "transport": "h.303",
      "hostname": "10.0.0.2",
      "authenticationMode": null,
      "nonAuthenticatedPrefix": 0,
      "priority": 2
    }
  ],
  "prev": null,
  "statistics": {
    "currentPage": 0,
    "totalPages": 1,
    "pageSize": 1
  },
  "next": null,
  "self": "http://<WSP IP Address>/wsp/accesspoints?pageSize=5&currentPage=0"
}

```

**Status codes:**

- 200: Successful read
- 500: Internal Server Error

**15.1.2 Create Access Point**

Creates an access point

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```

POST: http://<WSP IP Address>/wsp/accesspoints
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.accesspoint+json
    Content-type:       application/vnd.com.polycom.cloudAxis.accesspoint+json

Body:
{
    "hostname": "10.0.0.1",
    "geoZone": "EU",
    "transport": "sip",
    "authenticationMode": "AUTO",
    "nonAuthenticatedPrefix": 34,
    "priority": 1
}

```

**Response :**

```

HTTP/1.1 201 Created
Location: https://<WSP IP Address>/wsp/accesspoints/1
Content-Type: application/vnd.com.polycom.cloudAxis.accesspoint+json
{
    "self": "http://<WSP IP Address>/wsp/accesspoints/1",
    "id": 1,
    "hostname": "10.0.0.1",
    "geoZone": "EU",
    "transport": "sip",
    "authenticationMode": "AUTO",
    "nonAuthenticatedPrefix": 34,
    "priority": 1
}

```

**Status codes:**

- 201: Successful Access Point creation
- 500: Internal server error

**15.1.3 Modify Access Point**

Modifies the specified access point

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```

PUT: http://<WSP IP Address>/wsp/accesspoints/1
HEADER DETAILS:
    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:             <Auth token obtained after authentication>
    Content-type:           application/vnd.com.polycom.cloudAxis.accesspoint+json
Body:
{
    "hostname": "10.0.1.1",
    "geoZone": "Asia",
    "transport": "h.303",
    "authenticationMode": null,
    "nonAuthenticatedPrefix": 0,
    "priority": 1
}

```

**Response :**

```

HTTP/1.1 204 No Content

```

**Status codes:**

- 204: Successful update
- 500: Internal server error

**15.1.4 Get Access Point**

Gets the specified access point

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```

GET: http://<WSP IP Address>/wsp/accesspoints/1
HEADER DETAILS:
    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:             <Auth token obtained after authentication>
    ACCEPT:                 application/vnd.com.polycom.cloudAxis.accesspoint+json

```

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.accesspoint+json
{
    "self": "http://<WSP_IP_Address>/wsp/accesspoints/1",
    "id": 1,
    "hostname": "10.0.0.1",
    "geoZone": "EU",
    "transport": "sip",
    "authenticationMode": "AUTO",
    "nonAuthenticatedPrefix": 34,
    "priority": 1
}

```

**Status codes:**

- 200: Successful read
- 404: Access point is not found
- 500: Internal Server Error

**15.1.5 Delete Access Point**

Deletes the specified access point

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```

DELETE: http://<WSP_IP_Address>/wsp/accesspoints/1
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>

```

**Response :**

```

HTTP/1.1 204 NO CONTENT

```

**Status codes:**

- 204: Successful delete
- 404: Access point is not found
- 500: Internal Server Error

## 16 DMA Configuration Service

---

### 16.1 DMA Config Service

Provides APIs to perform CRUD operations for DMA configuration in WSP.

**NOTE :** These API's are for registering the DMA configuration in WSP server and not for configuring the DMA server itself. Accurate information as available in the DMA should be given for proper registration.

DMA needs to be configured with the correct values to be able to schedule a meeting. Atleast one DMA has to be registered as the primary DMA.

#### Properties:

- *name*: A nickname to assign to the DMA to distinguish it in WSP configuration.
- *hostname*: FQDN or IP of the DMA being configured.
- *port*: TCP port number of the DMA being configured. Commonly used port is 8443 corresponding to the HTTPS REST API for the DMA
- *defaultAdmin*: User account name with an admin role that exists on the DMA. This account will be used to for creating a meeting.
- *adminPassword*: Password of the default admin account.
- *ownerDomain*: Domain of the user account assigned for creating meetings in the DMA.
- *ownerUserName*: Username assigned for creating meetings in DMA.
- *conferenceTemplate*: Name of the conference template to be used for the meetings.
- *mcuPoolOrder*: MCU Pool Order to be used for the meetings.
- *vmrPrefix*: 2 Digit Dial-in-Prefix that will be attached to the VMR created by DMA.
- *primaryDMA*: This indicates which DMA is primary and used for dynamic VMR.
- *accessPoints*: List of created access points with id information. DMA has a relationship with access points.
- *commonSipUserName*: Common Sip username which will be used by MEA and other devices to authenticate a SIP call.
- *commonSipPassword*: Password for the the common SIP Username.
- *generateVmrFromRange*: True if required to generate VMR from a given range.
- *startRangeForVmr*: Start of vmr range, ex., 100000.
- *endRangeForVmr*: End of vmr range, ex., 999999.

**Mandatory Properties:** name, hostname, port, defaultAdmin, adminPassword, ownerDomain, ownerUserName

The supported REST APIs are:

#### 16.1.1 List all configured DMA's

Gets the list of all configured DMA's and their details

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/dma
```

**HEADER DETAILS:**

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.dmaconfigcollection+json

**Query Parameters:**

- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.dmaconfigcollection+json
{
  "self": "http://localhost:8080/wsp/dma?pageSize=5&currentPage=0",
  "statistics": {
    "pageSize": 2,
    "currentPage": 0,
    "totalPages": 1
  },
  "prev": null,
  "next": null,
  "dmaConfigs": [
    {
      "self": "http://localhost:8080/wsp/dma/776",
      "id": "776",
      "name": "DMA 1",
      "hostname": "video.poly.com",
      "port": "8443",
      "vmrPrefix": 72,
      "defaultAdmin": "admin",
      "adminPassword": null,
      "ownerDomain": "LOCAL",
      "ownerUserName": "wsp",
      "conferenceTemplate": "Factory Template",
      "mcuPoolOrder": "Factory Pool Order",
      "primaryDMA": false,
      "generateVmrFromRange": true,
      "startRangeForVmr": 100000,
      "endRangeForVmr": 999999,
      "commonSipUserName": "ancdefg",
      "commonSipPassword": "ancdefg",
      "accessPoints": []
    },
    {
      "self": "http://localhost:8080/wsp/dma/773",
      "id": "773",
      "name": "DMA 1",
      "hostname": "video.poly.com",
      "port": "8443",
      "vmrPrefix": 72,
      "defaultAdmin": "admin",
      "adminPassword": null,
      "ownerDomain": "LOCAL",
      "ownerUserName": "wsp",
      "conferenceTemplate": null,
      "mcuPoolOrder": null,
      "primaryDMA": false,
      "generateVmrFromRange": true,
      "startRangeForVmr": 10000,
      "endRangeForVmr": 99999,
      "commonSipUserName": "ancdefg",
      "commonSipPassword": "ancdefg",
      "accessPoints": [
        {
          "self": "http://localhost:8080/wsp/accesspoints/771",
          "id": 771,
          "geoZone": "Asia",
          "transport": "sip",
          "hostname": "10.0.0.1",
          "authenticationMode": "AUTO",
          "nonAuthenticatedPrefix": 34,

```

**Status codes:**

- 200: Successful listing
- 500: Internal Server Error

**16.1.2 Configure a DMA in WSP**

Configures the DMA details in WSP. Atleast one DMA should be configured as primary DMA.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
POST: http://<WSP IP Address>/wsp/dma
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.dmaconfig+json
    Content-type:       application/vnd.com.polycom.cloudAxis.dmaconfig+json
Body:
{
  "name": "DMA 1",
  "hostname": "vido.poly.com",
  "port": "8443",
  "vmrPrefix": 71,
  "defaultAdmin": "admin",
  "adminPassword": "admin",
  "ownerDomain": "LOCAL",
  "ownerUserName": "wsp",
  "conferenceTemplate": "Factory Template",
  "mcuPoolOrder": "Factory Pool Order",
  "primaryDMA": "false",
  "generateVmrFromRange": true,
  "startRangeForVmr": 100000,
  "endRangeForVmr": 999999,
  "commonSipUserName": "ancdefg",
  "commonSipPassword": "ancdefg",
  "accessPoints": [{"id": 771}]
}
```

**Response :**



```

HTTP/1.1 201 Created
Location: http://<WSP IP Address>/dma/158
Content-Type: application/vnd.com.polycom.cloudAxis.dmaconfig+json

{
  "self": "http://<WSP IP Address>/wsp/dma/158",
  "id": "158",
  "name": "DMA 1",
  "hostname": "vido.poly.com",
  "port": "8443",
  "vmrPrefix": 72,
  "defaultAdmin": "admin",
  "adminPassword": null,
  "ownerDomain": "LOCAL",
  "ownerUserName": "wsp",
  "conferenceTemplate": "Factory Template",
  "mcuPoolOrder": "Factory Pool Order",
  "primaryDMA": "false",
  "generateVmrFromRange": true,
  "startRangeForVmr": 100000,
  "endRangeForVmr": 999999,
  "commonSipUserName": "ancdefg",
  "commonSipPassword": "ancdefg",
  "accessPoints": [
    {
      "self": "http://localhost:8080/wsp/accesspoints/771",
      "id": 771,
      "geoZone": "Asia",
      "transport": "sip",
      "hostname": "10.0.0.1",
      "authenticationMode": "AUTO",
      "nonAuthenticatedPrefix": 34,
      "priority": 1
    }
  ]
}

```

**Status codes:**

- 201: Successful DMA addition
- 400: Bad Request
- 500: Internal server error

**16.1.3 List a DMA's config details**

Get a specific DMA's configuration details

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/dma/<DMA_ID>
```

#### HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.dmaconfig+json

## Response :

```
HTTP/1.1 200 OK
```

```
Content-Type: application/vnd.com.polycom.cloudAxis.dmaconfig+json
```

```
{
  "self": "http://<WSP IP Address>/wsp/dma/157",
  "id": "157",
  "name": "DMA 1",
  "hostname": "vido.poly.com",
  "port": "8443",
  "vmrPrefix": 72,
  "defaultAdmin": "admin",
  "adminPassword": null,
  "ownerDomain": "LOCAL",
  "ownerUserName": "wsp",
  "conferenceTemplate": "Factory Template",
  "mcuPoolOrder": "Factory Pool Order",
  "primaryDMA": "false",
  "generateVmrFromRange": true,
  "startRangeForVmr": 100000,
  "endRangeForVmr": 999999,
  "commonSipUserName": "ancdefg",
  "commonSipPassword": "ancdefg",
  "accessPoints": [
    {
      "self": "http://localhost:8080/wsp/accesspoints/771",
      "id": 771,
      "geoZone": "Asia",
      "transport": "sip",
      "hostname": "10.0.0.1",
      "authenticationMode": "AUTO",
      "nonAuthenticatedPrefix": 34,
      "priority": 1
    }
  ]
}
```

## Status codes:

- 200: Successful listing
- 404: Not Found
- 500: Internal Server Error

### 16.1.4 Update a DMA's Configuration

Modify a DMA's configuration

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
PUT: http://<WSP IP Address>/wsp/dma/<DMA_ID>
      (Example - http://<WSP IP Address>/wsp/dma/158)

HEADER DETAILS:
      X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
      X-CA-Token:         <Auth token obtained after authentication>
      Content-Type:       application/vnd.com.polycom.cloudAxis.dmaconfig+json

Body:
{
  "name": "DMA 1",
  "hostname": "vido.poly.com",
  "port": "8443",
  "vmrPrefix": 72,
  "defaultAdmin": "admin",
  "adminPassword": "admin",
  "ownerDomain": "LOCAL",
  "ownerUserName": "wsp",
  "conferenceTemplate": "Factory Template",
  "mcuPoolOrder": "Factory Pool Order",
  "primaryDMA": "false",
  "generateVmrFromRange": true,
  "startRangeForVmr": 100000,
  "endRangeForVmr": 999999,
  "commonSipUserName": "ancdefg",
  "commonSipPassword": "ancdefg",
  "accessPoints": [{"id": 772}]
}
```

**Response :**

```
HTTP/1.1 204 No Content
```

**Status codes:**

- 204: Successful Update
- 400: Bad Request
- 500: Internal Server Error

### 16.1.5 Remove a DMA configuration from WSP

Deletes a configured DMA and its details from WSP.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
DELETE: http://<WSP IP Address>/wsp/dma/157
```

HEADER DETAILS:

```
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
X-CA-Token:         <Auth token obtained after authentication>
```

On deletion of a DMA from WSP following steps are followed. 1) If any Ongoing meetings are available for the DMA, deletion is not allowed. 2) All the scheduled meetings are cancelled. 3) In all the Completed and Cancelled meeting the dmaused attribute is set to null.

**Response :**

```
HTTP/1.1 204 NO CONTENT
```

**Status codes:**

- 204: Successful delete
- 404: Not found
- 500: Internal Server Error

### 16.1.6 List a DMA's Conference Templates

Lists the conference templates available

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/wsp/dma/<DMA_ID>/templates
```

(Example - http://<WSP IP Address>/wsp/dma/157/templates)

HEADER DETAILS:

```
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.system.DmaTemplateCollection+json
```

**Response :**

```
HTTP/1.1 200 OK
```

```
Content-Type: application/vnd.com.polycom.cloudaxis.system.dmatemplatecollection+json
```

```
{
  "dmaTemplates": [
    "Factory Template",
    "cesconftemp",
    "BorisTemplate",
    "Akumar Template",
    "Schulze",
    "ccs",
    "Default Template",
    "Sample Renovo template"
  ]
}
```

**Status codes:**

- 200: Successful listing
- 400: Bad Request
- 500: Internal Server Error

**16.1.7 List a DMA's MCU Pool Orders**

List the MCU pool orders that are available

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/wsp/dma/DMA_ID/pool-orders
      (Example - http://<WSP IP Address>/wsp/dma/157/pool-orders)

HEADER DETAILS:
      X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
      X-CA-Token:            <Auth token obtained after authentication>
      Accept:                 application/vnd.com.polycom.cloudAxis.system.DmaPoolOrderCollection+json
```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.system.dmapoolordercollection+json
{
  "mcuPoolOrders": [
    "Factory Pool Order",
    "Adam's Pool Order",
    "Wayne's Pool Order",
    "cescpoolorder",
    "Alexey's PO"
  ]
}
```

**Status codes:**

- 200: Successful listing
- 400: Bad Request
- 500: Internal Server Error

## 17 Policy Management

### 17.1 Policy Management

Provides APIs to retrieve and update operations for social policies. The social connectors that are available are: GOOGLE, LINKEDIN

Policy resource enables social policies in WSP, which in turn allows WSP to integrate with the respective social connectors to get the users contact list and presence (if applicable). It also allows instant messages/invites to be sent to the user's social contacts.

#### Properties:

- *name*: Name of the social connector. Currently WSP allows GOOGLE and LINKEDIN connector integration.
- *value*: "enabled" if the connector is to be enabled. Else "disabled". Default value is "disabled".
- *client\_id*: Provide the client\_id that is obtained after registering the WSP application with the connector.
- *client\_secret*: Provide the client\_secret that is provided by the connector during the registration process.
- *authenticationUrl*: null at the moment. For future use.
- *authScope*: The scope of the apis that can be accessed for integration. Do not change the default values unless required.
- *redirectUri*: Redirect uri for the social connector to redirect to after authentication/authorization.
- *refreshInterval*: The interval at which the contact details should be refreshed from the social connector integrated with WSP. Default value is 5 minutes.

**Mandatory Properties:** name, client\_id, client\_secret, authScope, redirectUri

The supported REST APIs are::

#### 17.1.1 List all Policies

List all the policies that are available for integration with WSP

#### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

#### Request:

```
GET: http://<WSP IP Address>/wsp/policy
HEADER DETAILS:
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.policycollection+json
```

#### Query Parameters:

- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0

#### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.policycollection+json

{
  "statistics": null,
  "prev": null,
  "next": null,
  "policies": [
    {
      "self": "http://localhost:8080/wsp/policy/1",
      "id": 1,
      "name": "GOOGLE",
      "value": "enabled",
      "client_id": "212021495702.apps.googleusercontent.com",
      "client_secret": "zN6_Boxvfk5ZabLXYWYks8hg",
      "authenticationUrl": null,
      "authScope": "https://www.googleapis.com/auth/googletalk https://www.googleapis.com/auth/userinfo.profile https://www",
      "redirectUri": "https://<WSP IP ADDRESS>/wsp/wspconnect/connect/google",
      "refreshInterval": 5
    },
    {
      "self": "http://localhost:8080/wsp/policy/107",
      "id": 107,
      "name": "LINKEDIN",
      "value": "enabled",
      "client_id": "75e2dphtrdolia",
      "client_secret": "4kP61P7L7qlhX5bQfg",
      "authenticationUrl": null,
      "authScope": "r_basicprofile r_emailaddress r_network r_fullprofile rw_nus w_messages r_contactinfo",
      "redirectUri": "https://<WSP IP ADDRESS>/wsp/wspconnect/connect/linkedin",
      "refreshInterval": 5
    }
  ]
}

```

**Status codes:**

- 200: Successful listing
- 500: Internal Server Error

**17.1.2 Modify Policies**

Update multiple policy configurations

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

**Request:**

```

POST: http://<WSP IP Address>/wsp/policy
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.policycollection+json
Body:
{
  "policies": [
    {
      "name": "GOOGLE",
      "value": "enabled",
      "client_id": "212021495702.apps.googleusercontent.com",
      "client_secret": "zN6_Boxvfk5ZabLXYWYks8hg",
      "authenticationUrl": null,
      "authScope": "https://www.googleapis.com/auth/googletalk https://www.googleapis.com/auth/userinfo.profile https://www",
      "redirectUri": "https://<WSP IP ADDRESS>/wsp/wspconnect/connect/google",
      "refreshInterval": 5
    },
    {
      "self": "http://localhost:8080/wsp/policy/107",
      "id": 107,
      "name": "LINKEDIN",
      "value": "enabled",
      "client_id": "75e2dphtrdolia",
      "client_secret": "4kP61P7L7qlhX5bQfg",
      "authenticationUrl": null,
      "authScope": "r_basicprofile r_emailaddress r_network r_fullprofile rw_nus w_messages r_contactinfo",
      "redirectUri": "https://<WSP IP ADDRESS>/wsp/wspconnect/connect/linkedin",
      "refreshInterval": 5
    }
  ]
}

```

**Response :**



```

HTTP/1.1 200 OK
Location: http://<WSP IP Address>/policy
Content-Type: application/vnd.com.polycom.cloudAxis.policycollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "policies": [
    {
      "self": "http://localhost:8080/wsp/policy/1",
      "id": 1,
      "name": "GOOGLE",
      "value": "enabled",
      "client_id": "212021495702.apps.googleusercontent.com",
      "client_secret": "zN6_Boxvfk5ZabLXYWYks8hg",
      "authenticationUrl": null,
      "authScope": "https://www.googleapis.com/auth/googletalk https://www.googleapis.com/auth/userinfo.profile https://www",
      "redirectUri": "https://<WSP IP ADDRESS>/wsp/wspconnect/connect/google",
      "refreshInterval": 5
    },
    {
      "self": "http://localhost:8080/wsp/policy/107",
      "id": 107,
      "name": "LINKEDIN",
      "value": "enabled",
      "client_id": "75e2dphtredolia",
      "client_secret": "4kP61P7L7qlhX5bQfg",
      "authenticationUrl": null,
      "authScope": "r_basicprofile r_emailaddress r_network r_fullprofile rw_nus w_messages r_contactinfo",
      "redirectUri": "https://<WSP IP ADDRESS>/wsp/wspconnect/connect/linkedin",
      "refreshInterval": 5
    }
  ]
}

```

### Status codes:

- 200: Successful updation
- 404: Not Found
- 500: Internal server error

## 18 Certificate Management

---

### 18.1 Certificate Management

It provides a set of APIs to perform Certificate management related tasks like Generate Self-Signed, Certificate, Generate CSR, List Certificates, Upload Certificate, Download Certificate, Retrieve Certificate and Delete Certificate.

#### Properties:

- *organization*: Organization information ie Organization name.
- *organization Unit*: Organization Unit information ie Organization Unit name.
- *location*: Location information ie Location name.
- *state*: State information ie State name.
- *country*: Country name. Only two alphabetic capital letters are allowed.
- *email*: Email address.
- *subjectAltName*: Comma separated multiple Subject alternate names. This field generally contains other domain or IP on which certificate needs to be trusted.
- *generatorType*: The type of information required to generate.
- *component*: Component information for which certificate needs to be generated.

#### Supported generatorType

- *CERT*: related to Certificate
- *CSR*: related to CSR

#### Supported component

- *webserver*: For the webserver itself
- *webserver-trust*: For trust certificate

The supported REST APIs are:

#### 18.1.1 Generate Self-signed Certificate OR Certificate Signing Request

This API is used to generate

1. Self-signed certificate for the web-server
2. Certificate Signing Request ie CSR

#### Roles allowed:

- *ROLE\_SUPER\_ADMIN*
- *ROLE\_ADMIN*

**Request:** To generate Self-signed certificate for the web-server.

```
POST: http://<WSP IP Address>/wsp/pki/generate
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.certificate+json
    Content-type:       application/vnd.com.polycom.cloudAxis.pki+json
Body:
{
  "organization": "Polycom",
  "organizationUnit": "Cloud-Axis",
  "location": "Bangalore",
  "state": "Karnataka",
  "country": "IN",
  "email": "firstname.lastname@company.com",
  "subjectAltName": "abc.def.com,xyz.com,10.20.30.40",
  "generatorType": "CERT",
  "component": "webserver"
}
```

**Properties:**

- *generatorType*: CERT - related to Certificate
- *component*: component info for which CSR needs to be generated. e.g. webserver

**Response :**

```

HTTP/1.1 200 OK

Content-Type: application/vnd.com.polycom.cloudAxis.certificate+json

{
  "certificate": "[0]          Version: 3
    SerialNumber: 2581477293055175563
      IssuerDN: CN=A7P-00000-CKATU.asia.polycom.com,O=Polycom,OU=Cloud-Axis,L=Bangalore,ST=Karnataka,C=IN,E=chirag.katudia@polycom.com
      Start Date: Fri Jan 25 09:40:50 IST 2013
      Final Date: Thu Jan 25 09:40:50 IST 2018
      SubjectDN: CN=A7P-00000-CKATU.asia.polycom.com,O=Polycom,OU=Cloud-Axis,L=Bangalore,ST=Karnataka,C=IN,E=chirag.katudia@polycom.com
      Public Key: RSA Public Key
        modulus: b23cc178d2f65d418b359d10ee3d86d39aae2bd1151f21cc2c65539f999518b21bec6eea0b747da2d3a96887844054c23607f659d38e88cda9e
        public exponent: 10001

Signature Algorithm: SHA1WITHRSA
  Signature: 5d2b8bd5ffffbb147a26bb59e1d2390a7058d24ab
            8afb967f91d36a118361bba85de30505d254bc7e
            ec458dc2f5dda66c87384bc87ccc7070ca48fab6
            0bfc2124620c7a702a7023a96432cf86fc1fe973
            22b8e094f85d3e0331f445a3d0722f68f527d77d
            31c2c48e59e9f77350170ac736254f3f68d83309
            ad64dc16f9873da6a911635a795864c3a08e19c0
            f79e886028128c883fc64e414d8d6dd1d5214ee0
            e019544ae7f2be8102e7208e7585047035a4c9c6
            0855f021c5ef91b5260e5863b8a074aaf9e92f0b
            69f9b287b691e1b92da1204fec350b87640b5f39
            3eda6244c7ba9934e4001d95229f5640e76cdc9d
            d76caabf636e8589a6b1b6184c031b6c

  Extensions:
    critical(false) 2.5.29.35 value = Sequence
Tagged [0] IMPLICIT
  DER Octet String[20]

    critical(false) 2.5.29.14 value = DER Octet String[20]

    critical(true) BasicConstraints: isCa(false)
    critical(true) KeyUsage: 0xa0
    critical(false) 2.5.29.37 value = Sequence
ObjectIdentifier(1.3.6.1.5.5.7.3.1)
ObjectIdentifier(1.3.6.1.5.5.7.3.2)

    critical(false) 2.5.29.17 value = Sequence
Tagged [2] IMPLICIT
  DER Octet String[11]
Tagged [2] IMPLICIT
  DER Octet String[7]
Tagged [2] IMPLICIT
  DER Octet String[11]"
}

```

## Status Codes:

- 200: OK - Certificate Generated.

- 400: Bad Request with message.

**Request:** To generate CSR - Certificate Signing Request

```
POST: http://<WSP IP Address>/wsp/pki/generate
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.certificate+json
    Content-type:       application/vnd.com.polycom.cloudAxis.pki+json
Body:
{
  "organization": "Polycom",
  "organizationUnit": "Cloud-Axis",
  "location": "Bangalore",
  "state": "Karnataka",
  "country": "IN",
  "email": "firstname.lastname@company.com",
  "subjectAltName": "abc.def.com,xyz.com,10.20.30.40",
  "generatorType": "CSR",
  "component": "webserver"
}
```

### Properties:

- *generatorType*: CSR - related to CSR
- *component*: component info for which CSR needs to be generated. e.g. webserver

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.certificate+json

{
  "certificate": " -----BEGIN CERTIFICATE REQUEST-----
    MIIC+DCCAEACAQAwgbQxKTAnBgNVBAMMIEE3UC0wMDAwMCIzDS0FUVS5hc2lhLnBv
    bHlj20uY29tMRAwDgYDVQQKDAdQb2x5Y29tMRMwEQYDVQQLDAPDbG91ZC1BeGlz
    MRUwEwYDVQHDAXNb25hdGluIFZpZCcxEtAPBgNVBAGMCFNhb3NlMQswCQYD
    VQGEWJDQTEpMCCcGCSqGSIb3DQEJARYac3Jpa2FudGguaHVnYXJAcG9seWNvbS5j
    b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCPOqvUKaQVSAGm+Xv0
    39EH6eJlssuSbQHfQP2YQ3a+B9ppr7eP+AnsLtrTrFB287lSWxqykRiBgw3TElhp
    fWFLDTPDpZu5qkSyKlyakbILALQTPyW86BwD7dwzFe5QjMAEwvkJb9ZsaTX+Rhiw
    UC2ndtXy3j3i/n4SvR6xBQXwJpepTE7TH44i8tn95zFboFTQULTy6z/JD5/3uPXc
    2bUvM7Iv1zUrKEHlJWFPE/FQ7zzxeUfV+yVwFLp9LlQzcMG6tNgNCdh/FDuP9yGt
    IMDkpUdKcAgilgrollYhkB6clVcEPhDWhN5x8Nm8mrNtsdYsXCUGNOFpKAIyRlvk
    EORlAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAEYJtyIK/nkSkJQArtD3Lc77yLpi
    10tJtyPqteXIoHWba5Xnlob4XlREzODaLsEwSP4dv3pGHwUhtCTVjrzxqde2XTYk
    k+u35FQ0zOMF0rZwlkdZI+6z3z3lVdzvblR0ABH3OMCb6DNF+0sXyTdx4fybZDY2
    dxvGRcVF9o7DW1wO6jhJmtfyrmiGgrnhprh69OP3NUwzOglJZHr/M0lhh4VfnP0y
    35WWtrjaMWwv10k92NtxQ7wjs00JRF6LBH+q4q+Y/sPaQ7lHB9AotVrbN0YrdD8B
    cKWETzdnLdTMcpXdxJOaJz3Grdyvo6Z5rzDFsgPWmoP8knTSKmnWb7eY15c=
    -----END CERTIFICATE REQUEST-----"
}
```

### Status Codes:

- 200: OK - CSR Generated.
- 400: Bad Request with message.

### 18.1.2 Retrieve Component's Certificate.

This API is used to retrieve Component's Certificate which can be used for

1. Self-signed or CA-signed certificate
2. Certificate Signing Request ie CSR
3. Trust Certificate

### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

**Request:** To retrieve Self-signed or CA-signed certificate for a component.

```
GET: http://<WSP IP Address>/wsp/pki/retrieve?component=webserver&generatortype=CERT&filename=webserver
```

**HEADER DETAILS:**

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.certificate+json

**Example:**

```
generatortype=CERT  
component=webserver  
fileName=webserver
```

**Query Parameters:**

- *generatorType*: CERT - related to Certificate
- *component*: component info for which certificate is already generated. e.g. webserver
- *fileName*: Component's Certificate file name. It is always based on component name.

**Response :**

HTTP/1.1 200 OK

Content-Type: application/vnd.com.polycom.cloudAxis.certificate+json

```
{
  "certificate": "[0]          Version: 3
    SerialNumber: 2581477293055175563
      IssuerDN: CN=A7P-00000-CKATU.asia.polycom.com,O=Polycom,OU=Cloud-Axis,L=Bangalore,ST=Karnataka,C=IN,E=chirag.katudia@polycom.com
      Start Date: Fri Jan 25 09:40:50 IST 2013
      Final Date: Thu Jan 25 09:40:50 IST 2018
      SubjectDN: CN=A7P-00000-CKATU.asia.polycom.com,O=Polycom,OU=Cloud-Axis,L=Bangalore,ST=Karnataka,C=IN,E=chirag.katudia@polycom.com
      Public Key: RSA Public Key
        modulus: b23cc178d2f65d418b359d10ee3d86d39aae2bd1151f21cc2c65539f999518b21bec6eea0b747da2d3a96887844054c23607f659d38e88cda9e84b62
        public exponent: 10001

    Signature Algorithm: SHA1WITHRSA
      Signature: 5d2b8bd5ffffbb147a26bb59e1d2390a7058d24ab
                8afb967f91d36a118361bba85de30505d254bc7e
                ec458dc2f5dda66c87384bc87ccc7070ca48fab6
                0bfc2124620c7a702a7023a96432cf86fc1fe973
                22b8e094f85d3e0331f445a3d0722f68f527d77d
                31c2c48e59e9f77350170ac736254f3f68d83309
                ad64dc16f9873da6a911635a795864c3a08e19c0
                f79e886028128c883fc64e414d8d6dd1d5214ee0
                e019544ae7f2be8102e7208e7585047035a4c9c6
                0855f021c5ef91b5260e5863b8a074aaf9e92f0b
                69f9b287b691e1b92da1204fec350b87640b5f39
                3eda6244c7ba9934e4001d95229f5640e76cdc9d
                d76caabf636e8589a6b1b6184c031b6c

    Extensions:
      critical(false) 2.5.29.35 value = Sequence
    Tagged [0] IMPLICIT
      DER Octet String[20]

      critical(false) 2.5.29.14 value = DER Octet String[20]

      critical(true) BasicConstraints: isCa(false)
      critical(true) KeyUsage: 0xa0
      critical(false) 2.5.29.37 value = Sequence
    ObjectIdentifier(1.3.6.1.5.5.7.3.1)
    ObjectIdentifier(1.3.6.1.5.5.7.3.2)

      critical(false) 2.5.29.17 value = Sequence
    Tagged [2] IMPLICIT
      DER Octet String[11]
    Tagged [2] IMPLICIT
      DER Octet String[7]
    Tagged [2] IMPLICIT
      DER Octet String[11]"
}
```

### Status Codes:

- 200: OK - Certificate Retrieved .



- 400: Bad Request with message.

**Request:** To retrieve the Component's CSR.

```
GET: http://<WSP IP Address>/wsp/pki/retrieve?component=webserver&generatortype=CSR&filename=webserver
```

HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.certificate+json
Content-type:	application/vnd.com.polycom.cloudAxis.pki+json

Example:

```
{
  generatortype=CSR
  component=webserver
  filename=webserver
}
```

### Query Parameters:

- *generatorType*: CSR - related to CSR
- *component*: component info for which CSR is already generated. e.g. webserver
- *fileName*: Component's CSR file name. It is always component name.

**Response :**

```
HTTP/1.1 200 OK
```

```
Content-Type: application/vnd.com.polycom.cloudAxis.certificate+json
```

```
{
  "certificate": "-----BEGIN CERTIFICATE REQUEST-----
MIIC+DCCAeACAQAwbQxKTAnBgNVBAMMIEE3UC0wMDAwMCIzDS0FUVS5hc2lhLnBv
bHljY20uY29tMRAwDgYDVQQKDAdQb2x5Y29tMRMwEQYDVQQLDAPDbG91ZC1BeGlz
MRUwEwYDVQQHDAxNb25hdGluIFZpZCcETAPBgNVBAgMCFNhb3N1MQswCQYD
VQQGEwJQTEpMCCGCSqGSIb3DQEJARYAc3Jpa2FudGguaHVNyXJAcG9seWNVbS5j
b20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCPOqvUKaQVSAGm+Xv0
39EH6ej1ssuSbQHfQP2YQ3a+B9ppr7eP+AnsLtrTrFB2871SWxqykRiBgw3TE1hp
fWFLDTPDZu5qkSyKlyakbILALQTPyW86BwD7dwzFe5QjMAEwvkJb9ZsaTX+Rhiw
UC2nDtxy3j3i/n4SvR6xBQXwJpepTE7TH44i8tn95zFboFTQULTy6z/JD5/3uPXc
2bUvM7Iv1zUrKEH1JWFPE/FQ7zzxeUFV+yVwfLp9L1QzcMG6tNqNCdh/FDuP9yGt
IMDkpUdKcAgilgrollYhkB6clVcEphDWhN5x8Nm8mrNtsdYsXCUGN0fPKAIyRlvk
E0RlAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAEYJtyIK/nkSkJQArtd3Lc77yLpi
10tJtyPqteXIoHWba5Xnlob4X1REzODaLsEwSP4dv3pGHwUhtCTVjrzxqdE2XTYk
k+u35FQ0zOMF0rzWlkDZI+6z3z3lvDzvb1r0ABH3OMCbDNF+0sXyTdx4fybZDY2
dxvGRcVf9o7DW1wO6jhJmtfyrmiGgrnhprh69OP3NUwzOglJZHR/M0lhh4VfnP0y
35WWtrjaMWvwl0k92NtxQ7wjs00JRF6LBH+q4q+Y/sPaQ71HB9AOtVrbN0YrdD8B
cKWETzdnLdTMcpdxXJOaJz3Grdyvo6Z5rzDFsgPWmoP8knTSKmnWb7eY15c=
-----END CERTIFICATE REQUEST-----"
}
```

### Status Codes:

- 200: OK - CSR Retrieved.
- 400: Bad Request with message.

**Request:** To retrieve a Trust Certificate.

```
GET: http://<WSP IP Address>/wsp/pki/retrieve?component=webserver-trust&generatortype=CERT&filename=A7P_00000_CKATU_asia_polycom_com

HEADER DETAILS:

    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.certificate+json

Example:
{
  generatortype=CERT
  component=webserver-trust
  filename=A7P_00000_CKATU_asia_polycom_com
}
```

### Query Parameters:

- *generatorType*: CERT - related to Certificate
- *component*: Component's Trust info where CA certificates are uploaded. Naming convention is component-trust. e.g. webserver-trust.
- *fileName*: Trust Certificate file name displayed in UI or retrieved in List of Certificates.

**Response :**

HTTP/1.1 200 OK

Content-Type: application/vnd.com.polycom.cloudAxis.certificate+json

```
{
  "certificate": "[0]          Version: 3
    SerialNumber: 2581477293055175563
      IssuerDN: CN=A7P-00000-CKATU.asia.polycom.com,O=Polycom,OU=Cloud-Axis,L=Bangalore,ST=Karnataka,C=IN,E=chirag.katudia@polycom.com
      Start Date: Fri Jan 25 09:40:50 IST 2013
      Final Date: Thu Jan 25 09:40:50 IST 2018
      SubjectDN: CN=A7P-00000-CKATU.asia.polycom.com,O=Polycom,OU=Cloud-Axis,L=Bangalore,ST=Karnataka,C=IN,E=chirag.katudia@polycom.com
      Public Key: RSA Public Key
        modulus: b23cc178d2f65d418b359d10ee3d86d39aae2bd1151f21cc2c65539f999518b21bec6eea0b747da2d3a96887844054c23607f659d38e88cda9e84b62
        public exponent: 10001

    Signature Algorithm: SHA1WITHRSA
      Signature: 5d2b8bd5ffffbb147a26bb59e1d2390a7058d24ab
                8afb967f91d36a118361bba85de30505d254bc7e
                ec458dc2f5dda66c87384bc87ccc7070ca48fab6
                0bfc2124620c7a702a7023a96432cf86fc1fe973
                22b8e094f85d3e0331f445a3d0722f68f527d77d
                31c2c48e59e9f77350170ac736254f3f68d83309
                ad64dc16f9873da6a911635a795864c3a08e19c0
                f79e886028128c883fc64e414d8d6dd1d5214ee0
                e019544ae7f2be8102e7208e7585047035a4c9c6
                0855f021c5ef91b5260e5863b8a074aaf9e92f0b
                69f9b287b691e1b92da1204fec350b87640b5f39
                3eda6244c7ba9934e4001d95229f5640e76cdc9d
                d76caabf636e8589a6b1b6184c031b6c

    Extensions:
      critical(false) 2.5.29.35 value = Sequence
    Tagged [0] IMPLICIT
      DER Octet String[20]

      critical(false) 2.5.29.14 value = DER Octet String[20]

      critical(true) BasicConstraints: isCa(false)
      critical(true) KeyUsage: 0xa0
      critical(false) 2.5.29.37 value = Sequence
    ObjectIdentifier(1.3.6.1.5.5.7.3.1)
    ObjectIdentifier(1.3.6.1.5.5.7.3.2)

      critical(false) 2.5.29.17 value = Sequence
    Tagged [2] IMPLICIT
      DER Octet String[11]
    Tagged [2] IMPLICIT
      DER Octet String[7]
    Tagged [2] IMPLICIT
      DER Octet String[11]"
}
```

### Status Codes:

- 200: OK - Certificate Retrieved .

- 400: Bad Request with message.

### 18.1.3 Download Component's Certificate

This API is used to download Component's Certificate which can be used for

1. Self-signed or CA-signed certificate
2. Trust Certificate

#### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

**Request:** To download Self-signed or CA-signed certificate for a component.

```
GET: http://<WSP IP Address>/wsp/pki/download?component=<COMPONENT>&generatortype=<TYPE>&filename=<FILENAME>

HEADER DETAILS:

    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:             <Auth token obtained after authentication>
    Accept:                 text/plain

Example:
{
  generatortype=CERT
  component=webserver
  filename=webserver
}
```

#### Query Parameters:

- *generatorType*: CERT - related to Certificate
- *component*: component info for which certificate is already generated. e.g. webserver
- *fileName*: Component's Certificate file name. It is always based on component name.

#### Response :

```
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Disposition: attachment; filename="webserver.der"

Body:
  Binary certificate
```

#### Status Codes:

- 200: OK - Certificate Retrieved .
- 400: Bad Request with message.

**Request:** To download Trust Certificate.

```
GET: http://<WSP IP Address>/wsp/pki/download?component=<COMPONENT>&generatortype=<TYPE>&filename=<FILENAME>
```

#### HEADER DETAILS:

```
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             text/plain
```

#### Example:

```
generatorType=CERT
component=webserver-trust
fileName=A7P_00000_CKATU_asia_polycom_com
}
```

### Query Parameters:

- *generatorType*: CERT - related to Certificate
- *component*: Component's Trust info where CA certificates are uploaded. Naming convention is component-trust. e.g. webserver-trust.
- *fileName*: Trust Certificate file name displayed in UI or retrieved in List of Certificates.

### Response :

```
HTTP/1.1 200 OK
```

```
Content-Type: text/plain
```

```
Content-Disposition: attachment; filename="A7P_00000_CKATU_asia_polycom_com.der"
```

#### Body:

```
Binary certificate
```

### Status Codes:

- 200: OK - Certificate Retrieved .
- 400: Bad Request with message.

#### 18.1.4 List Certificates

Displays list of the certificates.

#### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>:8080/wsp/pki/list
```

#### HEADER DETAILS:

```
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.pkicollection+json
```

### Response :

```

HTTP/1.1 200 OK
Content-type: application/vnd.com.polycom.cloudAxis.pkicollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "pki": [
    {
      "organization": null,
      "organizationUnit": null,
      "location": null,
      "state": null,
      "country": null,
      "email": null,
      "subjectAltName": null,
      "component": "webserver",
      "generatorType": "CERT",
      "fileName": "webserver",
      "fileExtension": null
    },
    {
      "organization": null,
      "organizationUnit": null,
      "location": null,
      "state": null,
      "country": null,
      "email": null,
      "subjectAltName": null,
      "component": "webserver-trust",
      "generatorType": "CERT",
      "fileName": "A7P_00000_SHUGA_asia_polycom_com",
      "fileExtension": null
    }
  ]
}

```

**Status Codes:**

- 200: OK - Certificate Retrieved .
- 400: Bad Request with message.

**18.1.5 Delete Certificate**

Deletes the given certificate.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

**Request:**

```
DELETE: http://<WSP IP ADDRESS>/wsp/pki/delete?component=<COMPONENT>&filename=<FILENAME>
HEADER DETAILS:
    X-CA-UserName          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
    X-CA-Token             <Auth token obtained after authentication>

Example:
    component=webserver-trust
    fileName=A7P_00000_SHUGA_asia_polycom_com"
}
```

**Response :**

```
HTTP/1.1 200 OK
```

**Status Codes:**

- 200: OK - Certificate deleted .
- 400: Bad Request with message.

**18.1.6 Upload Certificate**

Upload the given certificate.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

**Request:**

```
POST: http://<WSP IP ADDRESS>/wsp/pki/upload?component=<COMPONENT>
HEADER DETAILS:
    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
    X-CA-Token:             <Auth token obtained after authentication>
    Content-type:           multipart/form-data

Example:
    component=webserver
}
```

**Response :**

```
HTTP/1.1 200 OK
```

**Status Codes:**

- 200: OK - Certificate Uploaded .
- 400: Bad Request with message.

## 19 Product Version Management

---

### 19.1 Product Version

Provides API to retrieve product version information.

#### Properties:

- *productVersion*: product version number
- *productName*: product name
- *productDescription*: product description

The supported REST APIs are:

#### 19.1.1 Get Product Version Number

##### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

##### Request:

```
GET: http://<WSP IP Address>/wsp/productversion
HEADER DETAILS:
    Accept:          application/vnd.com.polycom.cloudAxis.system.version+json
```

##### Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.system.version+json
Body:
{
    "productVersion": "1.0.0-SNAPSHOT",
    "productName": "CloudAxis Portal",
    "productDescription": "CloudAxis Portal"
}
```

##### Status codes:

- 200: Successful read
- 500: Internal Server Error
- 400: Invalid request



## 20 License Management

### 20.1 License Management REST APIs using Flexera Server

It provides API to get License related information, Activate/Deactivate Licenses, Generate/Download/Delete Activation Requests and Configure System for MEA for product/(s) and feature/(s).

*Properties:*

- *id*: Unique ID for each license.
- *product*: Name of the product like WSP/MEA
- *status*: Status of the license ACTIVATED/DEACTIVATED/TRIAL/EXPIRED/REVOKED
- *solutionMode*: The license can be activated in either Standalone Mode or Solution Mode (with Platform Director ie PD).
- *activationKey*: License Key which is used to activate the license.
- *activationDate*: Date on which license got activated.
- *hostId*: Unique ID of the system.
- *licenseType*: License type like PRODUCT/FEATURE
- *version*: Product version
- *daysBeforeExpiry*: Only when product is in Trial mode. It shows number of days left for Trial period to expire.
- *expiryDate*: Date when license is expiring.
- *featureType*: Type of the feature. Applicable only when licenseType is FEATURE.
- *featureCapacity*: Capacity of the feature. Applicable only when licenseType is FEATURE.
- *featureCapacityBuffer*: Feature capacity buffer if any. Applicable only when licenseType is FEATURE.

The supported REST APIs are:

#### 20.1.1 Get License Information

This API is used to list all available licenses for all products in the CloudAxis. To get product specific License information it supports query parameters ie PRODUCT.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: https://<IP Address>/platform/licenses?PRODUCT=<PRODUCT_NAME>

HEADER DETAILS:

X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.platform.licensecollection+json
```

**Query Parameters:**

- *PRODUCT*: To get product specific license information. Supported query parameter values are WSP and MEA.

**Response :**

HTTP/1.1 200 OK

```
{
  "licenseServer": "https://flexera.server.com/control/pycm/deviceservices",
  "licenseServerPort": null,
  "solutionMode": false,
  "licenses":[
    {
      "id": 10,
      "version": "1.3.0.198-119088",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "WSP",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/20/2013",
      "activationMode": "OFFLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 20,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 21,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": "50",
      "featureCapacityBuffer": "10",
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "FEATURE",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": "MEA_ATTENDEES",
      "gracePeriod": "30"
    },
    {
      "id": 22,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
```

**Status Codes:**

- 200: Successful read
- 500: Internal Server Error
- 404: If the request is not a valid request

**20.1.2 Activate license - Online Mode**

This API is used to activate the product and its feature. License can be activated for multiple products/features simultaneously. Since this is Online Mode of activating the license, only Activation key is required to activate the license. Except id none of the JSON object record can be null in the request. Id would be null only in case of new MEA\_ATTENDEES license.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```

POST: https://<IP Address>/platform/licenses/activation/online
HEADER DETAILS:
  X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
  X-CA-Token:         <Auth token obtained after authentication>
  Content-type:       application/vnd.com.polycom.cloudAxis.platform.licensecollection+json
  Accept:             application/vnd.com.polycom.cloudAxis.platform.licensecollection+json
Body:
{
  "licenses":[
    {
      "id":"283950",
      "product":"WSP",
      "activationKey":"1015fa79-f37b-4f47-b2cb-d5bb18ce04a0",
      "hostId":"6CB97A68",
      "licenseType":"PRODUCT",
      "version":"1.3.0.198-119088"
    },
    {
      "id":"38793805",
      "product":"MEA",
      "activationKey":"1015fa79-f37b-4f47-b2cb-d5bb18ce04a0",
      "hostId":"90EE069CE545",
      "licenseType":"PRODUCT",
      "version":"1.3.0.198-119088"
    },
    {
      "id":"4458792",
      "product":"MEA",
      "activationKey":"2222fa79-f37b-4f47-b2cb-d5bb18ce04a0",
      "hostId":"90EE069CE545",
      "licenseType":"FEATURE",
      "version":"1.3.0.198-119088",
      "featureType":"MEA_ATTENDEES"
    },
    {
      "id":"8458798",
      "product":"MEA",
      "activationKey":"2222fa79-f37b-4f47-b2cb-d5bb18ce04a0",
      "hostId":"90EE069CE545",
      "licenseType":"FEATURE",
      "version":"1.3.0.198-119088",
      "featureType":"MEA_ATTENDEES"
    }
  ]
}

```

### Properties:

- *id*: Licenseid which can be obtained using List Licenses API.
- *product*: Product name ie WSP or MEA.
- *activationKey*: Key to activate the license.
- *hostId*: Unique ID of the system - provided in GET API response.

- *licenseType*: PRODUCT / FEATURE
- *version*: Version of the product
- *featureType*: for which particular feature of product. Only when licenseType = FEATURE.

**Response :**

```

HTTP/1.1 200 OK
{
  "licenseServer": "https://flexera.server.com/control/pycm/deviceservices",
  "licenseServerPort": null,
  "solutionMode": false,
  "licenses":[
    {
      "id": 10,
      "version": "1.3.0.198-119088",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "WSP",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/20/2013",
      "activationMode": "OFFLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 20,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 21,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": "50",
      "featureCapacityBuffer": "10",
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "FEATURE",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": "MEA_ATTENDEES",
      "gracePeriod": "30"
    },
    {
      "id": 22,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",

```

**Status Codes:**

- 200: Successful activation
- 400: Activation failed
- 500: Internal Server Error

**20.1.3 Activate license - Offline Mode**

This API is used to activate the license for product and its feature in Offline Mode. Multiple licenses can be activated in one request. Since this is Offline Mode of activating the license, Activation key and Activation Key File are required to activate the license. The pre-requisite of this request is to have the 'Activation Key File' which can be obtained as follows.

1. Download the 'Activation Request File' using the "Activation Key". A separate API mentioned below is used for this.
2. Get the corresponding 'Activation Key File' in exchange to 'Activation Request File' using Flexera Server.

There must be only one multipart record in one request. The multipart key will be the combination of product name and license id as defined below. The Value of this key would be corresponding 'Activation Key File'.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request :**

POST: https://<IP Address>/platform/licenses/activation/offline

**HEADER DETAILS:**

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.platform.licensecollection+json
Content-type:	multipart/form-data

MultiParts: Each multipart key should be prefixed with product name. Eg. the license key for the WSP product license would be WSP-<licenseid>

Below are the examples to construct the Multipart key/value pairs:

1. key=WSP-10, Value=Attachment of activationFile. This can be a Consolidated Activation File of one or more licenses.
2. key=MEA-20, Value=Attachment of activationFile. This can be a Consolidated Activation File of one or more licenses.
3. key=MEA\_ATTENDEES-21, Value=Attachment of activationFile. This can be a Consolidated Activation File of one or more licenses.

**Response :**

```

HTTP/1.1 200 OK
{
  "licenseServer": "https://flexera.server.com/control/pycm/deviceservices",
  "licenseServerPort": null,
  "solutionMode": false,
  "licenses":[
    {
      "id": 10,
      "version": "1.3.0.198-119088",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "WSP",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/20/2013",
      "activationMode": "OFFLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 20,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 21,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": "50",
      "featureCapacityBuffer": "10",
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "FEATURE",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": "MEA_ATTENDEES",
      "gracePeriod": "30"
    },
    {
      "id": 22,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",

```



**Status Codes:**

- 200: Successful Offline activation
- 400: Activation Offline failed
- 500: Internal Server Error

**20.1.4 Deactivate License - Online Mode**

This API is used to deactivate the license for product or its feature in Online Mode. License can be deactivated for one product/feature at a time. The Body will be empty in the request.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
POST: https://<IP Address>/platform/licenses/{licenseid}/deactivation/online
HEADER DETAILS:
  X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
  X-CA-Token:         <Auth token obtained after authentication>
  Accept:             application/vnd.com.polycom.cloudAxis.platform.licensecollection+json
Body:
{
}
```

**Path Parameter:**

- *licenseid*: License ID of the product/feature. This ID is what is listed in the GET License API response.

**Response :**

```

HTTP/1.1 200 OK
{
  "licenseServer": "https://flexera.server.com/control/pycm/deviceservices",
  "licenseServerPort": null,
  "solutionMode": false,
  "licenses":[
    {
      "id": 10,
      "version": "1.3.0.198-119088",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "WSP",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/20/2013",
      "activationMode": "OFFLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 20,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 21,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": "50",
      "featureCapacityBuffer": "10",
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "FEATURE",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": "MEA_ATTENDEES",
      "gracePeriod": "30"
    },
    {
      "id": 22,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",

```

**Status Codes:**

- 200: Successful Online Deactivation
- 400: Online Deactivation failed
- 500: Internal Server Error

**20.1.5 Deactivate License - Offline Mode**

This API is used to deactivate the license for product or its feature in Offline Mode. License can be deactivated for one product/feature at a time. The Body will be empty in the request.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

POST: `https://<IP Address>/platform/licenses/{licenseid}/deactivation/offline`

**HEADER DETAILS:**

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.platform.licensecollection+json
Content-type:	multipart/form-data

MultiParts: Each multipart key should be prefixed with product name. Eg. the license key for the WSP product license would be WSP-<licenseid>

Below are the examples to construct the Multipart key/value pairs:

1. key=WSP-10, Value=Attachment of activationFile
2. key=MEA-20, Value=Attachment of activationFile
3. key=MEA\_ATTENDEES-21, Value=Attachment of activationFile

**Path Parameter:**

- *licenseid*: License ID of the product/feature. This ID is what is listed in the GET License API response.

**Response :**

```

HTTP/1.1 200 OK
{
  "licenseServer": "https://flexera.server.com/control/pycm/deviceservices",
  "licenseServerPort": null,
  "solutionMode": false,
  "licenses":[
    {
      "id": 10,
      "version": "1.3.0.198-119088",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "WSP",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/20/2013",
      "activationMode": "OFFLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 20,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 21,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": "50",
      "featureCapacityBuffer": "10",
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "FEATURE",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": "MEA_ATTENDEES",
      "gracePeriod": "30"
    },
    {
      "id": 22,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",

```

**Status Codes:**

- 200: Successful Offline Deactivation
- 400: Deactivation Offline failed
- 500: Internal Server Error

**20.1.6 Generate Activation Request - Offline Mode**

This API is used to generate the Activation Request for product or feature license to be activated. This is required only in case of Offline Activation mode. With this API the activation record will be created in the DB. With a separate Download API the consolidated Activation File can be downloaded in binary format. This API does not validate the activationKey since in Offline Activation Mode it does not contact the Flexera Server while issuing the Activation Request File. Nevertheless, the client is expected to validate the key format. In case the client generates the Activation Request record for a wrong key and hence downloads the wrong activation file, it would be rejected by the Flexera Server while requesting for an 'Activation Key File' in exchange to wrong 'Activation Request File'.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

POST: https://<IP Address>/platform/licenses/generate/activationrequest

HEADER DETAILS:

X-CA-UserName: <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn\_user>  
 X-CA-Token: <Auth token obtained after authentication>  
 Accept: application/vnd.com.polycom.cloudAxis.platform.licensecollection+json  
 Content-type: application/vnd.com.polycom.cloudAxis.platform.licensecollection+json

Body:

```
{
  "licenses":[
    {
      "id":"10",
      "product":"WSP",
      "activationKey":"4EXX-37XX-C4XX-ABXX",
      "hostId":"abcd-wsp-hostid-1",
      "licenseType":"PRODUCT",
      "version":"1.3.0.198-119088"
    },
    {
      "id":"20",
      "product":"MEA",
      "activationKey":"4EXX-37XX-C4XX-ABXX",
      "hostId":"abcd-mea-hostid-1",
      "licenseType":"PRODUCT"
    },
    {
      "id":"21",
      "product":"MEA",
      "activationKey":"4EXX-37XX-C4XX-ABXX",
      "hostId":"abcd-mea-hostid-1",
      "licenseType":"FEATURE"
    }
  ]
}
```

**Response :**

```

HTTP/1.1 200 OK
{
  "licenseServer": "https://flexera.server.com/control/pycm/deviceservices",
  "licenseServerPort": null,
  "solutionMode": false,
  "licenses":[
    {
      "id": 10,
      "version": "1.3.0.198-119088",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "WSP",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/20/2013",
      "activationMode": "OFFLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 20,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 21,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": "50",
      "featureCapacityBuffer": "10",
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "FEATURE",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": "MEA_ATTENDEES",
      "gracePeriod": "30"
    },
    {
      "id": 22,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",

```

**Status Codes:**

- 200: Successfully Generated the Activation Request
- 400: Generate Activation Request failed
- 500: Internal Server Error

**20.1.7 Download Activation Request File - Offline Mode**

This API is used to download the Activation Request File for product or feature license to be activated. This is required only in case of Offline Activation mode. This API is called after Generate Activation Request API which creates record/(s) in the CloudAxis. In case the client downloads the Activation Request File for a wrong key record created by above API, it would be rejected by the Flexera Server while requesting for an 'Activation Key File' in exchange to wrong 'Activation Request File'.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: https://<IP Address>/platform/licenses/{licenseid}/download/activationrequest?USERNAME=admin&TOKEN=63D1F5D9191E3CAC-558DB400-90517BF1-E
```

**Query Parameters:**

- **USERNAME:** UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn\_username@domain.com. The USERNAME must have a Super-Admin role.
- **TOKEN:** The token is a One Time Token(OTT) which can be obtained from a separate API [https:// IP Address/wsp/platformManagement/ott](https://IP Address/wsp/platformManagement/ott) along with headers X-CA-UserName & X-CA-Token.

**Path Parameters:**

- **licenseid:** License ID of the product/feature. This ID is what is listed in the GET License API response.

**Response :**

```
HTTP/1.1 200 OK
```

**Status Codes:**

- 200: Successful Download of Activation Request File
- 400: Download Activation File failed
- 500: Internal Server Error

**20.1.8 Delete Pending Activation Request - Offline Mode**

This API is used to delete the pending activation request. Every time a Download Activation Request API is used, it creates a new license record in the WSP. The status of this license record is PENDING. This API would be required when the Admin has entered the wrong key while downloading the Activation Request File and wants to clean the Pending Activation Request. While getting the licenseId from List Licenses API, make sure that the license record status is PENDING.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**



```
POST: https://<IP Address>/platform/licenses/{licenseid}/delete/pendingactivation
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.platform.licensecollection+json
Body:
{
}
```

**Path Parameters:**

- *licenseid*: License ID of the product/feature. This ID is what is listed in the GET License API response.

**Response :**

```

HTTP/1.1 200 OK
{
  "licenseServer": "https://flexera.server.com/control/pycm/deviceservices",
  "licenseServerPort": null,
  "solutionMode": false,
  "licenses":[
    {
      "id": 10,
      "version": "1.3.0.198-119088",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "WSP",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/20/2013",
      "activationMode": "OFFLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 20,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": null,
      "featureCapacityBuffer": null,
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "PRODUCT",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": null,
      "gracePeriod": "30"
    },
    {
      "id": 21,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",
      "daysBeforeExpiry": null,
      "featureCapacity": "50",
      "featureCapacityBuffer": "10",
      "expiryDate": null,
      "activationKey": "97XX-87XX-62XX-ClXX",
      "product": "MEA",
      "hostId": "423065DE-1679-901F-AEE8-8E97EB30568C",
      "licenseType": "FEATURE",
      "statusDate": "06/14/2014",
      "activationMode": "ONLINE",
      "featureType": "MEA_ATTENDEES",
      "gracePeriod": "30"
    },
    {
      "id": 22,
      "version": "1.2.1.9886587",
      "status": "ACTIVATED",

```

**Status Codes:**

- 200: Successful Delete of Pending Activation Request
- 400: Delete of Pending Activation Request failed
- 500: Internal Server Error

**20.1.9 Configure System Details**

This API is required to configure system details which will be used to activate the license. MEA calls this API to provide details to WSP which is used by WSP to activate license for MEA.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request :**

```
POST: https://<IP Address>/platform/licenses/systemconfig
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.platform.license+json
Body:
{
    "product"="MEA",
    "hostId"="123456789",
    "version"="1.2.1.9886587"
}
```

**Properties:**

- *product*: Product name. Since MEA calls this API, so product name would be MEA.
- *hostId*: Unique ID of the system - provided in GET API response.
- *version*: Product version

**Response:**

```
HTTP/1.1 200 OK
```

**Status Codes:**

- 200: Successfully configured
- 400: Configuration failed
- 500: Internal Server Error

## 21 NTP Configuration Management

### 21.1 Network Time Protocol (NTP) APIs:

Provides APIs for NTP related tasks.

#### Properties:

- *ntp-server*: NTP Server ip or fqdn. \* *timeZone*: Selected timezone. \* *datetime*: Date time of the server.

**Mandatory Properties:** ntp-server, timeZone

The Supported REST API's are :

#### 21.1.1 GET NTP details

Lists all of configured NTP servers and also provides latest NTP date and time

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/platformManagement/system/ntp
HEADER DETAILS:
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.system.ntp+json
```

#### Query Parameters:

- *validate*: This query parameter is optional and its value is true by default. If set to false, The NTP server list will be checked if each server is reachable.

#### Response :

```
HTTP/1.1 200 OK
{
  "ntpServerList": [
    {"ntp-server": "<server name>/<server ip>"},
    {"ntp-server": "<server name>/<server ip>"},
    {"ntp-server": "<server name>/<server ip>"}
  ],
  "timeZone": "timezone"
  "datetime": "<date, time and timezone>"
}
```

#### Status codes:

- 500: Internal Server Error
- 200: Request is successful
- 401 : Unauthorized if CA-Token is invalid

### 21.1.2 Modify the NTP server, Timezone details

Allows user to configure NTP servers and optionally user can also provide current system date and time.

#### Request:

```
PUT: http://<WSP IP Address>/wsp/platformManagement/system/ntp?validate=false
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-Type:       application/vnd.com.polycom.cloudAxis.system.ntp+json
Body:
{
  "ntpServerList": [{ "ntp-server": "<server name>/<server ip>" },
    { "ntp-server": "<server name>/<server ip>" },
    { "ntp-server": "<server name>/<server ip>" } ],
  "timeZone": "<timeZone>"
  "datetime": "<date, time and time zone>"
}
```

#### Query Parameters:

- *validate*: This query parameter is optional and its value is true by default. If set to false, The NTP server list will be checked if each server is reachable.

#### Response :

```
HTTP/1.1 201 CREATED
```

#### Status codes:

- 500: Internal Server Error
- 201: NTP server list is created
- 401 : Unauthorized if CA-Token is invalid

### 21.1.3 GET TimeZone List

Lists the timezones that can be configured for the system

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/platform/timeZones
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudaxis.timezones+json
```

#### Response :

```
HTTP/1.1 200 OK
```

```
{
  "timeZones": [
    "Africa_Abidjan",
    "Africa_Accra",
    "Africa_Addis_Ababa",
    "Africa_Algiers",
    "Africa_Asmara",
    "Africa_Asmera",
    "Africa_Bamako",
    "Africa_Bangui",
    "Africa_Banjul",
    "Africa_Bissau",
    "Africa_Blantyre",
    "Africa_Brazzaville",
    "Africa_Bujumbura",
    "Africa_Cairo",
    "Africa_Casablanca",
    "Africa_Ceuta",
    "Africa_Conakry",
    "Africa_Dakar",
    "Africa_Dar_es_Salaam",
    "Africa_Djibouti",
    "Africa_Douala",
    "Africa_El_Aaiun",
    "Africa_Freetown",
    "Africa_Gaborone",
    "Africa_Harare",
    "Africa_Johannesburg",
    "Africa_Juba",
    "Africa_Kampala",
    "Africa_Khartoum",
    "Africa_Kigali",
    "Africa_Kinshasa",
    "Africa_Lagos",
    "Africa_Libreville",
    "Africa_Lome",
    "Africa_Luanda",
    "Africa_Lubumbashi",
    "Africa_Lusaka",
    "Africa_Malabo",
    "Africa_Maputo",
    "Africa_Maseru",
    "Africa_Mbabane",
    "Africa_Mogadishu",
    "Africa_Monrovia",
    "Africa_Nairobi",
    "Africa_Ndjamena",
    "Africa_Niamey",
    "Africa_Nouakchott",
    "Africa_Ouagadougou",
    "Africa_Porto_Novo",
    "Africa_Sao_Tome",
    "Africa_Timbuktu",
    "Africa_Tripoli",
    "Africa_Tunis",
    "Africa_Windhoek",
    "America_Adak",
    "America_Anchorage",
    "America_Anguilla",
    "America_Antigua",
```

**Status codes:**

- 500: Internal Server Error
- 200: Request is successful
- 401 : Unauthorized if CA-Token is invalid

## 22 Logging Management

---

### 22.1 Logging APIs:

Provides APIs to perform logging related tasks.

Logging is a critical debugging tool for any application. The following log levels are supported in WSP : ALL, TRACE, DEBUG, INFO, WARN, ERROR.

The supported REST APIs are :

#### 22.1.1 GET all supported logging levels

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/wsp/platformManagement/system/log/levels
HEADER DETAILS:
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.system.logcollection+json
```

**Response :**



```

HTTP/1.1 200 OK
{
  "statistics": null,
  "prev": null,
  "next": null,
  "logLevel": [
    {
      "logLevel": "ALL"
    },
    {
      "logLevel": "TRACE"
    },
    {
      "logLevel": "DEBUG"
    },
    {
      "logLevel": "INFO"
    },
    {
      "logLevel": "WARN"
    },
    {
      "logLevel": "ERROR"
    },
    {
      "logLevel": "OFF"
    }
  ]
}

```

**Status codes:**

- 500: Internal Server Error
- 200: Request is successful
- 401 : Unauthorized if CA-Token is invalid

**22.1.2 GET current Log level****Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/wsp/platformManagement/system/log
```

**HEADER DETAILS:**

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.system.log+json

**Response :**

```
HTTP/1.1 200 OK
{
  "logLevel": "WARN"
}
```

**Status codes:**

- 500: Internal Server Error
- 200: Request is successful
- 401 : Unauthorized if CA-Token is invalid

**22.1.3 PUT level of logging****Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
PUT: http://<WSP IP Address>/wsp/platformManagement/system/log
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-Type:       application/vnd.com.polycom.cloudAxis.system.log+json
Body:
{
  "logLevel": "DEBUG"
}
```

**Response :**

```
HTTP/1.1 200 OK
```

**Status codes:**

- 500: Internal Server Error
- 204: Level of logging set
- 401 : Unauthorized if CA-Token is invalid

**22.1.4 Download logs**

Allows user to download all log files consolidated in single zip file.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/wsp/platformManagement/system/log/download?type=all
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-Type:       application/vnd.com.polycom.cloudAxis.system.log+json
    Accept:             application/zip
```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/zip
Content-Disposition: attachment; filename=log_file_name.zip
Body:
    XML file
```

**Status codes:**

- 500: Internal Server Error
- 200: Success
- 401 : Unauthorized if CA-Token is invalid

## 23 Conference Settings

---

### 23.1 Conference Settings Service

Provides APIs to retrieve and update the default conference settings.

Conference Settings resource stores the centralized properties to handle a conference.

#### Properties::

- **id**: Internal id for conference settings.
- **passcodeMandatory**: This indicates whether attendee passcode is mandatory or not for the conference.
- **chairpersonPasscodeMandatory**: This indicates whether chairperson passcode is mandatory or not for the conference.
- **adHocDurationInMin**: The duration of all the ad-hoc meetings created.
- **bufferBeforeStartMeetingInMin**: Buffer time before the start of meeting.
- **bufferAfterEndMeetingInMin**: Buffer time after the meeting end time.
- **allowUseOfPersonalVmr**: Is the use of personal VMR while creating a meeting allowed.
- **allowUseOfJoinBridge**: Is the use of Join bridge allowed.
- **exposePasscode**: Should the passcode be exposed in mail/URI
- **sendOnlyCalendarInvite**: By default, when false, an e-mail is sent with a calendar invite (\*.ics) as an attachment.

The supported REST APIs are:

#### 23.1.1 List the settings

##### Roles allowed:

- **ROLE\_SUPER\_ADMIN**
- **ROLE\_ADMIN**
- **ROLE\_USER**

##### Request:

```
GET: http://<WSP IP Address>/wsp/confsettings/
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.conferencesettings+json
```

##### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.conferencesettings+json
{
  "self": "http://localhost:81/wsp/confsettings/104",
  "id": "104",
  "passcodeMandatory": false,
  "adHocDurationInMin": 220,
  "bufferBeforeStartMeetingInMin": 20,
  "bufferAfterEndMeetingInMin": 10,
  "allowUseOfPersonalVmr": false,
  "allowUseOfJoinBridge": false,
  "exposePasscode": true,
  "sendOnlyCalendarInvite": true,
  "chairpersonPasscodeMandatory": false
}

```

**Status codes:**

- 200: Successful listing
- 500: Internal Server Error

**23.1.2 Update Settings****Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```

PUT: http://<WSP IP Address>/wsp/confsettings/104
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.conferencesettings+json
Body:
{
  "passcodeMandatory": false,
  "adHocDurationInMin": "220",
  "bufferBeforeStartMeetingInMin": 20,
  "bufferAfterEndMeetingInMin": 10,
  "allowUseOfPersonalVmr": true,
  "allowUseOfJoinBridge": true,
  "exposePasscode": true,
  "sendOnlyCalendarInvite": true,
  "chairpersonPasscodeMandatory": true
}

```

**Response :**

```

HTTP/1.1 204 No Content

```

**Status codes:**

- 204: Successful update

- 404: settings not found
- 400: Invalid request
- 500: Internal server error

## 24 Localization Management

### 24.1 Localization Management

Provides API to perform CRUD operations for localization.

#### Properties:

- *id*: internal id for localization.
- *langPackVersion*: version number of the language pack.
- *active*: Boolean flag to suggest whether the language pack is active.

The supported REST APIs are:

#### 24.1.1 List language packs

##### Roles allowed:

- ROLE\_ADMIN
- ROLE\_SUPER\_ADMIN

##### Request:

```
GET: http://<WSP IP Address>/wsp/language-packs

HEADER DETAILS:

X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.languagepackcollection+json
```

##### Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.languagepackcollection+json

{
  "statistics": null,
  "prev": null,
  "next": null,
  "languagePacks": [
    {
      "self": "http://<WSP IP Address>/wsp/language-packs/1.3.0_v2",
      "id": "1.3.0_v2",
      "langPackVersion": "1.3.0_v2",
      "active": false
    },
    {
      "self": "http://<WSP IP Address>/wsp/language-packs/1.3.0_v3",
      "id": "1.3.0_v3",
      "langPackVersion": "1.3.0_v3",
      "active": true
    }
  ]
}
```

**Status codes:**

- 200: Successful read
- 500: Internal Server Error

**24.1.2 Deploy Language Package****Roles allowed:**

- ROLE\_ADMIN
- ROLE\_SUPER\_ADMIN

**Request:**

```
POST: http://<WSP IP Address>/wsp/language-packs

HEADER DETAILS:

    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.languagepack+json
    Content-Type:       multipart/form-data

FORM PARAMETERS:

    file                <Language Package in zip format>
```

**Response :**

```
HTTP/1.1 201 Created
Location: https://<WSP IP Address>/wsp/language-packs/1.3.0_v3

{
  "self": "https://<WSP IP Address>/wsp/language-packs/1.3.0_v3",
  "id": "1.3.0_v3",
  "langPackVersion": "1.3.0_v3",
  "active": true
}
```

**Status codes:**

- 201: Successful Language upload
- 400: Invalid request
- 500: Internal server error

**24.1.3 Rollback to Previous version****Roles allowed:**

- ROLE\_ADMIN
- ROLE\_SUPER\_ADMIN

**Request:**



```

POST: http://<WSP IP Address>/wsp/language-packs/rollback
HEADER DETAILS:
    X-CA-UserName          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token             <Auth token obtained after authentication>

```

**Response :**

```
HTTP/1.1 204 No Content
```

**Status codes:**

- 201: Successful rollback operation
- 400: Invalid request
- 500: Internal server error

**24.1.4 Get Language Pack Details****Roles allowed:**

- ROLE\_ADMIN
- ROLE\_SUPER\_ADMIN

**Request:**

```

GET: http://<WSP IP Address>/wsp/language-packs/1.3.0_v2
HEADER DETAILS:
    X-CA-UserName:          <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:             <Auth token obtained after authentication>
    Accept:                 application/vnd.com.polycom.cloudAxis.languagepack+json

```

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.languagepack+json
{
    "self": "http://localhost:8080/wsp/language-packs/1.3.0_v2",
    "id": "1.3.0_v2",
    "langPackVersion": "1.3.0_v2",
    "active": false
}

```

**Status codes:**

- 200: Successful read
- 404: Language pack does not exists
- 500: Internal Server Error

**24.1.5 Get supported languages****Properties:**

- *id*: Internal id for the language pack

- *langPackVersion*: Version number of the language pack
- *locale*: Locale of the language
- *copyright*: copyright info
- *description*: More details for the supported language in the language pack
- *displayName*: User friendly display name for the supported language

**Roles allowed:**

- ROLE\_ADMIN
- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: http://<WSP IP Address>/wsp/languages
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.languagecollection+json
```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.languagecollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "languages": [
    {
      "self": "http://localhost:8080/wsp/languages/en",
      "id": "en",
      "langPackVersion": "1.3.0_v1",
      "locale": "en",
      "copyright": null,
      "description": "Localized strings in english",
      "displayName": "English"
    },
    {
      "self": "http://localhost:8080/wsp/languages/fr",
      "id": "fr",
      "langPackVersion": "1.3.0_v1",
      "locale": "fr",
      "copyright": null,
      "description": "Localized strings in French",
      "displayName": "French"
    }
  ]
}
```

**Status codes:**

- 200: Successful read

- 500: Internal Server Error

### 24.1.6 Get language details

#### Roles allowed:

- ROLE\_ADMIN
- ROLE\_SUPER\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/languages/en
```

##### HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.language+json

#### Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.language+json
{
  "self": "http://localhost:8080/wsp/languages/en",
  "id": "en",
  "langPackVersion": "1.3.0_v1",
  "locale": "en",
  "copyright": null,
  "description": "Localized strings in english",
  "displayName": "English"
}
```

#### Status codes:

- 200: Successful read
- 500: Internal Server Error

## 25 Proxy Configuration

### 25.1 Proxy Config Service

Provides APIs to retrieve and update proxy configuration.

Proxy config is required when WSP and MEA are behind a proxy environment and forward proxy is configured.

#### Properties:

- *server*: Proxy Server IP.
- *port*: Proxy Server Port
- *authenticated*: True if proxy server requires credentials, else false.
- *username*: Username to be authenticated for proxy. To be provided if authenticated = true.
- *password*: Password to be authenticated for proxy. To be provided if authenticated = true.
- *scheme*: Placeholder for type of authentication - BASIC (by default) or NTLM. For future use, not used currently.

**Mandatory Properties:** server, port, authenticated

The supported REST APIs are:

#### 25.1.1 List the settings

##### Roles allowed:

- ROLE\_SUPER\_ADMIN

##### Request:

```
GET: http://<WSP IP Address>/platform/proxyconfig/
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.platform.proxyconfig+json
```

##### Response :

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.platform.proxyconfig+json
{
  "self": "http://localhost:81/platform/proxyconfig/104",
  "id": "104",
  "server": "172.30.14.5",
  "port": "8080",
  "authenticated": true,
  "username": "username",
  "password": "password",
  "scheme": null
}
```

##### Status codes:

- 200: OK - Successful

- 500: Internal Server Error

### 25.1.2 Update Settings

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
PUT: http://<WSP IP Address>/platform/proxyconfig/104
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.platform.proxyconfig+json
Body:
{
  "server": "172.30.14.5",
  "port": "8080",
  "authenticated": false,
  "username": null,
  "password": null,
  "scheme": null
}
```

#### Response :

```
HTTP/1.1 204 No Content
```

#### Status codes:

- 204: Successful updation
- 404: settings not found
- 400: Invalid request
- 500: Internal server error

## 26 Template Customization

---

### 26.1 Mail Template Customization

It provides a set of APIs to customize Templates and manage them. With these APIs the templates can be listed, created, updated, activated and reset back to original template.

#### Properties:

- *id*: Template ID
- *type*: The type of the template
- *subType*: The subtype of the template
- *displayName*: The display name of the template
- *description*: The description of the template
- *defaultTemplate*: There are some templates which comes by default as part of the system. These templates are marked as defaultTemplate.
- *active*: At any point of time only one template of any type & subType can be activated in the CloudAxis. Whichever template is in the active state is marked as active.

#### Supported Template Types:

- *EMAIL*: Email templates
- *WHITELABEL*: White labelling templates

#### Supported Template Sub-Types:

- *MEETING\_CANCEL\_HOST*: Cancel Meeting Host template
- *MEETING\_CANCEL\_PARTICIPANT*: Cancel Meeting Participants template
- *MEETING\_CREATE\_UPDATE\_HOST\_NO\_EXPOSE\_PASSCODE*: Create/Update Meeting Host template without exposing passcode.
- *MEETING\_CREATE\_UPDATE\_HOST*: Create/Update Meeting Host template
- *MEETING\_CREATE\_UPDATE\_PARTICIPANT\_NO\_EXPOSE\_PASSCODE*: Create/Update Meeting Participants template without exposing passcode.
- *MEETING\_CREATE\_UPDATE\_PARTICIPANT*: Create/Update Participants template
- *USER\_CREATE*: Create User Template
- *USER\_UPDATE\_PASSWD*: User Update Password template
- *USER\_RESET\_PASSWD\_BY\_ADMIN*: User Reset Password by Admin template
- *CUSTOM\_UI*: Custom UI template

The supported REST APIs are:

#### 26.1.1 List all Templates

This API is used to list all available templates in the CloudAxis. Using multiple query parameters the list can be refined for a type, sub-type, defaultTemplate and active templates.

#### Roles allowed:

- *ROLE\_SUPER\_ADMIN*

**Request:** To list all templates without any filter criterion.

```
GET: http://<WSP IP Address>/wsp/templates

HEADER DETAILS:

X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudaxis.templatecollection+json
```

**Request:** To list templates matching the various filter criteria.

```
GET: http://<WSP IP Address>:8080/wsp/templates?subtype=MEETING_CANCEL_HOST&defaultTemplate=true

HEADER DETAILS:

X-CA-UserName:      <UserName of the user in UPN format ie upn_username@domain.com>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudaxis.templatecollection+json
```

### Query Parameters:

- *type*: Type of the template to filter out the list.
- *subtype*: Sub-Type of the template to filter out the list.
- *defaultTemplate*: Whether a template is default or not (true/false)
- *active*: Whether a template is active or not (true/false)

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.templatecollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "templates": [
    {
      "id": 5,
      "type": "EMAIL",
      "subType": "MEETING_CANCEL_HOST",
      "displayName": "Meeting Cancel Host",
      "description": "Cancel Meeting Host template",
      "defaultTemplate": true,
      "active": false
    },
    {
      "id": 201,
      "type": "EMAIL",
      "subType": "MEETING_CANCEL_HOST",
      "displayName": "Meeting Cancel Host",
      "description": null,
      "defaultTemplate": false,
      "active": true
    },
    {
      "id": 251,
      "type": "EMAIL",
      "subType": "MEETING_CANCEL_PARTICIPANT",
      "displayName": "Meeting Cancel Participants",
      "description": null,
      "defaultTemplate": false,
      "active": false
    }
  ]
}

```

### Status Codes:

- 200: OK - Success.
- 401: Unauthorized if CA-Token is invalid
- 405: Method not allowed
- 500: Internal Server Error.

#### 26.1.2 Upload a Template

This API is used to upload any template file. It can be called with 2 options ie with preview or without preview. In case of preview-option, the template will not be uploaded as final. Rather a follow up preview API (mentioned below) is called to see the preview before finally activating it. In case of without preview option, the API just uploads the template content as final. The API accepts just the HTML content of the template file. So, in case of any other format, it simply rejects the request.



**Roles allowed:**

- **ROLE\_SUPER\_ADMIN**

**Request:**

```
POST: http://<WSP IP Address>/wsp/templates?preview=false
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudaxis.templatecollection+json
    Content-Type:       multipart/form-data

Form-data:
    Key      TEMPLATE_SUB_TYPE. Key should be one among the template-sub-types
    Value    file (html)
```

**Query Parameters:**

- *preview*: true/false. True by default if not provided in the query param.

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.templatecollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "templates": [
    {
      "id": 5,
      "type": "EMAIL",
      "subType": "MEETING_CANCEL_HOST",
      "displayName": "Meeting Cancel Host",
      "description": "Cancel Meeting Host template",
      "defaultTemplate": true,
      "active": false
    },
    {
      "id": 201,
      "type": "EMAIL",
      "subType": "MEETING_CANCEL_HOST",
      "displayName": "Meeting Cancel Host",
      "description": null,
      "defaultTemplate": false,
      "active": true
    },
    {
      "id": 251,
      "type": "EMAIL",
      "subType": "MEETING_CANCEL_PARTICIPANT",
      "displayName": "Meeting Cancel Participants",
      "description": null,
      "defaultTemplate": false,
      "active": false
    }
  ]
}

```

### Status Codes:

- 200: Successful upload. It lists all the templates which are currently active
- 400: Bad Request with message.
- 401: Unauthorized if CA-Token is invalid
- 405: Method not allowed
- 413: Attachment size exceeds the allowable limit 1MB.
- 500: Internal server error

#### 26.1.3 Preview a template

This API is used to see the preview of the just uploaded template. In case of with-preview option, this API is called to preview the content. If preview looks fine, then the upload API is called with without-preview option to upload it finally.

**Roles allowed:**

- Any user with any ROLE who has One-time-token

**Request:**

```
GET: http://<WSP IP Address>/wsp/templates/preview?username=upn_username@domain.com&token=63D1F5D9191E3CAC-558DB400-90517BF1-E09229AA-54E0BA
HEADER DETAILS:
Accept: text/html
```

**Query Parameters:**

- username*: UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn\_username@domain.com
- token*: One-time-token

**Response :**

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Disposition: attachment; filename=PREVIEW_TEMPLATE.html
```

**Status Codes:**

- 200: OK
- 401: Unauthorized if CA-Token is invalid
- 405: Method Not Allowed
- 500: Internal Server Error.

**26.1.4 Activate a Template**

This API is called to activate any particular template with id as TEMPLATE\_ID.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
PUT: http://<WSP IP Address>/wsp/templates/<TEMPLATE_ID>/activate?reset=true
HEADER DETAILS:
X-CA-UserName: <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username>
X-CA-Token: <Auth token obtained after authentication>
Accept: application/vnd.com.polycom.cloudaxis.templatecollection+json
```

**Query Parameters:**

- reset*: true/false. False by default. If reset is set to true, the template with id TEMPLATE\_ID is deactivated and the corresponding default template of same subType is activated.

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.templatecollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "templates": [
    {
      "id": 5,
      "type": "EMAIL",
      "subType": "MEETING_CANCEL_HOST",
      "displayName": "Meeting Cancel Host",
      "description": "Cancel Meeting Host template",
      "defaultTemplate": true,
      "active": false
    },
    {
      "id": 201,
      "type": "EMAIL",
      "subType": "MEETING_CANCEL_HOST",
      "displayName": "Meeting Cancel Host",
      "description": null,
      "defaultTemplate": false,
      "active": true
    },
    {
      "id": 251,
      "type": "EMAIL",
      "subType": "MEETING_CANCEL_PARTICIPANT",
      "displayName": "Meeting Cancel Participants",
      "description": null,
      "defaultTemplate": false,
      "active": false
    }
  ]
}

```

### Status Codes:

- 200: Success. It lists all the templates which are currently active
- 500: Internal server error
- 400: Bad Request with message.
- 401: Unauthorized if CA-Token is invalid
- 405: Method not allowed

#### 26.1.5 Download an existing Template

This API is used to download any existing template from CloudAxis. The template can be a default template coming with the system or it can be a custom template which is uploaded later on. The response of this API will have the template file for the template with id as TEMPLATE\_ID.

### Roles allowed:

- Any User with any ROLE who has One-time-token

**Request:**

```
GET: http://<WSP IP Address>/wsp/templates/<TEMPLATE_ID>/download?preview=true&username=upn_username@domain.com&token=63D1F5D9191E3CAC-558DB
HEADER DETAILS:
Accept: text/html
```

**Path Parameters:**

- *TEMPLATE\_ID*: ID of the template

**Query Parameters:**

- *preview*: true/false. False by default if not provided in the query param.
- *username*: UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn\_username@domain.com.
- *token*: One-time-token

**Response :**

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Disposition: attachment; filename=PREVIEW_TEMPLATE.html
```

**Status Codes:**

- 200: OK
- 500: Internal Server error
- 400: Bad Request with a message.
- 401: Unauthorized if CA-Token is invalid
- 405: Method not allowed.

## 27 Single Sign-On (SSO) Configuration

---

### 27.1 Single Sign-On Configuration API

These set of APIs provide the configuration interface for Single Sign-On with SPNEGO and SAML approaches. The supported REST APIs are:

#### Properties:

- *id*: Auth Method ID
- *methodname*: Auth Method Name
- *description*: Auth Method Description
- *authtype*: Type of Auth Method like SSO or OTHER.
- *enabled*: Enabled status of Auth Method. Only one Auth Method can be enabled at a time.
- *priority*: The priority of the Auth Method
- *securitystrength*: The Security strength of the Auth Method
- *policyFallbackLdap*: Policy to allow authentication with LDAP as fall back in case if Single Sign-On authentication fails.
- *version*: Version of the Auth Method.

#### 27.1.1 List All Authentication Methods

This API lists all the authentication methods which are supported in CloudAxis. Each authentication method will have detail like method name, method type, enabled status, priority and version.

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/authmethods
```

#### HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.AuthMethodCollection+json

#### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.AuthMethodCollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "authMethods": [
    {
      "id": 1,
      "methodname": "SPNEGO",
      "description": "Single Sign On with SPNEGO",
      "authtype": "SSO",
      "enabled": false,
      "priority": 1,
      "securitystrength": 10,
      "version": 1,
      "spn": "HTTP/wsp-dev1.cloudax.is@POLYCOM.COM",
      "policyfallbackldap": "true"
    },
    {
      "id": 2,
      "methodname": "SAML",
      "description": "Single Sign On with SAML",
      "authtype": "SSO",
      "enabled": false,
      "priority": 2,
      "securitystrength": 10,
      "version": 1,
      "spn": null,
      "policyfallbackldap": "true"
    },
    {
      "id": 3,
      "methodname": "LDAP",
      "description": "Simple LDAP bind with a directory server",
      "authtype": "OTHER",
      "enabled": true,
      "priority": 2,
      "securitystrength": 5,
      "version": 1,
      "spn": null,
      "policyfallbackldap": null
    }
  ]
}

```

### Status Codes:

- 200: OK - Success.
- 401: Unauthorized if CA-Token is invalid
- 405: Method not allowed
- 500: Internal Server Error.

### 27.1.2 Activate Authentication Method

This API is used to activate any authentication method in CloudAxis. This API call will automatically de-activate the existing activated authentication method. Only one Auth Method can be enabled at a time. Once activated, all external clients like MEA or WSP-UI will be authenticated with the newly activated Auth Method. The API also updates policyFallbackLdap to LDAP. WSP uses the selected/activated method for authentication.

#### Roles allowed:

- **ROLE\_SUPER\_ADMIN**

#### Request:

```
PUT: http://<WSP IP Address>/wsp/authmethods/<AUTH_METHOD_ID>/activate?policyFallbackLdap=true
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.AuthMethodCollection+json
```

#### Properties:

- **AUTH\_METHOD\_ID**: ID of the Auth Method.
- **policyFallbackLdap**: true/false. True by default.

#### Response :



```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.AuthMethodCollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "authMethods": [
    {
      "id": 1,
      "methodname": "SPNEGO",
      "description": "Single Sign On with SPNEGO",
      "authtype": "SSO",
      "enabled": false,
      "priority": 1,
      "securitystrength": 10,
      "version": 1,
      "spn": "HTTP/wsp-dev1.cloudax.is@POLYCOM.COM",
      "policyfallbackldap": "true"
    },
    {
      "id": 2,
      "methodname": "SAML",
      "description": "Single Sign On with SAML",
      "authtype": "SSO",
      "enabled": false,
      "priority": 2,
      "securitystrength": 10,
      "version": 1,
      "spn": null,
      "policyfallbackldap": "true"
    },
    {
      "id": 3,
      "methodname": "LDAP",
      "description": "Simple LDAP bind with a directory server",
      "authtype": "OTHER",
      "enabled": true,
      "priority": 2,
      "securitystrength": 5,
      "version": 1,
      "spn": null,
      "policyfallbackldap": null
    }
  ]
}

```

### Status Codes:

- 200: Success
- 400: Bad Request with message.
- 401: Unauthorized if CA-Token is invalid
- 405: Method not allowed

- 500: Internal server error

### 27.1.3 Update SSO SPNEGO Configuration for Kerberos SPN and Keytab file

This API is used to configure SSO SPNEGO Auth Method in CloudAxis. It requires servicePrincipalName and its corresponding keytab file in the request.

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
POST: http://<WSP IP Address>/wsp/ssoconfig/spnego/keytab/upload
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-Type:       multipart/form-data

Form-data:
    Key                 <KRB_SRV_PRINC_NAME> eg HTTP/wsp_srv.example.com@EXAMPLE.COM
    Value               file (binary)
```

#### Properties:

- *Key*: Key should be the kerberos servicePrincipalName. Make sure this SPN is added on the service account created in AD.
- *Value*: Keytab file for the servicePrincipalName. The keytab file is generated by using the ktpass utility available in windows server.

**Mandatory Properties:** SPN, Keytab

#### Response :

```
HTTP/1.1 200 OK
```

#### Status Codes:

- 200: Successful upload.
- 400: Bad Request with message.
- 401: Unauthorized if CA-Token is invalid
- 405: Method not allowed
- 413: Attachment size exceeds the allowable limit 1MB.
- 500: Internal server error

### 27.1.4 Update SSO SAML configuration for Identity Provider ie IdP Metadata

This API is used to download CloudAxis SP metadata. This metadata has all configuration information of the CloudAxis. This metadata file is used to configure CloudAxis as a relying party or SP in IdP.

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```

POST: http://<WSP IP Address>/wsp/ssoconfig/saml/metadata/upload

HEADER DETAILS:

    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom
    X-CA-Token:         <Auth token obtained after authentication>
    Content-Type:       multipart/form-data

Form-data:

    Key                 IDP_METADATA
    Value               file (xml)

```

### Properties:

- *Key*: Key name ie IDP\_METADATA.
- *Value*: Identity Provider ie IdP metadata file. This metadata file is obtained by downloading it from IdP server. This file has all the IdP detail like entityID, SignedInfo, RoleDescriptor, SPSSODescriptor and IDPSSODescriptor. Uploading this to CloudAxis makes the IdP related configuration done at WSP end.

### Response :

```
HTTP/1.1 200 OK
```

### Status Codes:

- 200: Successful upload.
- 400: Bad Request with message.
- 401: Unauthorized if CA-Token is invalid
- 405: Method not allowed
- 413: Attachment size exceeds the allowable limit 1MB
- 500: Internal server error

#### 27.1.5 Download CloudAxis (Service Provider) Metadata for integrating it with IdP

##### Roles allowed:

- User with any ROLE who has OneTimeToken

##### Request:

```

GET: http://<WSP IP Address>/wsp/ssoconfig/saml/metadata/download/?username=upn_username%40domain.com&token=63D1F5D9191E3CAC-558DB400-90517B
HEADER DETAILS:

    Accept:             text/xml

```

### Properties:

- *userName*: UserName of the user. In case of enterprise user it must be in UPN format ie upn\_username@domain.com
- *token*: OneTimeToken to be used only for one time. This can be acquired by calling One Time Token API.

**Response :**

```

HTTP/1.1 200 OK
Content-Type:          text/xml
Content-Disposition:  attachment; filename=SP.xml

```

**Status Codes:**

- 200: OK
- 401: Unauthorized if CA-Token is invalid
- 405: Method Not Allowed
- 500: Internal Server Error.

**27.1.6 List SAML specific Metadata information like enitityId & entityName of CloudAxis (SP) and configured IdPs**

This API is required for SSO SAML configuration in CloudAxis. It lists the enitityId & entityName information for the CloudAxis (SP) and configured IdPs. This is not a ReST based API.

**Roles allowed:**

- Any user with any ROLE. This information is available and published for anonymous call of API.

**Request:**

```
GET: http://<WSP IP Address>/wsp-ui/secure/saml/metadata
```

**Response :**

```

HTTP/1.1 200 OK
Content-Type:          application/json
{
  "hostedSP": {
    "entityId": "https___wsp-saml.domain.com_443_wsp-ui_saml_metadata",
    "entityName": "https://wsp-saml.domain.com:443/wsp-ui/saml/metadata"
  },
  "idpList": [
    {
      "entityId": "_6764f9ad-f565-40fa-8fe9-531963648e06",
      "entityName": "http://sts.domain.com/adfs/services/trust"
    }
  ]
}

```

**Status Codes:**

- 200: OK
- 405: Method Not Allowed
- 500: Internal Server Error.

## 28 White Label Configuration

---

### 28.1 Whitelabel REST APIs

Provides APIs to get whitelabel configuration related information, update and restore default configuration.

Whitelabelling allows custom logo, favicon, background image to be uploaded on WSP. Admin can also control the footer related information like help links, product info visibility on the user facing page.

#### Properties:

- *logo*: Parent tag for logo image related information. Image formats of type JPEG,GIF and PNG can be uploaded. Contains the *selector*, *image* tags.
- *appTitle*: Parent tag for application title related information. This title will be applied to the browser title also. Contains the *selector*, *defVal* and *customVal* tags.
- *favIcon*: Parent tag for favIcon image related details. Contains the *selector*, *image* tags.
- *login*: Parent tag for login related information.
  - *showLogo*: Boolean flag to enable/disable logo on the WSP home page. True by default.
  - *showAppTitle*: Boolean flag to enable/disable application title on the WSP home page. True by default.
  - *logoBlank*: If *logo* is Blank, then this value is set to true internally. Else false.
  - *background*: Parent tag for background image details. Contains the *selector*, *image* and *thumbnail* tags.
- *logout*: Parent tag for logout related information.
  - *redirectUri*: Url for the redirection after logout. Contains *selector*, *defVal* and *customVal* tags.
- *footer*: Parent tag for footer related information.
  - *showFooter*: Boolean flag to enable/disable footer. \* *showProductInfo*: Boolean flag to enable/disable product info in the footer. \* *showHelp*: Boolean flag to enable/disable the help url in the product. \* *helpData*: Parent tag for help related information. Contains *selector*, *defVal*, *customVal* tags.

The below tags are child tags for the above tags. They are used as explained below:

- *selector*: Placeholder for user selection. Allowed values for logo are "customVal","defVal","blank". Allowed values for all other cases are "customVal","defVal".
- *defVal*: Placeholder for default value for an attribute.
- *customVal*: Placeholder for custom value for an attribute.
- *image*: Placeholder for image attributes based on the context of logo,favIcon,background
- *thumbnail*: Placeholder for thumbnail attributes for a given image.
- *title*: Placeholder for the application title
- *uri*: Placeholder for uris.

The supported REST APIs are:

#### 28.1.1 Get white label information

##### Roles allowed:

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: https://<IP Address>/wsp/whitelabel?id=<id1>&id=<id2>

HEADER DETAILS:

X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.whitelabel+json
```

**Query parameters**

- *id*: To get specific configuration of the id. Supported values are logo, appTitle, favIcon, login and footer.

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudaxis.whitelabel+json
{
  "logo":{
    "selector":"defVal",
    "image":{
      "defVal":{
        "uri":"/webapp/whitelabel/images/caxis/polycomLogo.png"
      },
      "customVal":{
        "uri":null
      }
    },
    "thumbnail":{
      "defVal":{
        "uri":null
      },
      "customVal":{
        "uri":null
      }
    }
  },
  "appTitle":{
    "selector":"defVal",
    "defVal":{
      "title":"RealPresence&reg; CloudAXIS&trade;"
    },
    "customVal":{
      "title":null
    }
  },
  "favicon":{
    "selector":"defVal",
    "image":{
      "defVal":{
        "uri":"/webapp/whitelabel/images/caxis/polycomFavicon.png"
      },
      "customVal":{
        "uri":null
      }
    },
    "thumbnail":{
      "defVal":{
        "uri":null
      },
      "customVal":{
        "uri":null
      }
    }
  },
  "login":{
    "showLogo":true,
    "showAppTitle":true,
    "logoBlank":false,
    "background":{
      "selector":"defVal",
      "image":{
        "defVal":{
          "uri":null
        },
        "customVal":{

```

**Status codes:**

- 200: Successful read
- 500: Internal Server Error
- 404: If the request is not a valid request

**28.1.2 Update configuration for whitelabelling****Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request :**

```
POST: https://<IP Address>/wsp/whitelabel?preview=false
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@dom>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       multipart/form-data

MultiParts :
    key=settings, Value=json content i.e. if login is to be updated the key settings and background
    are needed : {"login":{"showLogo":true,"showAppTitle":true,...}}
    Content-Type: application/vnd.com.polycom.cloudAxis.whitelabel+json

    key=logo Value=<image for logo>
    Content-Type: image/png,image/gif,image/jpeg

    key=favIcon Value=<image for favicon>
    Content-Type: image/png

    key=background Value=<image for background>
    Content-Type: image/jpeg
```

**Description:**

- Mandatory to have settings key because the json configuration is required for every update.
- If a custom image is being updated for the first time, the respective key is expected(along with the corresponding json content in settings).Ex: If settings has json content for updating a custom logo for the first time, then the key 'logo' along with the image should be sent with the request.For subsequent custom updates, the user is expected to send the attachment for the image which is to be updated.
- preview is false by default. If true, it is applicable for login preview only.

**Response :**

```
HTTP/1.1 204 No Content
```

**Status codes:**

- 204: Successful Update
- 400: Bad request
- 500: Internal Server Error

**28.1.3 Restore Defaults**

Restores the configuration to the default configuration.



**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Query Parameters:**

- *id* : to restore specific id configuration. id values supported are :  
logo,appTitle,favIcon,login,footer
- No body is expected.

**Request:**

```
POST: https://<IP Address>/wsp/whitelabel?id=<id1>&id<id2>..
```

**HEADER DETAILS:**

```
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
X-CA-Token:         <Auth token obtained after authentication>
```

**Note:**

If ids are not specified, the entire configuration will be restored to default.

Please use this API with caution.

**Response :**

```
HTTP/1.1 204 No Content
```

**Status codes:**

- 204: Successful update to restore defaults
- 400: Bad request
- 500: Internal Server Error

**28.1.4 Get login preview**

Gets whitelabel configuration login preview information.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```
GET: https://<IP Address>/wsp/whitelabel/preview
```

**HEADER DETAILS:**

```
X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
X-CA-Token:         <Auth token obtained after authentication>
Accept:             application/vnd.com.polycom.cloudAxis.whitelabeluser+json
```

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.whitelabeluser+json
{
  "logoImageUri": "/webapp/whitelabel/images/caxis/polycomLogo.png",
  "appTitle": "Custom App Title",
  "faviconImageUri": "/webapp/whitelabel/images/caxis/polycomFavicon.png",
  "showLogoOnLogin": true,
  "showAppTitleOnLogin": true,
  "backgroundImageUri": "/webapp/whitelabel/images/custom/tmp/customBackground.jpg",
  "logoutRedirectUrl": "/login/#reln",
  "footer": {
    "showFooter": true,
    "data": {
      "showProductInfo": true,
      "showHelp": true,
      "helpUri": "http://plcmtechnet.com/current/en/1048/1178/1621"
    }
  }
}
```

**Status codes:**

- 200: Successful read
- 500: Internal Server Error
- 404: If the request is not a valid request

**28.1.5 Update simple configuration for whitelabelling**

Updates the configuration for whitelabelling. Applicable only in the case no attachments are to be uploaded. Applicable for logo, appTitle, favicon, login, footer.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request :**

```

POST: https://<IP Address>/wsp/whitelabel?preview=false
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.whitelabel+json
Body:
{
  "logout":{
    "redirectUrl":{
      "selector":"defVal",
      "defVal":{
        "uri":"/login/#reln"
      },
      "customVal":{
        "uri":null
      }
    },
    "footer":{
      "showFooter":true,
      "showProductInfo":false,
      "showHelp":false,
      "helpData":{
        "selector":"defVal",
        "defVal":{
          "uri":"http://plcmtechnet.com/current/en/1048/1178/1621"
        },
        "customVal":{
          "uri":null
        }
      }
    }
  }
}

```

**Note:**

preview is false by default. If true, it is applicable for login preview only and login configuration should be present in the body.

**Response :**

```
HTTP/1.1 204 No Content
```

**Description:**

- 204: Successful Update
- 400: Bad request
- 500: Internal Server Error

## 29 Notification Message Configuration

### 29.1 Notification Message REST APIs

Provides APIs to get notification messages configured for the product.

Notification message customization allows the admin to provide maintenance messages, important notices to be displayed, on the home page, after user login. Admin can configure the time duration during which this message is to be displayed.

#### Properties:

- *id*: Internal id for notification message.
- *showMessage*: Boolean flag to enable/disable if the message is to be displayed. Default value is false.
- *title*: Title to be displayed for the notification message.
- *message*: Notification message to be displayed.
- *scheduled*: Boolean flag to enable/disable the time duration. Default value is false.
- *startTime*: start time for the message. **Format**: YYYY-MM-DDTHH:MM:SS.
- *endTime*: end time for the message. **Format**: YYYY-MM-DDTHH:MM:SS.

**Mandatory Properties:** showMessage, title, message, scheduled. If scheduled is enabled, startTime and endTime are mandatory.

The supported REST APIs are:

#### 29.1.1 List all Notification Messages.

##### Roles allowed:

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN
- ROLE\_USER

##### Request:

```
GET: http://<WSP IP Address>/wsp/notifications?activated=false
```

##### HEADER DETAILS:

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:	<Auth token obtained after authentication>
Accept:	application/vnd.com.polycom.cloudAxis.notificationMessageCollection+json

##### Query Parameters:

- *activated*: By default the value is false. If activated=true, then the collection will be empty if no applicable notification messages are scheduled for the current time. Else, it will have the applicable notification message entity.
- *pageSize*: Size of the current page request. Default: 5
- *currentPage*: Current page number of the request. Default: 0

##### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.notificationMessageCollection+json
{
    "statistics":null,
    "prev":null,
    "next":null,
    "notificationMessages":[
        {
            "self":"https://172.30.2.179:443/wsp/notifications/1",
            "id":"1",
            "showMessage":true,
            "title":"Important Note",
            "message":"Message goes in here",
            "scheduled":true,
            "startTime":"2014-08-20T19:30:00.000+0000",
            "endTime":"2014-08-28T00:30:00.000+0000"
        }
    ]
}

```

**Status codes:**

- 200: Successful listing
- 500: Internal Server Error

**29.1.2 Update Notification Message details****Roles allowed:**

- ROLE\_SUPER\_ADMIN
- ROLE\_ADMIN

**Request:**

PUT: http://<WSP IP Address>/wsp/notifications/<id>

**HEADER DETAILS:**

X-CA-UserName:	<UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
X-CA-Token:	<Auth token obtained after authentication>
Content-Type:	application/vnd.com.polycom.cloudAxis.notificationMessage+json

**Response :**

HTTP/1.1 204 No Content

**Status codes:**

- 204: Successful Update
- 400: Bad Request
- 500: Internal Server Error

## 30 Test Features Activation and Deactivation

---

### 30.1 Test Features Activation and Deactivation

This interface provides a set of APIs to list, activate and deactivate the test features.

#### Properties:

- *id*: ID of the feature
- *featurename*: The name of the feature
- *description*: The description of the feature
- *featuretype*: The type of the feature
- *enabled*: The enable status of the feature
- *recommendation*: The recommendation for the feature ie YES/NO
- *version*: The version of the feature

The supported REST APIs are:

#### 30.1.1 List all Test Features

This API is used to get all Test Features available in the CloudAxis.

#### Roles allowed:

- ROLE\_SUPER\_ADMIN

#### Request:

```
GET: http://<WSP IP Address>/wsp/features
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.FeatureCollection+json
```

#### Response :

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.FeatureCollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "features": [
    {
      "id": 102,
      "featurename": "EXCHANGE_INTEGRATION",
      "description": null,
      "featuretype": "TEST",
      "enabled": false,
      "recommendation": "YES",
      "version": 1
    },
    {
      "id": 101,
      "featurename": "SSO_WITH_SAML",
      "description": null,
      "featuretype": "TEST",
      "enabled": false,
      "recommendation": "YES",
      "version": 2
    }
  ]
}

```

**Status Codes:**

- 200: OK - Successful
- 500: Internal Server Error

**30.1.2 Activate Test Feature**

This API is used to activate a particular Test Feature. The Feature ID is provided in the path parameter.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```

PUT: http://<WSP IP Address>/wsp/features/<id>/activate
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.FeatureCollection+json
Body:
{
}

```

**Path Parameter:**

- *id*: Feature ID to be used coming from the get test feature list API.

**Response :**

```

HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.FeatureCollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "features": [
    {
      "id": 102,
      "featurename": "EXCHANGE_INTEGRATION",
      "description": null,
      "featuretype": "TEST",
      "enabled": false,
      "recommendation": "YES",
      "version": 1
    },
    {
      "id": 101,
      "featurename": "SSO_WITH_SAML",
      "description": null,
      "featuretype": "TEST",
      "enabled": true,
      "recommendation": "YES",
      "version": 2
    }
  ]
}

```

**Status Codes:**

- 200: OK - Successful
- 500: Internal Server Error

**30.1.3 Deactivate Test Feature**

This API is used to deactivate a particular Test Feature. The Feature ID is provided in the path parameter.

**Roles allowed:**

- ROLE\_SUPER\_ADMIN

**Request:**

```

PUT: http://<WSP IP Address>/wsp/features/<id>/deactivate
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
    X-CA-Token:         <Auth token obtained after authentication>
    Accept:             application/vnd.com.polycom.cloudAxis.FeatureCollection+json
Body:
{
}

```

**Path Parameter:**



- *id*: Feature ID to be used coming from the get test feature list API.

**Response :**

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.polycom.cloudAxis.FeatureCollection+json
{
  "statistics": null,
  "prev": null,
  "next": null,
  "features": [
    {
      "id": 102,
      "featurename": "EXCHANGE_INTEGRATION",
      "description": null,
      "featuretype": "TEST",
      "enabled": false,
      "recommendation": "YES",
      "version": 1
    },
    {
      "id": 101,
      "featurename": "SSO_WITH_SAML",
      "description": null,
      "featuretype": "TEST",
      "enabled": false,
      "recommendation": "YES",
      "version": 2
    }
  ]
}
```

**Status Codes:**

- 200: OK - Successful
- 500: Internal Server Error

## 31 SNMP Management

---

### 31.1 Snmp Agent API

It provides API to configure SNMP and Notification Agents

#### 31.1.1 Enable SNMP Configuration

This API should be used to update SNMP configuration for the Snmp Agent

**Request for Snmp v2c configuration with Notification Agents configuration :**

```

PUT: https://<IP ADDRESS>/platform/snmp-agent
HEADER DETAILS:
    X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain>
    X-CA-Token:         <Auth token obtained after authentication>
    Content-type:       application/vnd.com.polycom.cloudAxis.snmp-agent-config+json
Body:
{
  "location": "Earth",
  "port": "161",
  "version": "v2c",
  "transport": "UDP",
  "enabled": true,
  "snmpV2c": {
    "community": "public"
  },
  "notificationUsers": [
    {
      "username": "snmpuser",
      "encryptionType": "DES",
      "encryptionPassword": "EncryptionPwd",
      "authenticationPassword": "AuthenticationPwd",
      "authenticationType": "SHA"
    }
  ],
  "notificationAgents": [
    {
      "address": "10.230.149.191",
      "type": "Trap",
      "port": "162",
      "version": "v2c",
      "username": null,
      "transport": "UDP",
      "enabled": true
    },
    {
      "address": "10.230.149.192",
      "type": "Trap",
      "port": "162",
      "version": "v3",
      "username": "snmpuser",
      "transport": "UDP",
      "enabled": true
    }
  ],
  "contact": "Administrator"
}

```

### Request for Snmp v3 configuration with Notification Agents configuration:

```

PUT: https://<IP ADDRESS>/platform/snmp-agent
Content-type : application/vnd.com.polycom.cloudAxis.snmp-agent-config+json
X-CA-UserName : <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_username@domain.com>
X-CA-Token : <Auth token obtained after authentication>
Body:
{
  "location": "Earth",
  "port": "161",
  "version": "v3",
  "transport": "UDP",
  "enabled": true,
  "engineId": "0X123adf234asd837"
  "snmpV2c": {
    "community": "public"
  },
  "snmpV3": {
    "username": "wspnmp",
    "encryptionType": "DES",
    "encryptionPassword": "EncryptionPwd",
    "authenticationPassword": "AuthenticationPwd",
    "authenticationType": "SHA"
  },
  "notificationUsers": [
    {
      "username": "snmpuser",
      "encryptionType": "DES",
      "encryptionPassword": "EncryptionPwd",
      "authenticationPassword": "AuthenticationPwd",
      "authenticationType": "SHA"
    }
  ],
  "notificationAgents": [
    {
      "address": "10.230.149.191",
      "type": "Trap",
      "port": "162",
      "version": "v2c",
      "username": null,
      "transport": "UDP",
      "enabled": true
    },
    {
      "address": "10.230.149.192",
      "type": "Trap",
      "port": "162",
      "version": "v3",
      "username": "snmpuser",
      "transport": "UDP",
      "enabled": true
    }
  ],
  "contact": "Administrator"
}

```

**Description:**

- *enabled* : Boolean  
It should be set to true to enable Snmp Agent else to false to disable Snmp Agent
- *location* : String  
Location of machine, As of now used only for information purpose
- *contact* : String  
Admin contact, As of now used only for information purpose
- *version* : String  
Version of SNMP protocol for Snmp Agent  
It should be set as "v2c" or "v3"
- *transportType* : String  
Transport layer protocol for Snmp Agent  
It should be set as "TCP" or "UDP"
- *port* : Short  
Transport layer port no. on which SNMP messages are exchanged
- *snmpV2c* : JSON  
SNMP Credentials specific SNMP v2  
It should be set if version field is set as "v2c" else it is ignored
- *community* : String  
Community for Snmp Agent
- *snmpV3* : JSON  
SNMP Credentials specific SNMP v3  
It should be set if version field is set as "v3" else it is ignored
- *username* : String  
Authentication username for Snmp Agent
- *authenticationType* : String  
Authentication type for Snmp Agent  
It should be set as "MD5" or "SHA"
- *encryptionType* : String  
Encryption type for Snmp Agent  
It should be set as "DES" or "AES"
- *authenticationPassword* : String  
Authentication password for Snmp Agent  
It should be atleast 8 characters
- *encryptionPassword* : String  
Encryption password for Snmp Agent  
It should be atleast 8 characters

**Response :**

Status: 204 No Content
------------------------

**Description:**

- Returns with 204 No Content if Snmp Agent configuration is successfully updated
- Returns with 400 Bad Request with error messages if any of the input parameter is wrong
- Returns with 401 Unauthorized if authentication headers are not set properly
- Returns with 403 Forbidden if EULA is not accepted

**31.1.2 Get Configuration**

This API should be used to get current configuration of SnmpAgent

**Request:**

```
GET: https://<IP ADDRESS>/platform/snmp-agent
HEADER DETAILS:
  X-CA-UserName:      <UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn_user>
  X-CA-Token:         <Auth token obtained after authentication>
  Accept:             application/vnd.com.polycom.cloudAxis.snmp-agent-config+json
```

**Response :**

```

Status: 200 Ok
Body:
{
  "location": "Earth",
  "port": "161",
  "version": "v2c",
  "transport": "UDP",
  "enabled": true,
  "snmpV2c": {
    "community": "public"
  },
  "notificationUsers": [
    {
      "username": "snmpuser",
      "encryptionType": "DES",
      "encryptionPassword": "EncryptionPwd",
      "authenticationPassword": "AuthenticationPwd",
      "authenticationType": "SHA"
    }
  ],
  "notificationAgents": [
    {
      "address": "10.230.149.191",
      "type": "Trap",
      "port": "162",
      "version": "v2c",
      "username": null,
      "transport": "UDP",
      "enabled": true
    },
    {
      "address": "10.230.149.192",
      "type": "Trap",
      "port": "162",
      "version": "v3",
      "username": "snmpuser",
      "transport": "UDP",
      "enabled": true
    }
  ],
  "contact": "Administrator"
}

```

### Status Codes:

- Returns with 200 ok and Snmp Agent configuration params for successful request
- Returns with 400 Bad Request with error messages if any of the input parameter is wrong
- Returns with 401 Unauthorized if authentication headers are not set properly
- Returns with 403 Forbidden if EULA is not accepted
- Rest of parameters are same as "Update Configuration" request

### 31.1.3 Download MIB

This API should be used to download MIB files

#### Request:

```
GET: https://<IP ADDRESS>/platform/snmp-agent/mibs?userName=admin&token=04242616-FC46-D6A0-7ACF-D30CFA5E8FA4
```

#### Query Parameters:

- *userName*: UserName of the user authenticated. In case of enterprise user, it must be in UPN format ie upn\_username@domain.com.
- *token*: One-time-token

#### Response :

```
Content-Type: application/zip  
Content-Disposition: attachment; filename=mibs.zip  
Status: 200 Ok
```

#### Description:

- Returns with 400 Bad Request with error messages if any of the input parameter is wrong
- Returns with 401 Unauthorized if authentication headers are not set properly
- Returns with 403 Forbidden if EULA is not accepted