

Cloudpath

Enrollment System

Using APIs to Interact With External Systems

Software Release 5.1

March 2017

Summary: This document describes how to create API keys and use them in REST APIs to enable integration with existing processes or third-party applications.

Document Type: Configuration

Audience: Network Administrator



Using APIs to Interact With External Systems

Software Release 5.1

March 2017

Copyright © 2017 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex™, BeamFlex™, MediaFlex™, ChannelFly™, and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2016 Ruckus Wireless, Inc. All rights reserved.

Using APIs to Interact With External Systems

Overview

Cloudpath provides REST APIs to enable integration with existing processes or third-party applications. The REST APIs allow the system to actively notify external systems (outbound calls) and to be queried and manipulated by external systems (inbound calls).

Outbound: Sending Notifications to External Systems

You can pass data from Cloudpath using notifications through email or URL requests. Variables are populated in the Enrollment Record and may be passed through the URL call.

For example, you might want to include enrollment data in a certificate issuance notification email. In this case, the URL containing the variables is sent to the server using a simple GET request, and the HTTP reply is the result data, included as part of the email notification.

Note >>

Some API calls support POST requests. If supported, POST is listed in the parameters.

Format for Variables

Variables in Cloudpath are in the following format: \${MAC_ADDRESS}, \${USERNAME}, or \${IP_ADDRESS}. See the Enrollment Variables section on the Enrollment Record page to view available variables, variable syntax, and expected values.

The variables are passed through a URL as in this example: `http://test.company.net/registration?user=${USERNAME}&mac=${MAC_ADDRESS}`. The result from this example would be the username and device MAC address sent within the notification.

Only variables which are populated at the time of the notification event are sent. MAC addresses and other variables may be populated through events other than onboarding, such as data prompts.

Note >>

We recommend that you use URL requests for large amounts of data. Send the enrollment GUID value in the REST URL and then query the Cloudpath system for the enrollment record.

Inbound: Querying Cloudpath

You can retrieve information from Cloudpath through a REST type API query and perform an action, based on the result data. For example, you might use an API query to block a user or revoke a certificate.

The API query, containing the identifier information and appropriate action, is sent to the server and the objects are returned in either JSON or XML.

The REST API call is structured as follows:

http://test.company.net/admin/api/zAdBCLcgrwca/enrollment/IdentityCN/bob/get

http://test.company.net/admin = HTTP authentication

api = API entry point

zAdBCLcgrwca = API key

enrollment = realm

IdentityCN = Identity type

bob = Identity value

get = Action

Each realm allows a different set of identity information. See the appropriate sections in API Examples for the list of valid identity types.

Creating an API Key

For Cloudpath to honor inbound requests from external systems, the external system must authenticate using an API key. The API key is part of the REST API query used to retrieve information from the Cloudpath system.

To create an API Key, go to *Configuration > API Keys* and click *Add API Key*.

FIGURE 1. Create API Key

The screenshot shows a web interface for creating an API key. The breadcrumb navigation is 'Configuration > API Keys > Create'. There are 'Cancel' and 'Save' buttons in the top right. The form is titled 'API Key Information' and contains the following fields:

- Name:** Device Capabilities
- Description:** (empty text area)
- Enabled:**
- API Key:** BmGsez6evQc8
- Allowed Path Regex:** *
- Expiration Date:** 20180404

Cloudpath provides a generated *API Key*, or you can specify a custom key. An API key must be URL-safe.

The *Allowed Path Regex* is a regex specifying the paths allowed to be called with this API key. For example, `/admin/api/.*/certificate/.*` can query anything in the 'certificate' realm. If left blank, there is no restriction.

For the *Expiration Date*, the Cloudpath system defaults to a one-year expiration, but this value can be modified.

API Examples

This section provides some common API queries for use with Cloudpath.

Enrollment Queries and Actions

When specifying which enrollment should be queried or manipulated by a request, the enrollments can be specified in various formats, such as *Pk*, *Guid*, *MACAddress*, *Username*, *AssistanceId*, and *Email*. Many of the requests contain a section similar to *Username/bob*, meaning any environment where the *username* is *bob*.

Retrieve Enrollment Data

Returns data for the specified enrollment.

URI:

/admin/api/{API_KEY}/enrollment/{IDENTITY_TYPE}/{IDENTITY_VALUE}/get

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/enrollment/Username/bob/get

Revoke/Unrevoke Enrollment

Revoke (or unrevoke) the specified enrollment.

URI:

/admin/api/{API_KEY}/enrollment/{IDENTITY_TYPE}/{IDENTITY_VALUE}/revoke

/admin/api/{API_KEY}/enrollment/{IDENTITY_TYPE}/{IDENTITY_VALUE}/unrevoke

Examples:

http://test.company.net/admin/api/zAdBCLcgrwca/enrollment/Email/bob@company.net/revoke

http://test.company.net/admin/api/zAdBCLcgrwca/enrollment/MACAddress/A1:B2:C3:D4:E5:F6/
unrevoke

Certificate Queries

When specifying which certificate should be queried or manipulated by a request, the certificates can be specified in various formats, such as *Pk*, *Cn*, and *Serial*.

Generate Certificate

Generates a certificate based on the CSR provided. This query supports *description* (optional) and *CUSTOM_VARIABLES* (any variable used in the certificate template).

URI:

/admin/api/{API_KEY}/certificate/generate

GET/POST Parameters:

- *csr* - Required.
- *certificateTemplateName* - Required. Name of certificate template in Cloudpath from which to issue.

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/certificate/
generate?csr={CSR}&certificateTemplateName=TestCompanyTemplate

Generate a P12 Certificate

Generates a certificate in P12 format, without a CSR. This query supports *description* (optional) and *CUSTOM_VARIABLES* (any variable used in the certificate template).

URI:

/admin/api/{API_KEY}/certificate/generateP12

GET/POST Parameters:

- certificateTemplateName - Required. Name of certificate template in Cloudpath from which to issue.
- password - Required. Password to use to encrypt the P12. May be left blank if not encrypted.
- validForDaysOverride - Optional. If provided, this overrides the certificate template's validity period.

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/certificate/generateP12?certificateTemplateName=ServerTemplate&password=test

Revoke/Unrevoke Certificate

Revoke the specified certificate.

URI:

/admin/api/{API_KEY}/certificate/{IDENTITY_TYPE}/{IDENTITY_VALUE}/revoke
/admin/api/{API_KEY}/certificate/{IDENTITY_TYPE}/{IDENTITY_VALUE}/unrevoke

Examples:

http://test.company.net/admin/api/zAdBCLcgrwca/certificate/Pk/235/revoke

Unrevoke the specified certificate.

http://test.company.net/admin/api/zAdBCLcgrwca/certificate/Cn/bob@company.net/unrevoke

Note >>

For external CAs, the CA must support *unrevoke*.

Return Certificate Data

Returns data about the specified certificate.

URI:

/admin/api/{API_KEY}/certificate/{IDENTITY_TYPE}/{IDENTITY_VALUE}/get

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/certificate/Serial/d8a76ccc42e6f3c5048fee0aa7d6e411841db54b/get

Revoke Certificate by Certificate Serial Number

Revokes a certificate with a specified serial number.

URI:

/admin/api/{apiKey}/certificate/Serial/{serialNumber}/revoke

GET/POST Parameters:

- serialNumber - Required. Serial number of the certificate.
- reason - Optional. Description of why the certificate was revoked.

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/certificate/Serial/00fde721f1bb5e45e3feb7b49e1e8728b561936b/revoke

User Queries

When specifying which user should be queried or manipulated by a request, the user can be specified in various formats, such as *IdentityCN*, *IdentityDN*, *CertificateCN*, *CertificateSerial*, and *Email*. Many of the requests contain a section similar to *Email/bob@company.net*, meaning any environment where the *Email* is *bob@company.net*.

Blocking/Unblocking User

Blocks the specified user account, which includes revoking all associated certificates and MAC registrations, and prevents the user from enrolling again.

URI:

/admin/api/{API_KEY}/user/{IDENTITY_TYPE}/{IDENTITY_VALUE}/block
/admin/api/{API_KEY}/user/{IDENTITY_TYPE}/{IDENTITY_VALUE}/unblock

Examples:

http://test.company.net/admin/api/zAdBCLcgrwca/user/IdentityCN/bob/block

Unblocks the specified user account.

http://test.company.net/admin/api/zAdBCLcgrwca/user/CertificateCN/bob/unblock

Revoke Enrollments

Revokes all enrollments for the user account, which includes revoking all associated certificates and MAC registrations. This does not block the user account, and allows the user to enroll again.

URI:

/admin/api/{API_KEY}/user/{IDENTITY_TYPE}/{IDENTITY_VALUE}/revokeAll

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/user/Email/bob@company.net/revokeAll

Device Queries

When specifying which device should be queried or manipulated by a request, the devices can be specified by *MACAddress*. Many of the requests contain a section similar to *MACAddress/A1:B2:C3:D4:E5:F6*, meaning any environment where the device *MAC address* is *A1:B2:C3:D4:E5:F6*.

Block/Unblock Device

Blocks the specified device.

URI:

```
/admin/api/{API_KEY}/device/{IDENTITY_TYPE}/{IDENTITY_VALUE}/block  
/admin/api/{API_KEY}/device/{IDENTITY_TYPE}/{IDENTITY_VALUE}/unblock
```

Examples:

```
http://test.company.net/admin/api/zAdBCLcgrwca/device/MACAddress/A1:B2:C3:D4:E5:F6/block
```

Unblocks the specified device.

```
http://test.company.net/admin/api/zAdBCLcgrwca/device/MACAddress/A1:B2:C3:D4:E5:F6/  
unblock
```

Revoke Certificates

Revokes all certificate for the specified device.

URI:

```
/admin/api/{API_KEY}/device/{IDENTITY_TYPE}/{IDENTITY_VALUE}/revokeAll
```

Example:

```
http://test.company.net/admin/api/zAdBCLcgrwca/device/MACAddress/A1:B2:C3:D4:E5:F6/  
revokeAll
```

Register MAC address

Registers the MAC address for the specified device to a specified MAC Registration list.

URI:

```
/admin/api/{API_KEY}/device/registerMac
```

Parameters:

- *macRegistrationName* - Required. The name of the MAC registration list.
- *macAddress* - Required. The MAC address to register.
- *username* - Optional. If specified, this value is saved as the associated username.
- *email* - Optional. If specified, this value is saved as the associated email.
- *deviceName* - Optional. If specified, this value is saved as the device name.

- location - Optional. If specified, this value is saved as the location.
- expirationDate - Optional. If specified, this value overrides the default expiration date.

Note >>

The *expirationDate* must be entered using the UNIX time format (yyyymmdd), regardless of the date format of the system.

Example:

```
http://test.company.net/admin/api/zAdBCLcgrwca/device/
RegisterMac?macRegistrationName=MacRegList1&macAddress=A1:B2:C3:D4:E5:F6
```

Device Configuration Queries and Actions

Generate Mobileconfig File

Generates a signed mobileconfig file containing a certificate and device configuration. This query supports the optional parameters for *validForDaysOverride* and *description*, and *CUSTOM_VARIABLES* (any variable used in the certificate template must also be provided as a parameter).

URI:

```
/admin/api/{API_KEY}/deviceConfig/generateMobileconfig
```

Parameters:

- deviceConfigName - Required. Name of the device configuration in Cloudpath from which to use.
- certificateTemplateName - Required. Name of certificate template in Cloudpath from which to issue.
- validForDaysOverride - Optional. If not zero, this overrides the expiration date specified in the certificate template.

Example:

```
http://test.company.net/admin/api/zAdBCLcgrwca/deviceConfig/
generateMobileconfig?deviceConfigName=SecureNetwork1&certificateTemplateName=CertTemplat
e1
```

External Queries

Certain external queries (checkCapability and authorizeDevice) require the location URL name, which is specified in the *URL Name* field on the *Configuration > Workflows*, Properties tab.

FIGURE 2. Location URL Name

The screenshot shows a web interface for configuring workflows. At the top, there is a breadcrumb 'Configuration > Workflows' and an 'Add Workflow' button. Below this is a table with columns: Workflows, Status, Published URL, and Last Publish Time. The table contains one entry: 'Production' with a green 'Published' status, a URL '/enroll/Anna44TestXPC/Production/', and a publish time of '20170404 1035 MDT'. Below the table are tabs for 'Properties', 'Enrollment Process', 'Look & Feel', 'Snapshot(s)', and 'Advanced'. The 'Properties' tab is active, showing a 'Workflow Properties' section with a 'Name' field containing 'Production' and an empty 'Description' field. Below that is an 'Enrollment Portal URL Options' section with a 'URL Name' field containing 'Production' and two unchecked checkboxes: 'Enable DNS Shortcut' and 'Enforce Required Parameters'. A 'Save' button is located at the top right of the form area.

Workflows	Status	Published URL	Last Publish Time
Production	● Published	/enroll/Anna44TestXPC/Production/	20170404 1035 MDT

Workflow Properties

Name: *

Description:

Enrollment Portal URL Options

URL Name:

Enable DNS Shortcut:

Enforce Required Parameters:

The examples in this section use *Production* for the `locationUrlName`.

Device Capabilities Query

Queries the capabilities of a device based on the user agent and device configuration. An HS2R1 or HS2R2 response value is returned only if the HS2R1/HS2R2 *SSID Type* has been set for the device configuration.

URI:

`/admin/api/{apiKey}/external/{locationUrlName}/checkCapability`

GET/POST Parameters:

- `userAgent` - Required. A string representing the user agent of a device.
- `screenHeight` - Optional. Necessary to exclude iPhone 4s and iPad 2 and earlier devices from hotspot 2 support.
- `screenWidth` - Optional. Necessary to exclude iPhone 4s and iPad 2 and earlier devices from hotspot 2 support.

Example:

`http://test.company.net/admin/api/zAdBCLcgrwca/external/Production/checkCapability?userAgent=Mozilla%2F5.0%20(iPad%3B%20CPU%20OS%208_3%20like%20Mac%20OS%20X)%20AppleWebKit%2F537.51.1%20(KHTML%2C%20like%20Gecko)%20CriOS%2F30.0.1599.12%20Mobile%2F11A465%20Safari%2F8536.25%20`

Device Authorization

Authorizes a device using the customer account number and optional parameters.

URI:

`/admin/api/{apiKey}/external/{locationUrlName}/authorizeDevice`

GET/POST Parameters:

- `externalId` - Required. A string representing the customer account number. This can be up to 14 characters.
- `macAddress` - Optional. The device MAC address, formatted as aa:bb:cc:dd:ee:ff.
- `userAgent` - Optional. A string representing the user agent of a device.
- `username` - Optional. Username of the device.
- `screenHeight` - Optional. Necessary to exclude iPhone 4s and iPad 2 and earlier devices from hotspot 2 support.
- `screenWidth` - Optional. Necessary to exclude iPhone 4s and iPad 2 and earlier devices from hotspot 2 support.

Note >>

The `userAgent` parameter is optional. However, if the user agent is not part of the enrollment record, other API calls may not return the correct OS family.

Optional parameters, if specified, are set in the device record.

Example:

`http://test.company.net/admin/api/zAdBCLcgrwca/external/Production/authorizeDevice?externalId=123456789012&macAddress=aa:bb:cc:dd:ee:ff&username=bob&userAgent=Mozilla%2F5.0%20(iPad%3B%20CPU%20OS%208_3%20like%20Mac%20OS%20X)%20AppleWebKit%2F537.51.1%20(KHTML%2C%20like%20Gecko)%20CriOS%2F30.0.1599.12%20Mobile%2F11A465%20Safari%2F8536.25%20`

Change MAC Address

Changes the MAC address for an enrollment record.

URI:

`/admin/api/{apiKey}/external/changeMac`

GET/POST Parameters:

- **externalId** - Required. A string representing the customer account number. This can be up to 14 characters.
- **oldMacAddress** - Required. The MAC address currently populated in the enrollment record, formatted as aa:bb:cc:dd:ee:ff.
- **newMacAddress** - Required. The new MAC address to be set in the enrollment record, formatted as aa:bb:cc:dd:ff.

Example:

```
http://test.company.net/admin/api/zAdBCLcgrwca/external/
changeMac?externalId=123456789012&oldMacAddress=aa:bb:cc:dd:ee:ff&newMacAddress=11:22:3
3:44:55:66
```

Get Device Information by Certificate Serial Number

Queries the customer account number and MAC address associated with a certificate serial number. The associated information is returned regardless of revocation status.

URI:

```
/admin/api/{apiKey}/external/getDeviceBySerialNumber
```

GET/POST Parameters:

- **certificateSerialNumber** - Required. The serial number of the client certificate to query, formatted 00fde721f1bb5e45e3feb7b49e1e8728b561936b. The serial number must be exactly 40 characters. If less than 40 characters, the value must be left-padded with zeros.

Example:

```
http://test.company.net/admin/api/zAdBCLcgrwca/external/
getDeviceBySerialNumber?certificateSerialNumber=00fde721f1bb5e45e3feb7b49e1e8728b561936b
```

Get Devices Associated with a Customer Account Number

Returns all devices associated with a customer account number.

Note >>

This call places a heavy load on the system.

URI:

```
/admin/api/{apiKey}/external/getDevices
```

GET/POST Parameters:

- **externalId** - Required. A string representing the customer account number. This can be up to 14 characters.
- **includeRevoked** - Optional. If '1', the response includes revoked enrollments and certificates. If not specified or '0', revoked enrollments and certificates are excluded from the response.

Example:

<http://test.company.net/admin/api/zAdBCLcgrwca/external/getDevices?externalId=123456789012>

Get Device Information by MAC Address and Customer Account Number

Returns the data associated with a customer account number and specified MAC address.

URI:

`/admin/api/{apiKey}/external/getDeviceByMacAddress`

GET/POST Parameters:

- `externalId` - Required. A string representing the customer account number. This can be up to 14 characters.
- `macAddress` - Required. The device MAC address, formatted as `aa:bb:cc:dd:ee:ff`.

Example:

<http://test.company.net/admin/api/zAdBCLcgrwca/external/getDevice?externalId=CustomerA&macAddress=00:bb:cc:dd:ee:ff>

Revoke Certificate by MAC Address and Customer Account Number

Revokes one or more certificates associated with a customer account number and specified MAC address.

URI:

`/admin/api/{apiKey}/external/revokeByMacAndExternalId`

GET/POST Parameters:

- `externalId` - Required. A string representing the customer account number. This can be up to 14 characters.
- `macAddress` - Required. The device MAC address, formatted as `aa:bb:cc:dd:ee:ff`.
- `destroy` - Optional. If specified and set to '1', the enrollment record(s) are permanently deleted rather than revoked. This causes the enrollment record and all associated data (including certificates) to be permanently deleted. After deletion, the log will be the only record of the existence of the certificate. OCSP responses will be "not found".

Example:

<http://test.company.net/admin/api/zAdBCLcgrwca/external/revokeByMacAndExternalId?externalId=CustomerA&macAddress=00:bb:cc:dd:ee:ff>

Clear Device Capability Cache (For Testing Only)

This method allows the cache to be flushed without restarting the server.

Note >>

Caching occurs by a combination of the user agent and location. The only time the cache should need to be cleared is if the location's device configuration is changed.

URI:

/admin/api/{apiKey}/external/clearCache

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/external/clearCache

Destroy Enrollment Records by Customer Account Number (For Testing Only)

Allows a call to destroy all elements for a specified customer account number.

URI:

/admin/api/{apiKey}/external/destroyByExternalIdForTestingOnly

GET/POST Parameters:

- externalId - Required. The customer account number for which all enrollments will be destroyed. If the externalId is blank, this call is ignored by the system.

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/external/destroyByExternalIdForTestingOnly?externalId=CustomerA

Destroy Enrollment Records by GUID

This method allows a caller to destroy all data related to an enrollment based on the enrollment's GUID. This causes the enrollment record and all associated data (including certificates) to be permanently deleted.

Note >>

After deletion, the log will contain the only record of the existence of the certificate in the system. OCSP responses will be "not found".

URI:

/admin/api/{apiKey}/external/destroyByEnrollmentGuid

GET/POST Parameters:

- guid - Required. The GUID for the enrollment to be destroyed.

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/external/destroyByEnrollmentGuid?guid=xyz

Logs

The system logs a message (at INFO level) containing the enrollment GUID, MAC address, external ID, certificate PK, certificate serial number, certificate thumbprint, certificate expiration date, MAC registration PK, and the MAC registration expiration date. If permanent storage is desired, use the syslog.

Modifying Settings in Cloudpath

Settings can be manipulated using REST APIs. When specifying which setting should be manipulated by a request, specify the *OBJECT_GUID* for *passphrase* information, and the desired parameter for *voucher* information. See the appropriate *Parameters* section for details.

Return Passphrase Information

Returns information about the specified shared passphrase.

URI:

/admin/api/{API_KEY}/object/ss/{OBJECT_GUID}/get

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/object/ss/SharedSecretPrompt-FC1C020C-6A62-4581-B661-18ED883831C2/get

Return Passphrase String

Returns only the shared passphrase string for a shared passphrase.

URI:

/admin/api/{API_KEY}/object/ss/{OBJECT_GUID}/get/ss

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/object/ss/SharedSecretPrompt-FC1C020C-6A62-4581-B661-18ED883831C2/get/ss

Change Passphrase

Changes the shared passphrase.

URI:

/admin/api/{API_KEY}/object/ss/{OBJECT_GUID}/change

Parameters:

- *newSs* - Optional. If specified, this value is used as the new shared passphrase. If not specified, a random shared passphrase is generated.
- *length* - Optional. If a random shared passphrase is generated, this will be the length of it.

Example:

http://test.company.net/admin/api/zAdBCLcgrwca/object/ss/SharedSecretPrompt-FC1C020C-6A62-4581-B661-18ED883831C2/change?newSs=brandnewpassphrase

Create Voucher Object

Sets a value in the voucher.

URI:

/admin/api/{API_KEY}/object/otp/{OBJECT_GUID}/create

Parameters:

- name - Optional. If specified, this value will be set as the name in the voucher.
- company - Optional. If specified, this value will be set as the company in the voucher.
- email - Optional. If specified, this value will be set as the email in the voucher.
- sponsor - Optional. If specified, this value will be set as the sponsor in the voucher.
- accessDays - Optional. If specified, this value will be set as the number of days of access in the voucher.
- sms - Optional. If specified, this value will be set as the SMS in the voucher.
- otp - Optional. If specified, this value will be set as the voucher in the voucher. If not specified, a random voucher will be generated.
- sendEmail - Optional. Defaults to 1. If 1, the user will be emailed the voucher code (if an email is populated).
- sendSms - Optional. Defaults to 1. If 1, the user will be sent the voucher code (if an SMS is populated) via SMS.
- daysToRedeem - Optional. Defaults to 3. If specified, this is the number of days within which the voucher must be redeemed.

Example:

`http://test.company.net/admin/api/zAdBCLcgrwca/object/otp/xyz/create?name=bob&email=bob@test.com&sendEmail=1`

Troubleshooting

To assist with troubleshooting, append the following to the API query.

- Append `?debug=true` for diagnostics.
- Append `?format=xml` for XML formatted response on GETs.

Error Messages

TABLE 1. Common API Error Messages

Error Code	Error Message
204	No records found matching parameters.
400	Invalid parameter or value.
401	Unauthorized.
500	Internal Server Error.