

Global Auth API

Developer Guide

API v1.0 (Feb 1, 2012)



docs.rackspace.com/api

Global Auth API Developer Guide

API v1.0 (2012-02-01)

Copyright © 2010-2012 Rackspace Hosting, Inc. All rights reserved.

This document is intended for software developers interested in developing applications which utilizes Global Auth API System as the authentication engine. It includes details on how to integrate with Global Auth API.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Table of Contents

1. Concepts	1
2. General API Information	2
2.1. Request/Response Types	2
2.2. Contracts	3
2.3. Faults	5
2.4. Getting Started	7
2.5. Authorization Header	7
3. Admin API (Service Developer Operations)	8
3.1. Token Operations	10
3.1.1. Authenticate	11
3.1.2. Validate Token	15
3.1.3. Revoke Token	17
3.1.4. Check if Token has access to an Application	18
3.1.5. Check if Token has Role on an Application	19
3.2. User Operations	19
3.2.1. Get Users	21
3.2.2. Add a User	23
3.2.3. Get a User	26
3.2.4. Update a User	27
3.2.5. Delete a User	29
3.2.6. Get User Secret Q/A	30
3.2.7. Set User Secret Q/A	31
3.2.8. Get User's Password	32
3.2.9. Set User's Password	33
3.2.10. Reset User's Password	34
3.2.11. Get Password Recovery Token	35
3.2.12. Get the Applications that a User has Provisioned	36
3.2.13. Provision an Application for a User	37
3.2.14. Remove Provisioned Application from a User	38
3.2.15. Get User Tenants Roles	39
3.2.16. Grant User Role on Tenant	41
3.2.17. Revoke a User Role on Tenant	42
3.2.18. Get User Global Roles	43
3.2.19. Grant User a Global Role	44
3.2.20. Remove User's Global Role	45
3.3. Application Operations	45
3.3.1. Get Applications	47
3.3.2. Add an Application	49
3.3.3. Get an Application	51
3.3.4. Update an Application	52
3.3.5. Delete an Application	54
3.3.6. Reset Application's Secret	55
3.3.7. Get the Applications that an Application has Provisioned	56
3.3.8. Provision an Application for an Application	57
3.3.9. Remove Provisioned Application from an Application	58
3.3.10. Get Application Tenants Roles	59
3.3.11. Grant Application Role on Tenant	61
3.3.12. Revoke an Application Role on Tenant	62

3.3.13. Get Application Global Roles	63
3.3.14. Grant Application a Global Role	64
3.3.15. Remove Application's Global Role	65
3.4. Customer Identity Profile Operations	65
3.4.1. Adds a Customer's Identity Profile	66
3.4.2. Get a Customer's Identity Profile	67
3.4.3. Delete a Customer's Identity Profile	68
3.4.4. Updates a Customer's Identity Profile	69
3.4.5. Get Password Rotation Policy	70
3.4.6. Set Password Rotation Policy	71
3.4.7. Get Users	72
3.4.8. Get Applications	74
3.5. Password Operations	75
3.5.1. Get Password Rules	76
3.5.2. Password Validation Check	77
3.6. Role Operations	78
3.6.1. Get All Roles	79
3.6.2. Add a Role	80
3.6.3. Get Role	81
3.6.4. Modify a Role	82
3.6.5. Delete a Role	83

List of Tables

2.1. Response Types	2
2.2. Fault Types	6
2.3. Application Information needed to register with Global Auth API	7
3.1. Validate Token Request Parameters	15
3.2. Revoke Token Request Parameters	17
3.3. Check if Token has access to an Application Request Parameters	18
3.4. Check if Token has Role on an Application Request Parameters	19
3.5. Get Users Request Parameters	22
3.6. Add a User Request Parameters	24
3.7. Add a User Response Parameters	24
3.8. Get a User Request Parameters	26
3.9. Update a User Request Parameters	28
3.10. Delete a User Request Parameters	29
3.11. Get User Secret Q/A Request Parameters	30
3.12. Set User Secret Q/A Request Parameters	31
3.13. Get User's Password Request Parameters	32
3.14. Set User's Password Request Parameters	33
3.15. Reset User's Password Request Parameters	34
3.16. Get Password Recovery Token Request Parameters	35
3.17. Get the Applications that a User has Provisioned Request Parameters	36
3.18. Provision an Application for a User Request Parameters	37
3.19. Remove Provisioned Application from a User Request Parameters	38
3.20. Get User Tenants Roles Request Parameters	39
3.21. Grant User Role on Tenant Request Parameters	41
3.22. Revoke a User Role on Tenant Request Parameters	42
3.23. Get User Global Roles Request Parameters	43
3.24. Grant User a Global Role Request Parameters	44
3.25. Remove User's Global Role Request Parameters	45
3.26. Get Applications Request Parameters	47
3.27. Add an Application Request Parameters	50
3.28. Add an Application Response Parameters	50
3.29. Get an Application Request Parameters	51
3.30. Update an Application Request Parameters	53
3.31. Delete an Application Request Parameters	54
3.32. Reset Application's Secret Request Parameters	55
3.33. Get the Applications that an Application has Provisioned Request Parameters.....	56
3.34. Provision an Application for an Application Request Parameters	57
3.35. Remove Provisioned Application from an Application Request Parameters	58
3.36. Get Application Tenants Roles Request Parameters	59
3.37. Grant Application Role on Tenant Request Parameters	61
3.38. Revoke an Application Role on Tenant Request Parameters	62
3.39. Get Application Global Roles Request Parameters	63
3.40. Grant Application a Global Role Request Parameters	64
3.41. Remove Application's Global Role Request Parameters	65
3.42. Adds a Customer's Identity Profile Request Parameters	66
3.43. Adds a Customer's Identity Profile Response Parameters	66
3.44. Get a Customer's Identity Profile Request Parameters	67
3.45. Delete a Customer's Identity Profile Request Parameters	68

3.46. Updates a Customer's Identity Profile Request Parameters	69
3.47. Get Password Rotation Policy Request Parameters	70
3.48. Set Password Rotation Policy Request Parameters	71
3.49. Get Users Request Parameters	73
3.50. Get Applications Request Parameters	74
3.51. Get Password Rules Request Parameters	76
3.52. Password Validation Check Request Parameters	78
3.53. Get All Roles Request Parameters	79
3.54. Add a Role Request Parameters	80
3.55. Add a Role Response Parameters	80
3.56. Get Role Request Parameters	81
3.57. Modify a Role Request Parameters	82
3.58. Delete a Role Request Parameters	83

List of Examples

2.1. JSON Request with Headers	2
2.2. XML Response with Headers	2
2.3. Request with URI versioning	3
2.4. Service Profile Request	3
2.5. Service Profile Response	4
2.6. Service Contract Request	4
2.7. Service Contract Response	5
2.8. XML Fault Response	5
2.9. JSON Fault Response	5
2.10. XML Username Conflict Fault	6
2.11. JSON Username Conflict Fault	6
2.12. Authorization Header Request Format	7
3.1. Auth as Application Request: XML	11
3.2. Auth as Application Request: JSON	11
3.3. Auth as Application Response: XML	11
3.4. Auth as Application Response: JSON	11
3.5. Auth as Customer Request: XML	12
3.6. Auth as Customer Request: JSON	12
3.7. Auth as Customer Response: XML	12
3.8. Auth as Customer Response: JSON	12
3.9. Auth as Racker Request: XML	13
3.10. Auth as Racker Request: JSON	13
3.11. Auth as Racker with RSA token Request: XML	13
3.12. Auth as Racker with RSA token Request: JSON	13
3.13. Auth as Racker Response: XML	13
3.14. Auth as Racker Response: JSON	14
3.15. Validate Token Response: XML	15
3.16. Validate Token Response: JSON	15
3.17. Get Users Response: XML	21
3.18. Get Users Response: JSON	21
3.19. Add User Request: XML	23
3.20. Add User Request: JSON	23
3.21. Add User Response: XML	24
3.22. Add User Response: JSON	24
3.23. Get User Response: XML	26
3.24. Get User Response: JSON	26
3.25. Update User Request: XML	27
3.26. Update User Request: JSON	27
3.27. Update User Response: XML	27
3.28. Update User Response: JSON	27
3.29. Get User Secret Response: XML	30
3.30. Get User Secret Response: JSON	30
3.31. Set User Secret Request: XML	31
3.32. Set User Secret Request: JSON	31
3.33. Get Password Credentials Response: XML	32
3.34. Get Password Credentials Response: JSON	32
3.35. Set User Credential Request: XML	33
3.36. Set User Credential Request: JSON	33

3.37. Get Credentials Recovery Token Response: XML	35
3.38. Get Credentials Recovery Token Response: JSON	35
3.39. Get User Applications Response: XML	36
3.40. Get User Applications Response: JSON	36
3.41. Get User Tenant Roles Response: XML	39
3.42. Get User Tenant Roles Response: JSON	39
3.43. Get User Roles Response: XML	43
3.44. Get User Roles Response: JSON	43
3.45. Get Applications Response: XML	47
3.46. Get Applications Response: JSON	47
3.47. Add Application Request: XML	49
3.48. Add Application Request: JSON	49
3.49. Add Application Request: XML	49
3.50. Add Application Request: JSON	49
3.51. Get Application Response: XML	51
3.52. Get Application Response: JSON	51
3.53. Update Application Request: XML	52
3.54. Update Application Request: JSON	52
3.55. Update Application Response: XML	52
3.56. Update Application Response: JSON	52
3.57. Reset Application Secret Response: XML	55
3.58. Reset Application Secret Response: JSON	55
3.59. Get Provisioned Applications Response: XML	56
3.60. Get Provisioned Applications Response: JSON	56
3.61. Get Application Tenant Roles Response: XML	59
3.62. Get Application Tenant Roles Response: JSON	59
3.63. Get Application Roles Response: XML	63
3.64. Get Application Roles Response: JSON	63
3.65. Customer Identity Profile Add Request: XML	66
3.66. Customer Identity Profile Add Request: JSON	66
3.67. Get Customer Identity Profile Response: XML	67
3.68. Get Customer Identity Profile Response: JSON	67
3.69. Customer Identity Profile Update Request: XML	69
3.70. Customer Identity Profile Update Request: JSON	69
3.71. Password Rotation Policy Response: XML	70
3.72. Password Rotation Policy Response: JSON	70
3.73. Password Rotation Policy Request: XML	71
3.74. Password Rotation Policy Request: JSON	71
3.75. Get Users Response: XML	72
3.76. Get Users Response: JSON	72
3.77. Get Applications Response: XML	74
3.78. Get Applications Response: JSON	74
3.79. Get Password Rules Response: XML	76
3.80. Get Password Rules Response: JSON	76
3.81. Password Validation Request: XML	77
3.82. Password Validation Request: JSON	77
3.83. Password Validation Response: XML	77
3.84. Password Validation Response: JSON	77
3.85. Get Roles Response: XML	79
3.86. Get Roles Response: JSON	79
3.87. Add Role Request: XML	80

3.88. Add Role Request: JSON	80
3.89. Get Role Response: XML	81
3.90. Get Role Response: JSON	81
3.91. Update Role Request: XML	82
3.92. Update Role Request: JSON	82

1. Concepts

The Global Customer IDM system has several key concepts that are important to understand

Token	This is an opaque string that grants a client the right to access one or more Applications. Tokens may be revoked at any time and are valid for a finite duration..
User	This is a type of client associated with a person that has access to Rackspace Applications.
Application	An application is a user interface or service API that a client can interact with to consume specific business functionality. e.g Control Panel, Customer Service, Billing Service, etc.
Customer Identity Profile	This describes identity-related information about its associated customer. Examples include whether or not the customer is locked, its password rotation policy, etc.
Tenant	This is a container that contains a collection of a customers products and services that Rackspace provides.
Role	Clients interact with Applications to invoke specific functions. Applications use the Roles assigned to a client to determine what functions that client can perform in the context of those interactions. A Role in this context is basically analagous with a traditional LDAP role.

2. General API Information

This document is intended for software developers interested in developing applications which utilizes Global Auth API as the authentication engine. It includes details on how to integrate with Global Auth API.

The Global Auth API is implemented using a RESTful web service interface. All requests to authenticate and operate against the Global Auth API are performed using SSL over HTTP (HTTPS) on TCP port 443.

This Guide assumes the reader is familiar with RESTful web services, HTTP/1.1, and JSON and/or XML serialization formats.

2.1. Request/Response Types

The Global Auth API supports both the JSON and XML data serialization formats. The request format is specified using the `Content-Type` header and is required for operations that have a request body. The response format can be specified in requests using either the `Accept` header or adding an `.xml` or `.json` extension to the request URI. Note that it is possible for a response to be serialized using a format different from the request (see example below). If no response format is specified, XML is the default. If conflicting formats are specified using both an `Accept` header and a query extension, the query extension takes precedence.

Table 2.1. Response Types

Format	Accept Header	Query Extension	Default
JSON	application/json	.json	No
XML	application/xml	.xml	Yes

Example 2.1. JSON Request with Headers

```
POST /v1.0/token HTTP/1.1
Host: {host name TBD}
Content-Type: application/json
Accept: application/xml
```

```
{ "authCredentials": {
  "grant_type": "PASSWORD",
  "client_id": "8972348923400fdshasdf",
  "client_secret": "0923899flewriudsb",
  "username": "testuser",
  "password": "P@ssword1"
}
```

Example 2.2. XML Response with Headers

```
HTTP/1.1 200 OKAY
```

```
Date: Mon, 12 Nov 2010 15:55:01 GMT
Server: Apache
Content-Length:
Content-Type: application/xml; charset=UTF-8
```

```
<?xml version="1.0" encoding="UTF-8"?>

<auth xmlns="http://idm.api.rackspace.com/v1.0">
  <access_token
    expires_in="3600"
    id="ab48a9efdfedb23ty3494" />
  <refresh_token
    id="8792gdfskjbadf98y234r" />
  <user
    customerId="RCN-000-000-000"
    username="jqsmith" />
</auth>
```

2.2. Contracts

The Global Auth API uses a URI versioning scheme. The first element of the path contains the target version identifier (e.g. <https://idm.api.rackspace.com/v1.0/...>) All requests (except to query for contract version - see below) must contain a target version. Any features or functionality changes that would necessitate a break in API-compatibility will require a new version, which will result in the URI version being updated accordingly. When new API versions are released, older versions will be marked as **Deprecated**. Rackspace will work with developers and partners to ensure there is adequate time to migrate to the new version before deprecated versions are discontinued.

Example 2.3. Request with URI versioning

```
GET /v1.0/users HTTP/1.1
Host: idm.api.rackspace.com
Accept: application/xml
Authorization: ab48a9efdfedb23ty3494
```

Your application can programmatically determine available API contract versions by performing a **GET** on the root URL (i.e. with the version and everything to the right of it truncated) returned from the authentication system.

Example 2.4. Service Profile Request

```
GET HTTP/1.1
Host: idm.api.rackspace.com
Accept: application/xml
```

This operation does not require a request body.

Normal Response Code(s):200

Error Response Code(s):400, 500, 503

Your application can programmatically determine available API contract versions by performing a **GET** on the root URL (<https://idm.api.rackspace.com/>).

Example 2.5. Service Profile Response

```
<service-profile
  xmlns="http://service-registry.api.rackspace.com/service-profile"
  xmlns:atom="http://www.w3.org/2005/Atom"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="https://service-registry.api.rackspace.com/service-
profile ../../resources/xsd/service-profile-v2.0.xsd"

  id="000"
  name="Customer Idm"
  canonical-name="idm"
  dns-zone="idm.api.rackspace.com"
  service-model="Utility">

  <atom:link rel="self" href="https://idm.api.rackspace.com" />

  <short-description>Allows users access Rackspace resources and systems.</
short-description>

  <detailed-description>
    The customer idm api allows Rackspace clients to obtain tokens that can
    be used to access resources in Rackspace.
    It also allows clients manage identities and delegate access to
    resources.
  </detailed-description>

  <contract version="v1.0" status="BETA">
    <media-types>
      <media-type base="application/xml" type="application/vnd.rackspace.
idm-v1.0+xml">
        <atom:link rel="describedby" type="application/xml" href=
"${baseUrl}v1.0/docs/xsd/idmapi.xsd" />
      </media-type>
    </media-types>

    <atom:link rel="self" href="${baseUrl}v1.0"/>
    <atom:link rel="describedby" type="application/vnd.sun.wadl+xml" href=
"${baseUrl}v1.0/application.wadl" title="Wadl" />
    <atom:link rel="documentation" href="${baseUrl}docs/v1.0/developerguide.
pdf" title="Developer Guide"/>
  </contract>
</service-profile>
```

You can also obtain additional information about a contract version by performing a **GET** on the base version URL (e.g. <https://idm.api.rackspace.com/v1.0>).

Example 2.6. Service Contract Request

```
GET HTTP/1.1
Host: idm.api.rackspace.com/v1.0
Accept: application/xml
```

This operation does not require a request body.

Normal Response Code(s):200

Error Response Code(s):400, 500, 503

Example 2.7. Service Contract Response

```
<contract xmlns="http://service-registry.api.rackspace.com/service-
profile"
  xmlns:atom="http://www.w3.org/2005/Atom" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
  xsi:schemaLocation="https://service-registry.api.rackspace.com/service-
profile ../../resources/xsd/service-profile-v2.0.xsd"

  version="v1.0" status="BETA">

  <media-types>
    <media-type base="application/xml" type="application/vnd.rackspace.idm-
v1.0+xml">
      <atom:link rel="describedby" type="application/xml"
        href="https://idm.api.rackspace.com/v1.0/docs/xsd/idmapixsd" />
    </media-type>
  </media-types>

  <atom:link rel="self" href="https://idm.api.rackspace.com/v1.0" />
  <atom:link rel="describedby" type="application/vnd.sun.wadl+xml" href=
"https://idm.api.rackspace.com/v1.0/application.wadl" />
  <atom:link rel="documentation" href="https://idm.api.rackspace.com/docs/v1.
0/developerguide.pdf" />
</contract>
```

2.3. Faults

When an error occurs the system will return an HTTP error response code denoting the type of error. The system will also return additional information about the fault in the body of the response.

Example 2.8. XML Fault Response

```
<?xml version="1.0" encoding="UTF-8"?>

<serviceFault xmlns="http://common.api.rackspace.com/v1.0"
  code="500">
  <message>Fault</message>
  <details>Error Details...</details>
</serviceFault>
```

Example 2.9. JSON Fault Response

```
{ "serviceFault": {  
  "message": "Fault",  
  "details": "Error Details...",  
  "code": 500  
}
```

The error code is returned in the body of the response for convenience. The message section returns a human readable message. The details section is optional and may contain useful information for tracking down an error (e.g a stack trace).

The root element of the fault (serviceFault) may change depending on how important it is to explicitly identify a specific fault type for a service. E.g it might be important to a client to distinguish between usernameConflict and applicationConflict even though they both have an error code of 409. The following is an example of a usernameConflict error.

Example 2.10. XML Username Conflict Fault

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
  
<usernameConflict xmlns="http://idm.api.rackspace.com/v1.0"  
  code="409">  
  <message>Conflict.</message>  
  <details>Error Details.</details>  
</usernameConflict>
```

Example 2.11. JSON Username Conflict Fault

```
{ "usernameConflict": {  
  "message": "Conflict",  
  "details": "Error Details...",  
  "code": 409  
}
```

The following is a list of possible fault types along with their associated error codes.

Table 2.2. Fault Types

Fault Element	Associated Error Code	Expected in Most Requests
serviceFault	500	✓
badRequest	400	✓
serviceUnavailable	503	✓
unauthorized	401	✓
forbidden	403	
itemNotFound	404	
passwordValidation	400	
userDisabled	403	
applicationNameConflict	409	

Fault Element	Associated Error Code	Expected in Most Requests
usernameConflict	409	

From an XML schema perspective, all API faults are extensions of the base fault type Fault. When working with a system that binds XML to actual classes (such as JAXB), one should be capable of using Fault as a “catch-all” if there's no interest in distinguishing between individual fault types.

2.4. Getting Started

The first step to using the Global Auth API is registering your application with Global Auth. The Global Auth Team will need the following information in order to register your application.

Table 2.3. Application Information needed to register with Global Auth API

Item	Description	Example
Name	The name of the application	Cloud Servers API
Simple Name	A continuous lower case name	cloud_servers_api
Description	A human readable description of what the application does, which should be presentable to end users.	Cloud Servers API is ...

Once the Global Auth Team has this information we will add your application to the Global Auth System and send you the `clientId` and `clientSecret` that you will need in order to authenticate with the Global Auth API (see api details below for Authentication).

2.5. Authorization Header

Most calls made against the Global Auth API require the addition of an authorization header in the request.

The format of the authorization header is the access token id that belongs to the entity making the call. Here is an example request below

Example 2.12. Authorization Header Request Format

```
POST /v1.0/users HTTP/1.1
Host: {host name TBD}
Accept: application/xml
X-Auth-Token: ab48a9efdfedb23ty3494
```


3. Admin API (Service Developer Operations)

Verb	URI	Description
Token Operations		
POST	/v1.0/tokens	Authenticate a client and generate an access token.
GET	/v1.0/tokens/{tokenId}	Check that a token is valid and return the token details.
DELETE	/v1.0/tokens/{tokenId}	Revoke Token.
GET	/v1.0/tokens/{tokenId}/applications/{applicationId}	Check if token has access to an application.
GET	/v1.0/tokens/{tokenId}/applications/{applicationId}/roles/{roleId}	Check if token has role on an application.
User Operations		
GET	/v1.0/users?username=string&offset=int&limit=int	Gets a list of users.
POST	/v1.0/users	Adds a new user.
GET	/v1.0/users/{userId}	Get a user.
PUT	/v1.0/users/{userId}	Update a user.
DELETE	/v1.0/users/{userId}	Delete a user.
GET	/v1.0/users/{userId}/secret	Get a user's secret question and answer.
PUT	/v1.0/users/{userId}/secret	Sets a user's secret question and answer.
GET	/v1.0/users/{userId}/passwordcredentials	Get a user's password credentials.
PUT	/v1.0/users/{userId}/passwordcredentials	Sets a user's password credentials.
POST	/v1.0/users/{userId}/passwordcredentials	Reset a user's password credentials.
GET	/v1.0/users/{userId}/passwordcredentials/recoverytoken	Get a token that can be used to reset a user's password credentials.
GET	/v1.0/users/{userId}/applications	Get the applications that have been provisioned for a user.
PUT	/v1.0/users/{userId}/applications/{applicationId}	Provision an application for a user.
DELETE	/v1.0/users/{userId}/applications/{applicationId}	Removed a provisioned application from a user.
GET	/v1.0/users/{userId}/tenants/roles?applicationId=string&tenantId=string	Get a list of user's roles on all tenants.
PUT	/v1.0/users/{userId}/tenants/{tenantId}/roles/{roleId}	Grant user a role on the tenant
DELETE	/v1.0/users/{userId}/tenants/{tenantId}/roles/{roleId}	Revoke a user's role on a tenant.
GET	/v1.0/users/{userId}/roles?applicationId=string	Get a list of user's global roles.
PUT	/v1.0/users/{userId}/roles/{roleId}	Grant user a global role.
DELETE	/v1.0/users/{userId}/roles/{roleId}	Remove global role from user.
Application Operations		

Verb	URI	Description
GET	/v1.0/applications?name=string&offset=int&limit=int	Gets a list of applications.
POST	/v1.0/applications	Add an application.
GET	/v1.0/applications/{applicationId}	Get an application.
PUT	/v1.0/applications/{applicationId}	Update an application.
DELETE	/v1.0/applications/{applicationId}	Delete as application.
POST	/v1.0/applications/{applicationId}/secretcredentials	Reset application secret.
GET	/v1.0/applications/{applicationId}/applications	Get all applications that have been provisioned for this application..
PUT	/v1.0/applications/{applicationId}/applications/{provisionedApplicationId}	Provision an application for this application.
DELETE	/v1.0/applications/{applicationId}/applications/{provisionedApplicationId}	Removes a provisioned application from this application.
GET	/v1.0/applications/{applicationId}/tenants/roles?applicationId=string&tenantId=string	Get a list of applications's roles on all tenants.
PUT	/v1.0/applications/{applicationId}/tenants/{tenantId}/roles/{roleId}	Grant application a role on the tenant
DELETE	/v1.0/applications/{applicationId}/tenants/{tenantId}/roles/{roleId}	Revoke an application's role on a tenant.
GET	/v1.0/applications/{applicationId}/roles?applicationId=string	Get a list of applications's global roles.
PUT	/v1.0/applications/{applicationId}/roles/{roleId}	Grant application a global role.
DELETE	/v1.0/applications/{applicationId}/roles/{roleId}	Remove global role from application.
Customer Identity Profile Operations		
POST	/v1.0/customeridentityprofiles	Adds a customer's identity profile.
GET	/v1.0/customeridentityprofiles/{customerId}	Gets a customer's identity profile.
DELETE	/v1.0/customeridentityprofiles/{customerId}	Delete a customer's identity profile.
PUT	/v1.0/customeridentityprofiles/{customerId}	Updates a customer's identity profile.
GET	/v1.0/customeridentityprofiles/{customerId}/passwordrotationpolicy	Gets the password rotation policy for a customer.
PUT	/v1.0/customeridentityprofiles/{customerId}/passwordrotationpolicy	Sets the password rotation policy for a customer.
GET	/v1.0/customeridentityprofiles/{customerId}/users?offset=int&limit=int	Gets a list of users that this customer owns.
GET	/v1.0/customeridentityprofiles/{customerId}/applications?offset=int&limit=int	Gets a list of applications that this customer owns.
Password Operations		

Verb	URI	Description
GET	/v1.0/passwordrules	Get password rules.
POST	/v1.0/passwordrules/validation	Validate password to ensure it conforms to password rules.
Role Operations		
GET	/v1.0/roles?name= <i>string</i> &applicationId= <i>string</i>	Get all roles.
POST	/v1.0/roles	Add a new role.
GET	/v1.0/roles/{roleId}	Get a Role
PUT	/v1.0/roles/{roleId}	Modify an existing role.
DELETE	/v1.0/roles/{roleId}	Delete an existing role.

3.1. Token Operations

The operations described in this section allow service developers to get and validate access tokens.

Verb	URI	Description
POST	/v1.0/tokens	Authenticate a client and generate an access token.
GET	/v1.0/tokens/{tokenId}	Check that a token is valid and return the token details.
DELETE	/v1.0/tokens/{tokenId}	Revoke Token.
GET	/v1.0/tokens/{tokenId}/applications/{applicationId}	Check if token has access to an application.
GET	/v1.0/tokens/{tokenId}/applications/{applicationId}/roles/{roleId}	Check if token has role on an application.

3.1.1. Authenticate

Verb	URI	Description
POST	/v1.0/tokens	Authenticate a client and generate an access token.

Normal Response Code(s): 200, 203

Error Response Code(s): userDisabled (403), serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

There are various ways to authenticate in the global auth system. You can authenticate as a Racker, an application on behalf of a customer, or an application directly. Examples below show the different authentication mechanisms.

Example 3.1. Auth as Application Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<authCredentials
  xmlns="http://idm.api.rackspace.com/v1.0"
  client_secret="0923899flewriudsb"
  client_id="8972348923400fdshasdf"
  grant_type="CLIENT_CREDENTIALS" />
```

Example 3.2. Auth as Application Request: JSON

```
{ "authCredentials": {
  "grant_type": "CLIENT_CREDENTIALS",
  "client_id": "8972348923400fdshasdf",
  "client_secret": "0923899flewriudsb"
}
```

Example 3.3. Auth as Application Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<auth xmlns="http://idm.api.rackspace.com/v1.0">
  <access_token
    expires_in="3600"
    id="ab48a9efdfedb23ty3494" />
  <refresh_token
    id="8792gdfskjbadf98y234r" />
  <application
    customerId="RCN-000-000-000"
    clientId="781hhh47kj34kj3434" />
</auth>
```

Example 3.4. Auth as Application Response: JSON

```
{ "auth": {
  "accessToken": {
    "id": "ab48a9efdfedb23ty3494",
    "expiresIn": 3600
  },
  "refreshToken": {
```

```
{
  "id": "8792gdfskjbadf98y234r"
},
"user" : {
  "clientId": "781hhh47kj34kj3434",
  "customerId": "RCN-000-000-000",
}
}
```

Example 3.5. Auth as Customer Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<authCredentials
  xmlns="http://idm.api.rackspace.com/v1.0"
  password="P@ssword1"
  username="testuser"
  client_secret="0923899flewriudsb"
  client_id="8972348923400fdshasdf"
  grant_type="PASSWORD" />
```

Example 3.6. Auth as Customer Request: JSON

```
{
  "authCredentials": {
    "grant_type": "PASSWORD",
    "client_id": "8972348923400fdshasdf",
    "client_secret": "0923899flewriudsb",
    "username": "testuser",
    "password": "P@ssword1"
  }
}
```

Example 3.7. Auth as Customer Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<auth xmlns="http://idm.api.rackspace.com/v1.0">
  <access_token
    expires_in="3600"
    id="ab48a9efdfedb23ty3494" />
  <refresh_token
    id="8792gdfskjbadf98y234r" />
  <user
    customerId="RCN-000-000-000"
    username="jqsmith" />
</auth>
```

Example 3.8. Auth as Customer Response: JSON

```
{
  "auth": {
    "accessToken": {
      "id": "ab48a9efdfedb23ty3494",
      "expiresIn": 3600
    },
    "refreshToken": {
      "id": "8792gdfskjbadf98y234r"
    },
    "user" : {
```

```
"username": "jqsmith",
"customerId": "RCN-000-000-000",
}
}
```

Example 3.9. Auth as Racker Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<rackerCredentials
  xmlns="http://idm.api.rackspace.com/v1.0"
  password="password"
  username="racker.sso"
  client_secret="0923899flewriudsb"
  client_id="8972348923400fdshasdf"
  grant_type="PASSWORD" />
```

Example 3.10. Auth as Racker Request: JSON

```
{ "rackerCredentials": {
  "grant_type": "PASSWORD",
  "client_id": "8972348923400fdshasdf",
  "client_secret": "0923899flewriudsb",
  "username": "racker.sso",
  "password": "password"
}
}
```

Example 3.11. Auth as Racker with RSA token Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<rsaCredentials
  xmlns="http://idm.api.rackspace.com/v1.0"
  password="rsaToken"
  username="racker.sso"
  client_secret="0923899flewriudsb"
  client_id="8972348923400fdshasdf"
  grant_type="PASSWORD" />
```

Example 3.12. Auth as Racker with RSA token Request: JSON

```
{ "rsaCredentials": {
  "grant_type": "PASSWORD",
  "client_id": "8972348923400fdshasdf",
  "client_secret": "0923899flewriudsb",
  "username": "racker.sso",
  "password": "rsaToken"
}
}
```

Example 3.13. Auth as Racker Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<auth xmlns="http://idm.api.rackspace.com/v1.0">
```

```
<access_token
  expires_in="3600"
  id="ab48a9efdfedb23ty3494" />
<refresh_token
  id="8792gdfskjbadf98y234r" />
<racker username="john.so/">

</auth>
```

Example 3.14. Auth as Racker Response: JSON

```
{ "auth": {
  "accessToken": {
    "id": "ab48a9efdfedb23ty3494",
    "expiresIn": 3600
  },
  "refreshToken": {
    "id": "8792gdfskjbadf98y234r"
  },
  "racker" : {
    "username": "john.so"
  }
}
```

3.1.2. Validate Token

Verb	URI	Description
GET	/v1.0/tokens/{tokenId}	Check that a token is valid and return the token details.

Normal Response Code(s): 200, 203

Error Response Code(s): userDisabled (403), serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.15. Validate Token Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<auth xmlns="http://idm.api.rackspace.com/v1.0">
  <access_token
    expires_in="3600"
    id="ab48a9efdfedb23ty3494" />
  <user
    customerId="RCN-000-000-000"
    username="jqsmith">
    <roles xmlns="http://idm.api.rackspace.com/v1.0">
      <role name="network_admin" applicationId="compute"/>
      <role name="technical_reviewer" tenantId="57884" applicationId="swift"/>
    </roles>
  </user>
</auth>
```

Example 3.16. Validate Token Response: JSON

```
{ "auth": {
  "access_token": {
    "id": "ab48a9efdfedb23ty3494",
    "expires_in": "3600"
  },
  "user": {
    "username": "jqsmith",
    "customerId": "RCN-000-000-000",
  },
  "roles": [{ "name": "network_admin",
    "applicationId": "compute"},
    { "name": "technical_reviewer",
    "tenantId": "57884",
    "applicationId": "swift"},
    { "name": "admin",
    "tenantId": "cf_89983",
    "applicationId": "billing"}]
}
```

Table 3.1. Validate Token Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.

Name	Style	Type	Description
tokenId	template	String	

This operation does not require a request body.

3.1.3. Revoke Token

Verb	URI	Description
DELETE	/v1.0/tokens/{tokenId}	Revoke Token.

Normal Response Code(s): 204

Error Response Code(s): userDisabled (403), serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.2. Revoke Token Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
tokenId	template	String	

This operation does not require a request body and does not return a response body.

3.1.4. Check if Token has access to an Application

Verb	URI	Description
GET	/v1.0/tokens/{tokenId}/ applications/{applicationId}	Check if token has access to an application.

Normal Response Code(s): 204, 404

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.3. Check if Token has access to an Application Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
tokenId	template	String	
applicationId	template	String	

This operation does not require a request body and does not return a response body.

3.1.5. Check if Token has Role on an Application

Verb	URI	Description
GET	/v1.0/tokens/{tokenId}/ applications/{applicationId}/ roles/{roleId}	Check if token has role on an application.

Normal Response Code(s): 204, 404

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.4. Check if Token has Role on an Application Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
tokenId	template	String	
applicationId	template	String	
roleId	template	String	

This operation does not require a request body and does not return a response body.

3.2. User Operations

The operations described in this section allows service developers manage users.

Verb	URI	Description
GET	/v1.0/users?username= <i>string</i> & offset= <i>int</i> &limit= <i>int</i>	Gets a list of users.
POST	/v1.0/users	Adds a new user.
GET	/v1.0/users/{userId}	Get a user.
PUT	/v1.0/users/{userId}	Update a user.
DELETE	/v1.0/users/{userId}	Delete a user.
GET	/v1.0/users/{userId}/secret	Get a user's secret question and answer.
PUT	/v1.0/users/{userId}/secret	Sets a user's secret question and answer.
GET	/v1.0/users/{userId}/ passwordcredentials	Get a user's password credentials.
PUT	/v1.0/users/{userId}/ passwordcredentials	Sets a user's password credentials.
POST	/v1.0/users/{userId}/ passwordcredentials	Reset a user's password credentials.
GET	/v1.0/users/{userId}/ passwordcredentials/recoverytoken	Get a token that can be used to reset a user's password credentials.
GET	/v1.0/users/{userId}/applications	Get the applications that have been provisioned for a user.
PUT	/v1.0/users/{userId}/applications/ {applicationId}	Provision an application for a user.
DELETE	/v1.0/users/{userId}/applications/ {applicationId}	Removed a provisioned application from a user.

Verb	URI	Description
GET	/v1.0/users/{userId}/tenants/ roles?applicationId= <i>string</i> & tenantId= <i>string</i>	Get a list of user's roles on all tenants.
PUT	/v1.0/users/{userId}/tenants/ {tenantId}/roles/{roleId}	Grant user a role on the tenant
DELETE	/v1.0/users/{userId}/tenants/ {tenantId}/roles/{roleId}	Revoke a user's role on a tenant.
GET	/v1.0/users/{userId}/roles? applicationId= <i>string</i>	Get a list of user's global roles.
PUT	/v1.0/users/{userId}/roles/ {roleId}	Grant user a global role.
DELETE	/v1.0/users/{userId}/roles/ {roleId}	Remove global role from user.

3.2.1. Get Users

Verb	URI	Description
GET	/v1.0/users?username= <i>string</i> &offset= <i>int</i> &limit= <i>int</i>	Gets a list of users.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.17. Get Users Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<users xmlns="http://idm.api.rackspace.com/v1.0"
  limit="10"
  offset="0"
  totalRecords="2">
  <user
    enabled="true"
    region="America/Chicago"
    prefLanguage="US_en" displayName="John Smith"
    lastName="Smith" middleName="Quincy"
    firstName="John" personId="RPN-111-111-111"
    email="john.smith@example.org"
    customerId="RCN-000-000-000"
    username="jqsmith" />
  <user enabled="true"
    region="America/Chicago"
    prefLanguage="US_en" displayName="Bob Anderson"
    lastName="Anderson" middleName="Mark"
    firstName="Bob" personId="RPN-111-111-222"
    email="bob.anderson@example.org"
    customerId="RCN-000-000-000"
    username="bmanderson" />
</users>
```

Example 3.18. Get Users Response: JSON

```
{ "user": {
  "user": [
    {
      "username": "jqsmith",
      "customerId": "RCN-000-000-000",
      "email": "john.smith@example.org",
      "personId": "RPN-111-111-111",
      "firstName": "John",
      "middleName": "Quincy",
      "lastName": "Smith",
      "displayName": "John Smith",
      "prefLanguage": "US_en",
      "region": "America/Chicago",
      "enabled": true
    },
    {
      "username": "bmanderson",
      "customerId": "RCN-000-000-000",
```

```
{
  "email": "bob.anderson@example.org",
  "personId": "RPN-111-111-222",
  "firstName": "Bob",
  "middleName": "Mark",
  "lastName": "Anderson",
  "displayName": "Bob Anderson",
  "prefLanguage": "US_en",
  "timeZone": "America/Chicago",
  "region": "SAT",
  "enabeld": true
},
"totalRecords": 2,
"offset": 0,
"limit": 10
}
```

Table 3.5. Get Users Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
username	query	String	Allows you search for a user by username Optional.
offset	query	Int	0 based index to start list Optional.
limit	query	Int	Number of records to be returned Optional.

3.2.2. Add a User

Verb	URI	Description
POST	/v1.0/users	Adds a new user.

Normal Response Code(s): 200

Error Response Code(s): passwordValidationFault (400), usernameConflict (409), serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

The Username attribute is required in this request. If a blank password is passed in the Password element, the API will generate a random password for the user. The prefLanguage attribute defaults to "US_en" and the timeZone attribute defaults to "America/Chicago".

Example 3.19. Add User Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>
<user xmlns="http://idm.api.rackspace.com/v1.0"
  region="SAT" prefLanguage="US_en" timeZone="America/Chicago"
  displayName="John Smith" lastName="Smith"
  middleName="Quincy" firstName="John"
  personId="RPN-111-111-111"
  email="john.smith@example.org"
  customerId="RCN-000-000-000" username="jqsmith">
  <secret secretAnswer="Francis"
    secretQuestion="What is your dogs name?" />
  <passwordCredentials xmlns="http://idm.api.rackspace.com/v1.0" >
    <currentPassword password="C@n+f00lme!" />
  </passwordCredentials>
</user>
```

Example 3.20. Add User Request: JSON

```
{ "user": {
  "secret": {
    "secretAnswer": "Francis",
    "secretQuestion": "What is your dogs name?"
  },
  "passwordCredentials": {
    "currentPassword": {
      "password": "P@ssword1"
    }
  },
  "username": "jqsmith",
  "customerId": "RCN-000-000-000",
  "email": "john.smith@example.org",
  "personId": "RPN-111-111-111",
  "firstName": "John",
  "middleName": "Quincy",
  "lastName": "Smith",
  "displayName": "John Smith",
  "prefLanguage": "US_en",
  "region": "America/Chicago"
}
```


Example 3.21. Add User Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<user xmlns="http://idm.api.rackspace.com/v1.0"
  region="SAT" prefLanguage="US_en" timeZone="America/Chicago"
  displayName="John Smith" lastName="Smith"
  middleName="Quincy" firstName="John"
  personId="RPN-111-111-111"
  email="john.smith@example.org"
  customerId="RCN-000-000-000" username="jqsmith"
  timeZone="America/Chicago"
  prefLanguage="US_en"
  region="SAT">
  <secret secretAnswer="Francis"
    secretQuestion="What is your dogs name?" />
  <passwordCredentials xmlns="http://idm.api.rackspace.com/v1.0" >
    <currentPassword password="C@n+f00lme!" />
  </passwordCredentials>
</user>
```

Example 3.22. Add User Response: JSON

```
{ "user": {
  "secret": {
    "secretQuestion": "What is your dogs name?",
    "secretAnswer": "Francis"
  },
  "passwordCredentials": {
    "currentPassword": {
      "password": "C@n+f00lme!"
    }
  },
  "username": "jqsmith",
  "customerId": "RCN-000-000-000",
  "email": "john.smith@example.org",
  "personId": "RPN-111-111-111",
  "firstName": "John",
  "middleName": "Quincy",
  "lastName": "Smith",
  "displayName": "John Smith",
  "prefLanguage": "US_en",
  "timeZone": "America/Chicago",
  "region": "SAT",
  "enabled": "true",
  "softDeleted": false
}
```

Table 3.6. Add a User Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.

Table 3.7. Add a User Response Parameters

Name	Style	Type	Description
Location	header	String	Location to the uri of the newly created resource

Name	Style	Type	Description
			Required.

3.2.3. Get a User

Verb	URI	Description
GET	/v1.0/users/{userId}	Get a user.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.23. Get User Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<user
  xmlns="http://idm.api.rackspace.com/v1.0"
  softDeleted="false" locked="false"
  status="ACTIVE" region="America/Chicago"
  prefLanguage="US_en" displayName="John Smith"
  lastName="Smith" middleName="Quincy"
  firstName="John" personId="RPN-111-111-111"
  email="john.smith@example.org"
  customerId="RCN-000-000-000"
  username="jqsmith">
</user>
```

Example 3.24. Get User Response: JSON

```
{ "user": {
  "username": "jqsmith",
  "customerId": "RCN-000-000-000",
  "email": "john.smith@example.org",
  "personId": "RPN-111-111-111",
  "firstName": "John",
  "middleName": "Quincy",
  "lastName": "Smith",
  "displayName": "John Smith",
  "prefLanguage": "US_en",
  "region": "America/Chicago",
  "status": "ACTIVE",
  "locked": false,
  "softDeleted": false
}
```

Table 3.8. Get a User Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

This operation does not require a request body.

3.2.4. Update a User

Verb	URI	Description
PUT	/v1.0/users/{userId}	Update a user.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.25. Update User Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<user xmlns="http://idm.api.rackspace.com/v1.0"
  email="john.smith@somenewemail.org"
  username="jqsmith" />
```

Example 3.26. Update User Request: JSON

```
{ "user " : {
  "email": "john.smith@example.org",
  "username": "jqsmith"
}
```

Example 3.27. Update User Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<user xmlns="http://idm.api.rackspace.com/v1.0"
  timeZone="America/Chicago" prefLanguage="US_en"
  displayName="John Smith" lastName="Smith"
  middleName="Quincy" firstName="John"
  region="SAT" personId="RPN-111-111-111"
  email="john.smith@somenewemail.org"
  customerId="RCN-000-000-000" username="jqsmith" />
```

Example 3.28. Update User Response: JSON

```
{ "user": {
  "username": "jqsmith",
  "customerId": "RCN-000-000-000",
  "customerInum": "@!FFFF.FFFF.FFFF.FFFF!EEEE.EEEE",
  "email": "john.smith@somenewemail.org",
  "personId": "RPN-111-111-111",
  "firstName": "John",
  "middleName": "Quincy",
  "lastName": "Smith",
  "displayName": "John Smith",
  "prefLanguage": "US_en",
  "inum": "@!FFFF.FFFF.FFFF.FFFF!EEEE.EEEE!1111",
  "iname": "@Example.Smith*John",
  "region": "America/Chicago",
  "status": "ACTIVE",
```

```
"locked": false,  
"softDeleted": false  
}  
}
```

Table 3.9. Update a User Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

3.2.5. Delete a User

Verb	URI	Description
DELETE	/v1.0/users/{userId}	Delete a user.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.10. Delete a User Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

This operation does not require a request body and does not return a response body.

3.2.6. Get User Secret Q/A

Verb	URI	Description
GET	/v1.0/users/{userId}/secret	Get a user's secret question and answer.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.29. Get User Secret Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<secret xmlns="http://idm.api.rackspace.com/v1.0"
  secretAnswer="Not a very good one."
  secretQuestion="Is this a secret question?" />
```

Example 3.30. Get User Secret Response: JSON

```
{ "secret " : {
  "secretQuestion": "Is this a secret question?",
  "secretAnswer": "Not a very good one."
}
}
```

Table 3.11. Get User Secret Q/A Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

This operation does not require a request body.

3.2.7. Set User Secret Q/A

Verb	URI	Description
PUT	/v1.0/users/{userId}/secret	Sets a user's secret question and answer.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.31. Set User Secret Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<secret xmlns="http://idm.api.rackspace.com/v1.0"
  secretAnswer="Not a very good one."
  secretQuestion="Is this a secret question?" />
```

Example 3.32. Set User Secret Request: JSON

```
{ "secret ": {
  "secretQuestion": "Is this a secret question?",
  "secretAnswer": "Not a very good one."
}
```

Table 3.12. Set User Secret Q/A Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

This operation does not return a response body.

3.2.8. Get User's Password

Verb	URI	Description
GET	/v1.0/users/{userId}/passwordcredentials	Get a user's password credentials.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.33. Get Password Credentials Response: XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<passwordCredentials xmlns="http://idm.api.rackspace.com/v1.0" >
  <currentPassword password="mypassword" />
</passwordCredentials>
```

Example 3.34. Get Password Credentials Response: JSON

```
{ "passwordCredentials": {
  "currentPassword": {
    "password": "mypassword"
  }
}
```

Table 3.13. Get User's Password Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

This operation does not require a request body.

3.2.9. Set User's Password

Verb	URI	Description
PUT	/v1.0/users/{userId}/passwordcredentials	Sets a user's password credentials.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.35. Set User Credential Request: XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<passwordCredentials xmlns="http://idm.api.rackspace.com/v1.0"
  verifyCurrentPassword="true">
  <newPassword password="newpassword" />
  <currentPassword password="oldpassword" />
</passwordCredentials>
```

Example 3.36. Set User Credential Request: JSON

```
{ "passwordCredentials": {
  "newPassword": {
    "password": "newpassword"
  },
  "currentPassword": {
    "password": "oldpassword"
  },
  "verifyCurrentPassword" : "true"
}
```

Table 3.14. Set User's Password Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

This operation does not return a response body.

3.2.10. Reset User's Password

Verb	URI	Description
POST	/v1.0/users/{userId}/passwordcredentials	Reset a user's password credentials.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.15. Reset User's Password Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

This operation does not require a request body.

3.2.11. Get Password Recovery Token

Verb	URI	Description
GET	/v1.0/users/{userId}/passwordcredentials/recoverytoken	Get a token that can be used to reset a user's password credentials.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.37. Get Credentials Recovery Token Response: XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<token xmlns="http://idm.api.rackspace.com/v1.0"
  expires_in="3600"
  id="309487987f0892397a9439875900b" />
```

Example 3.38. Get Credentials Recovery Token Response: JSON

```
{ "token": {
  "id": "309487987f0892397a9439875900b",
  "expiresIn": 3600
}
}
```

Table 3.16. Get Password Recovery Token Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

This operation does not require a request body.

3.2.12. Get the Applications that a User has Provisioned

Verb	URI	Description
GET	/v1.0/users/{userId}/applications	Get the applications that have been provisioned for a user.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.39. Get User Applications Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<application xmlns="http://idm.api.rackspace.com/v1.0">
  <application
    name="Test Application2"
    customerId="RCN-000-000-000"
    clientId="ab4820dhcb39347" />
  <application
    name="Test Application2"
    customerId="RCN-000-000-000"
    clientId="632h389cv902bde" />
</application>
```

Example 3.40. Get User Applications Response: JSON

```
{ "application": {
  "application": [
    {
      "clientId": "ab4820dhcb39347",
      "customerId": "RCN-000-000-000",
      "name": "Test Application2",
    },
    {
      "clientId": "632h389cv902bde",
      "customerId": "RCN-000-000-000",
      "name": "Test Application2",
    }
  ]
}
```

Table 3.17. Get the Applications that a User has Provisioned Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	

This operation does not require a request body.

3.2.13. Provision an Application for a User

Verb	URI	Description
PUT	/v1.0/users/{userId}/applications/{applicationId}	Provision an application for a user.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.18. Provision an Application for a User Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	
applicationId	template	String	

This operation does not require a request body and does not return a response body.

3.2.14. Remove Provisioned Application from a User

Verb	URI	Description
DELETE	/v1.0/users/{userId}/applications/{applicationId}	Removed a provisioned application from a user.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Table 3.19. Remove Provisioned Application from a User Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	
applicationId	template	String	

This operation does not require a request body and does not return a response body.

3.2.15. Get User Tenants Roles

Verb	URI	Description
GET	/v1.0/users/{userId}/tenants/roles?applicationId=string&tenantId=string	Get a list of user's roles on all tenants.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.41. Get User Tenant Roles Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>
<roles xmlns="http://idm.api.rackspace.com/v1.0">
  <role name="network_admin" applicationId="compute" tenantId="332"/>
  <role name="technical_reviewer" tenantId="57884" applicationId="swift"/>
  <role name="admin" tenantId="cf_89983" applicationId="billing"/>
</roles>
```

Example 3.42. Get User Tenant Roles Response: JSON

```
{ "roles ": {
  "role": [
    {
      "name": "network_admin",
      "applicationId": "compute",
      "tenantId": "332"
    },
    {
      "name": "technical_reviewer",
      "tenantId": "57884",
      "applicationid": "swift"
    },
    {
      "name": "admin",
      "tenantId": "cf_89983",
      "applicationId": "billing"
    }
  ]
}
}
```

Table 3.20. Get User Tenants Roles Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	query	String	Filter list of user tenant roles by applicationId Optional.
tenantId	query	String	Filter list of user tenant roles by tenantId Optional.

Name	Style	Type	Description
userId	template	String	

3.2.16. Grant User Role on Tenant

Verb	URI	Description
PUT	/v1.0/users/{userId}/tenants/{tenantId}/roles/{roleId}	Grant user a role on the tenant

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Table 3.21. Grant User Role on Tenant Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	
tenantId	template	String	
roleId	template	String	

This operation does not require a request body and does not return a response body.

3.2.17. Revoke a User Role on Tenant

Verb	URI	Description
DELETE	/v1.0/users/{userId}/tenants/{tenantId}/roles/{roleId}	Revoke a user's role on a tenant.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Table 3.22. Revoke a User Role on Tenant Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	
tenantId	template	String	
roleId	template	String	

This operation does not require a request body and does not return a response body.

3.2.18. Get User Global Roles

Verb	URI	Description
GET	/v1.0/users/{userId}/roles? applicationId=string	Get a list of user's global roles.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.43. Get User Roles Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<roles xmlns="http://idm.api.rackspace.com/v1.0">
  <role id="23" name="network_admin" applicationId="compute"/>
  <role id="24" name="technical_reviewer" applicationId="swift"/>
  <role id="56" name="admin" />
</roles>
```

Example 3.44. Get User Roles Response: JSON

```
{ "roles": {
  "role": [
    {
      "name": "network_admin",
      "applicationId": "compute"
      "id": "23"
    },
    {
      "name": "technical_reviewer",
      "applicationid": "swift"
      "id": "24"
    }
    {
      "name": "admin",
      "id": "56"
    }
  ]
}
```

Table 3.23. Get User Global Roles Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	query	String	Filter list of user roles by applicationId Optional.
userId	template	String	

3.2.19. Grant User a Global Role

Verb	URI	Description
PUT	/v1.0/users/{userId}/roles/{roleId}	Grant user a global role.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

A global role is one that is not restricted just to a tenant. A global role could be application specific. A user could have the global admin role for the nova application, or a global admin role for all applications.

Table 3.24. Grant User a Global Role Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	
roleId	template	String	

This operation does not require a request body and does not return a response body.

3.2.20. Remove User's Global Role

Verb	URI	Description
DELETE	/v1.0/users/{userId}/roles/{roleId}	Remove global role from user.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Table 3.25. Remove User's Global Role Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
userId	template	String	
roleId	template	String	

This operation does not require a request body and does not return a response body.

3.3. Application Operations

The operations described in this section allows service developers manage applications.

Verb	URI	Description
GET	/v1.0/applications?name=string&offset=int&limit=int	Gets a list of applications.
POST	/v1.0/applications	Add an application.
GET	/v1.0/applications/{applicationId}	Get an application.
PUT	/v1.0/applications/{applicationId}	Update an application.
DELETE	/v1.0/applications/{applicationId}	Delete as application.
POST	/v1.0/applications/{applicationId}/secretcredentials	Reset application secret.
GET	/v1.0/applications/{applicationId}/applications	Get all applications that have been provisioned for this application..
PUT	/v1.0/applications/{applicationId}/applications/{provisionedApplicationId}	Provision an application for this application.
DELETE	/v1.0/applications/{applicationId}/applications/{provisionedApplicationId}	Removes a provisioned application from this application.
GET	/v1.0/applications/{applicationId}/tenants/roles?applicationId=string&tenantId=string	Get a list of applications's roles on all tenants.
PUT	/v1.0/applications/{applicationId}/tenants/{tenantId}/roles/{roleId}	Grant application a role on the tenant
DELETE	/v1.0/applications/{applicationId}/tenants/{tenantId}/roles/{roleId}	Revoke an application's role on a tenant.

Verb	URI	Description
GET	/v1.0/applications/ {applicationId}/roles? applicationId= <i>string</i>	Get a list of applications's global roles.
PUT	/v1.0/applications/ {applicationId}/roles/{roleId}	Grant application a global role.
DELETE	/v1.0/applications/ {applicationId}/roles/{roleId}	Remove global role from application.

3.3.1. Get Applications

Verb	URI	Description
GET	/v1.0/applications?name= <i>string</i> &offset= <i>int</i> &limit= <i>int</i>	Gets a list of applications.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.45. Get Applications Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<application xmlns="http://idm.api.rackspace.com/v1.0">
  <application
    name="Test Application2"
    customerId="RCN-000-000-000"
    clientId="ab4820dhcb39347"/>
  <application
    name="Test Application2"
    customerId="RCN-000-000-000"
    clientId="632h389cv902bde"/>
</application>
```

Example 3.46. Get Applications Response: JSON

```
{ "application": {
  "application": [
    {
      "clientId": "ab4820dhcb39347",
      "customerId": "RCN-000-000-000",
      "name": "Test Application2",
    },
    {
      "clientId": "632h389cv902bde",
      "customerId": "RCN-000-000-000",
      "name": "Test Application2",
    }
  ]
}
```

Table 3.26. Get Applications Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
name	query	String	Allows you search for an application by name Optional.
offset	query	Int	0 based index to start list Optional.
limit	query	Int	Number of records to be returned

Name	Style	Type	Description
			Optional.

3.3.2. Add an Application

Verb	URI	Description
POST	/v1.0/applications	Add an application.

Normal Response Code(s): 200

Error Response Code(s): applicationNameConflict (409), serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Example 3.47. Add Application Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<application xmlns="http://idm.api.rackspace.com/v1.0"
  name="Test Application2"
  customerId="RCN-000-000-000"
  description="Used for adding all applications in Rackspace" />
```

Example 3.48. Add Application Request: JSON

```
{ "application":
  { "customerId": "RCN-000-000-000",
    "name": "Test Application2",
    "description": "Used for adding all applications in Rackspace"
  }
}
```

Example 3.49. Add Application Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<application xmlns="http://idm.api.rackspace.com/v1.0"
  softDeleted="false"
  enabled="true"
  name="Test Application2"
  customerId="RCN-000-000-000"
  clientId="ab4820dhcb39347">
  <secretCredentials clientSecret="3af738fbeiwu23" />
</application>
```

Example 3.50. Add Application Request: JSON

```
{ "application": {
  "secretCredentials": {
    "clientSecret": "3af738fbeiwu23"
  },
  "clientId": "ab4820dhcb39347",
  "customerId": "RCN-000-000-000",
  "name": "Test Application2",
  "enabled": true,
  "softDeleted": false
}
```

Table 3.27. Add an Application Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.

Table 3.28. Add an Application Response Parameters

Name	Style	Type	Description
Location	header	String	Location to the uri of the newly created resource Required.

3.3.3. Get an Application

Verb	URI	Description
GET	/v1.0/applications/{applicationId}	Get an application.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.51. Get Application Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<application xmlns="http://idm.api.rackspace.com/v1.0"
  softDeleted="false"
  enabled="true"
  name="Test Application2"
  customerId="RCN-000-000-000"
  clientId="ab4820dhcb39347" />
```

Example 3.52. Get Application Response: JSON

```
{ "application": {
  "clientId": "ab4820dhcb39347",
  "customerId": "RCN-000-000-000",
  "name": "Test Application2",
  "enabled": true,
  "softDeleted": false
}
```

Table 3.29. Get an Application Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	

This operation does not require a request body.

3.3.4. Update an Application

Verb	URI	Description
PUT	/v1.0/applications/{applicationId}	Update an application.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.53. Update Application Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<application xmlns="http://idm.api.rackspace.com/v1.0"
  scope="cloud_servers"
  clientId="ab4820dhcb39347" />
```

Example 3.54. Update Application Request: JSON

```
{ "application": {
  "clientId": "ab4820dhcb39347",
  "scope": "cloud_servers"
}
```

Example 3.55. Update Application Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<application xmlns="http://idm.api.rackspace.com/v1.0"
  softDeleted="false"
  locked="false"
  status="ACTIVE"
  iname="@Rackspace*Rackspace*ControlPanel"
  inum="@FFFF.FFFF.FFFF.FFFF!EEEE.EEEE!0001"
  name="Test Application2"
  customerId="RCN-000-000-000"
  clientId="ab4820dhcb39347"
  scope="cloud_servers" />
```

Example 3.56. Update Application Response: JSON

```
{ "application": {
  "clientId": "ab4820dhcb39347",
  "customerId": "RCN-000-000-000",
  "name": "Test Application2",
  "inum": "@FFFF.FFFF.FFFF.FFFF!EEEE.EEEE!0001",
  "scope": "cloud_servers",
  "status": "ACTIVE",
  "locked": false,
  "softDeleted": false
}
```

Table 3.30. Update an Application Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	

3.3.5. Delete an Application

Verb	URI	Description
DELETE	/v1.0/applications/{applicationId}	Delete as application.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.31. Delete an Application Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	

This operation does not require a request body and does not return a response body.

3.3.6. Reset Application's Secret

Verb	URI	Description
POST	/v1.0/applications/ {applicationId}/secretcredentials	Reset application secret.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.57. Reset Application Secret Response: XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<secretCredentials xmlns="http://idm.api.rackspace.com/v1.0"
  clientSecret="cncv9823823bfb" />
```

Example 3.58. Reset Application Secret Response: JSON

```
{ "secretCredentials": {
  "clientSecret": "cncv9823823bfb"
}
```

Table 3.32. Reset Application's Secret Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	

This operation does not require a request body.

3.3.7. Get the Applications that an Application has Provisioned

Verb	URI	Description
GET	/v1.0/applications/ {applicationId}/applications	Get all applications that have been provisioned for this application..

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.59. Get Provisioned Applications Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://idm.api.rackspace.com/v1.0">
  <application
    name="Test Application2"
    customerId="RCN-000-000-000"
    clientId="ab4820dhcb39347" />
  <application
    name="Test Application2"
    customerId="RCN-000-000-000"
    clientId="632h389cv902bde" />
</application>
```

Example 3.60. Get Provisioned Applications Response: JSON

```
{ "application": {
  "application": [
    {
      "clientId": "ab4820dhcb39347",
      "customerId": "RCN-000-000-000",
      "name": "Test Application2",
    },
    {
      "clientId": "632h389cv902bde",
      "customerId": "RCN-000-000-000",
      "name": "Test Application2",
    }
  ]
}
```

Table 3.33. Get the Applications that an Application has Provisioned Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	

This operation does not require a request body.

3.3.8. Provision an Application for an Application

Verb	URI	Description
PUT	/v1.0/applications/ {applicationId}/applications/ {provisionedApplicationId}	Provision an application for this application.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.34. Provision an Application for an Application Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	
provisionedApplicationId	template	String	

This operation does not require a request body and does not return a response body.

3.3.9. Remove Provisioned Application from an Application

Verb	URI	Description
DELETE	/v1.0/applications/ {applicationId}/applications/ {provisionedApplicationId}	Removes a provisioned application from this application.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.35. Remove Provisioned Application from an Application Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	
provisionedApplicationId	template	String	

This operation does not require a request body and does not return a response body.

3.3.10. Get Application Tenants Roles

Verb	URI	Description
GET	/v1.0/applications/ {applicationId}/tenants/ roles?applicationId=string& tenantId=string	Get a list of applications's roles on all tenants.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.61. Get Application Tenant Roles Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<roles xmlns="http://idm.api.rackspace.com/v1.0">
  <role name="network_admin" applicationId="compute" tenantId="332"/>
  <role name="technical_reviewer" tenantId="57884" applicationId="swift"/>
  <role name="admin" tenantId="cf_89983" applicationId="billing"/>
</roles>
```

Example 3.62. Get Application Tenant Roles Response: JSON

```
{ "roles ": {
  "role": [
    {
      "name": "network_admin",
      "applicationId": "compute",
      "tenantId": "332"
    },
    {
      "name": "technical_reviewer",
      "tenantId": "57884",
      "applicationid": "swift"
    },
    {
      "name": "admin",
      "tenantId": "cf_89983",
      "applicationId": "billing"
    }
  ]
}
}
```

Table 3.36. Get Application Tenants Roles Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	query	String	Filter list of application tenant roles by applicationId Optional.
tenantId	query	String	Filter list of application tenant roles by tenantId

Name	Style	Type	Description
			Optional.
applicationId	template	String	

3.3.11. Grant Application Role on Tenant

Verb	URI	Description
PUT	/v1.0/applications/ {applicationId}/tenants/ {tenantId}/roles/{roleId}	Grant application a role on the tenant

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Table 3.37. Grant Application Role on Tenant Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	
tenantId	template	String	
roleId	template	String	

This operation does not require a request body and does not return a response body.

3.3.12. Revoke an Application Role on Tenant

Verb	URI	Description
DELETE	/v1.0/applications/ {applicationId}/tenants/ {tenantId}/roles/{roleId}	Revoke an application's role on a tenant.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Table 3.38. Revoke an Application Role on Tenant Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	
tenantId	template	String	
roleId	template	String	

This operation does not require a request body and does not return a response body.

3.3.13. Get Application Global Roles

Verb	URI	Description
GET	/v1.0/applications/ {applicationId}/roles? applicationId=string	Get a list of applications's global roles.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.63. Get Application Roles Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<roles xmlns="http://idm.api.rackspace.com/v1.0">
  <role id="23" name="network_admin" applicationId="compute"/>
  <role id="24" name="technical_reviewer" applicationId="swift"/>
  <role id="56" name="admin" />
</roles>
```

Example 3.64. Get Application Roles Response: JSON

```
{ "roles": {
  "role": [
    {
      "name": "network_admin",
      "applicationId": "compute"
      "id": "23"
    },
    {
      "name": "technical_reviewer",
      "applicationid": "swift"
      "id": "24"
    }
    {
      "name": "admin",
      "id": "56"
    }
  ]
}
```

Table 3.39. Get Application Global Roles Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	query	String	Filter list of application roles by applicationId Optional.
applicationId	template	String	

3.3.14. Grant Application a Global Role

Verb	URI	Description
PUT	/v1.0/applications/ {applicationId}/roles/{roleId}	Grant application a global role.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

A global role is one that is not restricted just to a tenant. A global role could be application specific. An application could have the global admin role for the nova application, or a global admin role for all applications.

Table 3.40. Grant Application a Global Role Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	
roleId	template	String	

This operation does not require a request body and does not return a response body.

3.3.15. Remove Application's Global Role

Verb	URI	Description
DELETE	/v1.0/applications/ {applicationId}/roles/{roleId}	Remove global role from application.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Table 3.41. Remove Application's Global Role Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
applicationId	template	String	
roleId	template	String	

This operation does not require a request body and does not return a response body.

3.4. Customer Identity Profile Operations

The operations described in this section allows service developers manage customer identity profiles.

Verb	URI	Description
POST	/v1.0/customeridentityprofiles	Adds a customer's identity profile.
GET	/v1.0/customeridentityprofiles/ {customerId}	Gets a customer's identity profile.
DELETE	/v1.0/customeridentityprofiles/ {customerId}	Delete a customer's identity profile.
PUT	/v1.0/customeridentityprofiles/ {customerId}	Updates a customer's identity profile.
GET	/v1.0/customeridentityprofiles/ {customerId}/ passwordrotationpolicy	Gets the password rotation policy for a customer.
PUT	/v1.0/customeridentityprofiles/ {customerId}/ passwordrotationpolicy	Sets the password rotation policy for a customer.
GET	/v1.0/customeridentityprofiles/ {customerId}/users?offset=int& limit=int	Gets a list of users that this customer owns.
GET	/v1.0/customeridentityprofiles/ {customerId}/applications? offset=int&limit=int	Gets a list of applications that this customer owns.

3.4.1. Adds a Customer's Identity Profile

Verb	URI	Description
POST	/v1.0/customeridentityprofiles	Adds a customer's identity profile.

Normal Response Code(s): 201

Error Response Code(s): customerIdConflict (409), serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Example 3.65. Customer Identity Profile Add Request: XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<customerIdentityProfile xmlns="http://idm.api.rackspace.com/v1.0"
  enabled="true"
  customerId="RCN-123-549-034" />
```

Example 3.66. Customer Identity Profile Add Request: JSON

```
{ "customerIdentityProfile": {
  "customerId": "RCN-123-549-034",
  "enabled": true,
}
}
```

Table 3.42. Adds a Customer's Identity Profile Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.

Table 3.43. Adds a Customer's Identity Profile Response Parameters

Name	Style	Type	Description
Location	header	String	Location to the uri of the newly created customer identity profile Required.

This operation does not return a response body.

3.4.2. Get a Customer's Identity Profile

Verb	URI	Description
GET	/v1.0/customeridentityprofiles/{customerId}	Gets a customer's identity profile.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.67. Get Customer Identity Profile Response: XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<customerIdentityProfile xmlns="http://idm.api.rackspace.com/v1.0"
  enabled="false"
  customerId="RCN-123-549-034" />
```

Example 3.68. Get Customer Identity Profile Response: JSON

```
{ "customerIdentityProfile": {
  "customerId": "RCN-123-549-034",
  "enabled": false,
}
}
```

Table 3.44. Get a Customer's Identity Profile Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
customerId	template	String	This is the customer's RCN.

This operation does not require a request body.

3.4.3. Delete a Customer's Identity Profile

Verb	URI	Description
DELETE	/v1.0/customeridentityprofiles/ {customerId}	Delete a customer's identity profile.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Table 3.45. Delete a Customer's Identity Profile Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
customerId	template	String	This is the customer's RCN.

This operation does not require a request body and does not return a response body.

3.4.4. Updates a Customer's Identity Profile

Verb	URI	Description
PUT	/v1.0/customeridentityprofiles/{customerId}	Updates a customer's identity profile.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.69. Customer Identity Profile Update Request: XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<customerIdentityProfile xmlns="http://idm.api.rackspace.com/v1.0"
  enabled="false"
  customerId="RCN-123-549-034" />
```

Example 3.70. Customer Identity Profile Update Request: JSON

```
{ "customerIdentityProfile": {
  "customerId": "RCN-123-549-034",
  "enabled": false,
}
}
```

Table 3.46. Updates a Customer's Identity Profile Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
customerId	template	String	This is the customer's RCN.

This operation does not return a response body.

3.4.5. Get Password Rotation Policy

Verb	URI	Description
GET	/v1.0/customeridentityprofiles/{customerId}/passwordrotationpolicy	Gets the password rotation policy for a customer.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.71. Password Rotation Policy Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<passwordRotationPolicy xmlns="http://idm.api.rackspace.com/v1.0"
  enabled="true"
  duration="90" />
```

Example 3.72. Password Rotation Policy Response: JSON

```
{ "passwordRotationPolicy": {
  "enabled": true,
  "duration": "60"
}
}
```

Table 3.47. Get Password Rotation Policy Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
customerId	template	String	This is the customer's RCN.

This operation does not require a request body.

3.4.6. Set Password Rotation Policy

Verb	URI	Description
PUT	/v1.0/customeridentityprofiles/{customerId}/passwordrotationpolicy	Sets the password rotation policy for a customer.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.73. Password Rotation Policy Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<passwordRotationPolicy xmlns="http://idm.api.rackspace.com/v1.0"
  enabled="true"
  duration="90" />
```

Example 3.74. Password Rotation Policy Request: JSON

```
{ "passwordRotationPolicy": {
  "enabled": true,
  "duration": "60"
}
}
```

Table 3.48. Set Password Rotation Policy Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
customerId	template	String	This is the customer's RCN.

This operation does not return a response body.

3.4.7. Get Users

Verb	URI	Description
GET	/v1.0/customeridentityprofiles/{customerId}/users?offset=int&limit=int	Gets a list of users that this customer owns.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.75. Get Users Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<users xmlns="http://idm.api.rackspace.com/v1.0"
  limit="10"
  offset="0"
  totalRecords="2">
  <user
    enabled="true"
    region="America/Chicago"
    prefLanguage="US_en" displayName="John Smith"
    lastName="Smith" middleName="Quincy"
    firstName="John" personId="RPN-111-111-111"
    email="john.smith@example.org"
    customerId="RCN-000-000-000"
    username="jqsmith" />
  <user enabled="true"
    region="America/Chicago"
    prefLanguage="US_en" displayName="Bob Anderson"
    lastName="Anderson" middleName="Mark"
    firstName="Bob" personId="RPN-111-111-222"
    email="bob.anderson@example.org"
    customerId="RCN-000-000-000"
    username="bmanderson" />
</users>
```

Example 3.76. Get Users Response: JSON

```
{ "user": {
  "user": [
    {
      "username": "jqsmith",
      "customerId": "RCN-000-000-000",
      "email": "john.smith@example.org",
      "personId": "RPN-111-111-111",
      "firstName": "John",
      "middleName": "Quincy",
      "lastName": "Smith",
      "displayName": "John Smith",
      "prefLanguage": "US_en",
      "region": "America/Chicago",
      "enabled": true
    },
    {
      "username": "bmanderson",
```

```
{
  "customerId": "RCN-000-000-000",
  "email": "bob.anderson@example.org",
  "personId": "RPN-111-111-222",
  "firstName": "Bob",
  "middleName": "Mark",
  "lastName": "Anderson",
  "displayName": "Bob Anderson",
  "prefLanguage": "US_en",
  "timeZone": "America/Chicago",
  "region": "SAT",
  "enabled": true
},
{
  "totalRecords": 2,
  "offset": 0,
  "limit": 10
}
```

Table 3.49. Get Users Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
offset	query	Int	0 based index to start list Optional.
limit	query	Int	Number of records to be returned Optional.
customerId	template	String	This is the customer's RCN.

3.4.8. Get Applications

Verb	URI	Description
GET	/v1.0/customeridentityprofiles/{customerId}/applications?offset=int&limit=int	Gets a list of applications that this customer owns.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.77. Get Applications Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://idm.api.rackspace.com/v1.0">
  <application
    name="Test Application2"
    customerId="RCN-000-000-000"
    clientId="ab4820dhcb39347"/>
  <application
    name="Test Application2"
    customerId="RCN-000-000-000"
    clientId="632h389cv902bde"/>
</application>
```

Example 3.78. Get Applications Response: JSON

```
{ "application": {
  "application": [
    {
      "clientId": "ab4820dhcb39347",
      "customerId": "RCN-000-000-000",
      "name": "Test Application2",
    },
    {
      "clientId": "632h389cv902bde",
      "customerId": "RCN-000-000-000",
      "name": "Test Application2",
    }
  ]
}
```

Table 3.50. Get Applications Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
offset	query	Int	0 based index to start list Optional.
limit	query	Int	Number of records to be returned Optional.
customerId	template	String	This is the customer's RCN.

Name	Style	Type	Description
------	-------	------	-------------

3.5. Password Operations

The operations described in this section allows service developers manage password policies.

Verb	URI	Description
GET	/v1.0/passwordrules	Get password rules.
POST	/v1.0/passwordrules/validation	Validate password to ensure it conforms to password rules.

3.5.1. Get Password Rules

Verb	URI	Description
GET	/v1.0/passwordrules	Get password rules.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.79. Get Password Rules Response: XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<passwordRuleResults
  xmlns="http://idm.api.rackspace.com/v1.0">
  <passwordRuleResults
    ruleMessage="Password must be at least 7 characters."
    ruleName="Minimum Length"
    ruleId="1"
    passed="true" />
  <passwordRuleResults
    ruleMessage="Password must contain a lowercase."
    ruleName="Lowercase Character"
    ruleId="2"
    passed="true" />
</passwordRuleResults>
```

Example 3.80. Get Password Rules Response: JSON

```
{ "passwordRuleResults": {
  "passwordRuleResult": [
    {
      "passed": true,
      "ruleId": 1,
      "ruleName": "Minimum Length",
      "ruleMessage": "Password must be at least 7 characters long."
    },
    {
      "passed": true,
      "ruleId": 2,
      "ruleName": "Lowercase Character",
      "ruleMessage": "Password must contain a lowercase character."
    }
  ]
}
```

Table 3.51. Get Password Rules Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.

This operation does not require a request body.

3.5.2. Password Validation Check

Verb	URI	Description
POST	/v1.0/passwordrules/validation	Validate password to ensure it conforms to password rules.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.81. Password Validation Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<userPassword xmlns="http://idm.api.rackspace.com/v1.0"
  password="newpassword" />
```

Example 3.82. Password Validation Request: JSON

```
{ "userPassword": {
  "password": "newpassword"
}
```

Example 3.83. Password Validation Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<passwordValidation xmlns="http://idm.api.rackspace.com/v1.0"
  validPassword="true">
  <passwordRuleResults>
    <passwordRuleResults
      ruleMessage="Password must be at least 7 characters long."
      ruleName="Minimum Length"
      ruleId="1"
      passed="true" />
    <passwordRuleResults
      ruleMessage="Password must contain a lowercase character."
      ruleName="Lowercase Character"
      ruleId="2"
      passed="true" />
  </passwordRuleResults>
</passwordValidation>
```

Example 3.84. Password Validation Response: JSON

```
{ "passwordValidation": {
  "passwordRuleResults": {
    "passwordRuleResults": [
      {
        "passed": true,
        "ruleId": 1, "ruleName":
        "Minimum Length",
        "ruleMessage": "The password must be at least 7 characters long"
      },

```

```
{
  "passed":false,
  "ruleId":2,"ruleName":
  "Uppercase Rule","ruleMessage":
  "The password must contain an uppercase charater"
},
"validPassword":false
}
```

Table 3.52. Password Validation Check Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.

3.6. Role Operations

The operations described in this section allows service developers manage roles.

Verb	URI	Description
GET	/v1.0/roles?name= <i>string</i> & applicationId= <i>string</i>	Get all roles.
POST	/v1.0/roles	Add a new role.
GET	/v1.0/roles/{roleId}	Get a Role
PUT	/v1.0/roles/{roleId}	Modify an existing role.
DELETE	/v1.0/roles/{roleId}	Delete an existing role.

3.6.1. Get All Roles

Verb	URI	Description
GET	/v1.0/roles?name= <i>string</i> &applicationId= <i>string</i>	Get all roles.

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.85. Get Roles Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<roles xmlns="http://idm.api.rackspace.com/v1.0">
  <role id="23" name="network_admin" applicationId="compute"/>
  <role id="24" name="technical_reviewer" applicationId="swift"/>
  <role id="56" name="admin" />
</roles>
```

Example 3.86. Get Roles Response: JSON

```
{ "roles": {
  "role": [
    {
      "name": "network_admin",
      "applicationId": "compute"
      "id": "23"
    },
    {
      "name": "technical_reviewer",
      "applicationid": "swift"
      "id": "24"
    }
    {
      "name": "admin",
      "id": "56"
    }
  ]
}
```

Table 3.53. Get All Roles Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
name	query	String	Name of the role Optional.
applicationId	query	String	Application that role is tied to. Optional.

3.6.2. Add a Role

Verb	URI	Description
POST	/v1.0/roles	Add a new role.

Normal Response Code(s): 201

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Adds a role to the specified application.

Example 3.87. Add Role Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<role xmlns="http://idm.api.rackspace.com/v1.0" name="admin"
  description="Can admin the heck out of anything" applicationId=
  "18e7a7032733486cd32f472d7bd58f709ac0d221" />
```

Example 3.88. Add Role Request: JSON

```
{ "role": {
  "name": "admin",
  "description": "Can admin the heck out of anything",
  "applicationId": "18e7a7032733486cd32f472d7bd58f709ac0d221"
}
```

Table 3.54. Add a Role Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.

Table 3.55. Add a Role Response Parameters

Name	Style	Type	Description
Location	header	String	Location to the uri of the newly created role Required.

This operation does not return a response body.

3.6.3. Get Role

Verb	URI	Description
GET	/v1.0/roles/{roleId}	Get a Role

Normal Response Code(s): 200

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503), itemNotFound (404)

Example 3.89. Get Role Response: XML

```
<?xml version="1.0" encoding="UTF-8"?>
<role id="452" name="admin" />
```

Example 3.90. Get Role Response: JSON

```
{ "role": {
  "id": "452",
  "name": "admin"
}}
```

Table 3.56. Get Role Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
roleId	template	String	

This operation does not require a request body.

3.6.4. Modify a Role

Verb	URI	Description
PUT	/v1.0/roles/{roleId}	Modify an existing role.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Example 3.91. Update Role Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>

<role xmlns="http://idm.api.rackspace.com/v1.0" name="admin"
  description="Can admin the heck out of anything" applicationId=
  "18e7a7032733486cd32f472d7bd58f709ac0d221" />
```

Example 3.92. Update Role Request: JSON

```
{ "role": {
  "name": "admin",
  "description": "Can admin the heck out of anything",
  "applicationId": "18e7a7032733486cd32f472d7bd58f709ac0d221"
}
```

Table 3.57. Modify a Role Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
roleId	template	String	

This operation does not return a response body.

3.6.5. Delete a Role

Verb	URI	Description
DELETE	/v1.0/roles/{roleId}	Delete an existing role.

Normal Response Code(s): 204

Error Response Code(s): serviceFault (500), badRequest (400), unauthorized (401), forbidden (403), serviceUnavailable (503)

Table 3.58. Delete a Role Request Parameters

Name	Style	Type	Description
X-Auth-Token	header	String	You need a valid token for access. Required.
roleId	template	String	

This operation does not require a request body and does not return a response body.