

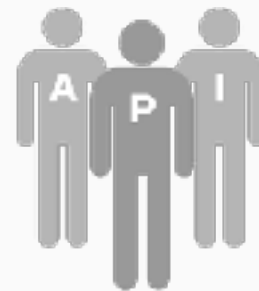


Edge Overview Series

Role-based Access Control (RBAC)

Edge – Role-Based Access Control

- **Permissions** define create/read/update/delete access to resources
- **Roles** identify a collection of permissions that can be assigned to a user
- **Custom Roles** can be created to augment the prebuilt roles



User

- API Developer
- Creates API proxies and tests them in the test environment

Business User

- API program manager
- Creates and manages API products, developers, apps, companies; creates custom reports

Developer Administrator

- Community Manager
- DevPortal integration to Edge and should not be used for any other users

Operations Administrator

- API Operation Manager
- Deploys and tests APIs

Read Only Organization Administrator

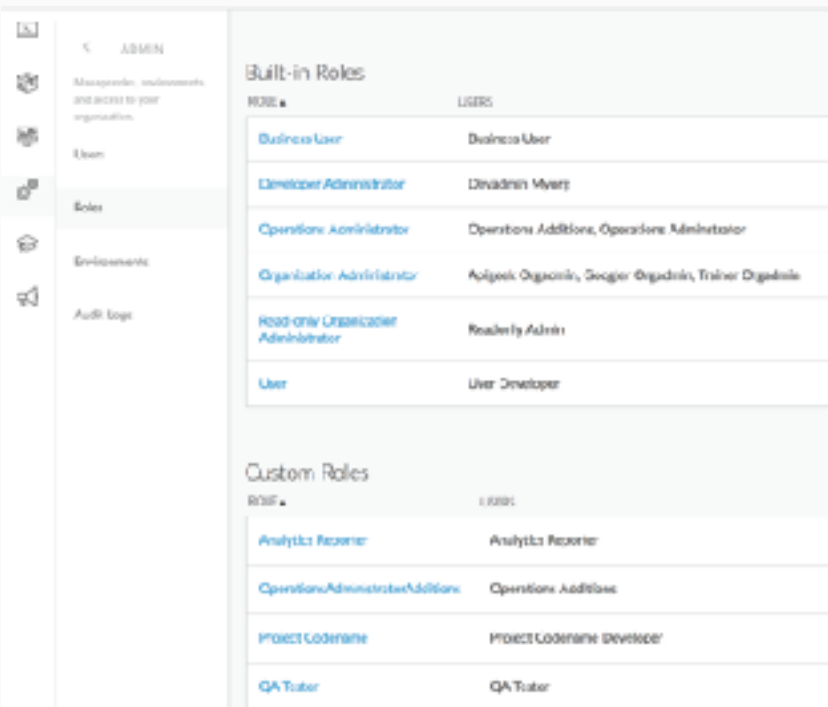
- Read-only access to all resources in the organization

Organization Administrator

- Administrator of an organization
- Superuser, full CRUD access to resources in the organization

Roles and Permissions Management

Management UI



The screenshot displays the Apigee Management UI. On the left is a sidebar with navigation icons and labels: ADMIN, Manage roles, permissions, and access to your organization, Users, Roles (highlighted), Environments, and Audit logs. The main content area is titled 'Built-in Roles' and contains a table with columns 'ROLE' and 'USERS'. Below this is a section for 'Custom Roles' with a similar table structure.

ROLE	USERS
Business User	Business User
Developer Administrator	Devadmin Myert
Operations Administrator	Operations Additions, Operations Administrator
Organization Administrator	Apigee Organization, Google Organization, Trainer Organization
Read-only Organization Administrator	Readonly Admin
User	User Developer

ROLE	USERS
Analytics Reporter	Analytics Reporter
Operations Administrator Additions	Operations Additions
PROJECT CODENAME	PROJECT CODENAME DEVELOPER
QA Tester	QA Tester

Documentation

<http://docs.apigee.com/api-services/content/edge-built-roles>

<http://docs.apigee.com/api-services/content/managing-roles-api>

Management API

<https://api.enterprise.apigee.com/v1/o/{org}/userroles>

<https://api.enterprise.apigee.com/v1/o/{org}/userroles/{role}/permissions>

<https://api.enterprise.apigee.com/v1/o/{org}/userroles/{role}/users>

<https://api.enterprise.apigee.com/v1/users/{user}/userroles>

[illegible]

- Role Restricted Developer
- Analytics Reporter
- QA Tester
- Existing Resources Developer

- Role Restricted Developer
- Analytics Reporter
- QA Tester
- Existing Resources Developer

Custom Roles - Role Restricted Developer

Organization Roles > Project Codename

API Profiles

API Profile	Operations	Permissions
API Profile	View, Edit, Delete	200, 400, 401, 403, 404, 405, 406, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500

Statement Roles

Environments

Environment	Operations	Permissions
prod	View, Edit, Delete	200, 400, 401, 403, 404, 405, 406, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500

Products

Product	Operations	Permissions
Product	View, Edit, Delete	200, 400, 401, 403, 404, 405, 406, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500

Developers and Apps

Developer/App	Operations	Permissions
Developer	View, Edit, Delete	200, 400, 401, 403, 404, 405, 406, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500

Reports

Report	Operations	Permissions
Report	View, Edit, Delete	200, 400, 401, 403, 404, 405, 406, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500

Key Concepts

- Newly created resources by users in a custom role are only visible to users in that role.
- Apps and Developers consuming resources are not restricted and reside at the org level.

Custom Roles - Analytics Reporter



Key Concepts

- View built in reports
- Creating and run custom reports

Custom Roles - QA Tester



Key concepts

- Trace proxy to view coverage
- Verify boundary conditions
- Adjust configurations for test cases
- Manipulate caches, KVMs

Custom Roles - Existing Resources Developer

Organization Role > Project Collaborator

AP Profiles

All API Profiles

Specific API Profiles	Operations	Environment Operations
project-codebase	<input type="button" value="View"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	prod <input type="button" value="View"/> <input type="button" value="Deploy"/> <input type="button" value="Rollback"/> <input type="button" value="Delete"/>

Deployment Status ☒ View

Environments

prod

All Caches

Specific Caches

test

All Caches

Specific Caches

Products

All Products

Specific Products	Operations
test-product	<input type="button" value="View"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Developers and Apps

Developers

All Apps

Developer Apps

Developer Apps

Reports

All Reports

Specific Reports	Operations
test-report	<input type="button" value="View"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Key Concepts:

- Restrict access to existing APIs and related resources
- Requires Org Admin to create project related resources and associate with the project specific role

Lab

Create and test custom role in UI

1. Create one of the custom roles or create your own
2. Verify access restrictions
3. As a user in a custom role, create new entities and verify visibility in custom Role

Use Management API to manage roles and users

1. View permission for custom role
2. List user roles
3. List users for role
4. Add user to custom role
5. Remove user from custom role

THANK YOU