ORACLE®

Aconex

User Roles API Developer Guide

Aconex User Role Services

Aconex User Role APIs

User Role Search (Organization)

Get User Roles and Corresponding Secured Asset details

The service returns user roles and their corresponding secured assets for an organization.

URL structure

HTTP GET - Role Secured Asset permissions assigned to a user role in an organization
`HTTP GET: https://{hostname}/api/roles?queryparams`

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
role_name	string(20)	0..1	Optional. If provided secured assets will be filtered based on the role name eg: role_name=Basic User

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Notes
Roles	Group	1	List of User Roles in an organization
*Role	Attribute	1..n	A specific user role in an organization
**DefaultRole	Attribute Boolean	1	Describes user role is default in an organization or not
**NewOrgRole	Attribute Boolean	1	Describes whether a user role is a new organization role or not
**OrganizationAdminRole	Attribute Boolean	1	Describes if current user role is an organization admin or not
**OwningOrganizationId	Attribute Long	1	User Role's owning organization id
**ProjectId	Attribute Long	1	Default value is 0, as user roles are fetched from organization

**RoleId	Attribute Integer	1	Provides id of the user role
**RoleName	Attribute String	1	Name of the user role
**SecuredAssets	Group	1..n	List of secured assets related to a user role
***SecuredAsset	Attribute	1	Action intended to be performed on an asset
****Permission	Attribute String	1	Describes the permission Grant to secured asset in context of a user role Permissions are: • `Grant` • `Deny` • `N/A`
****SecuredAssetName	Attribute String	1	Name of the secured title

Role Secured Asset Names with UI Mapping:

The tag value of `<SecuredAssetName></SecuredAssetName>` can be mapped to the UI using the below table

S.No	UI Secured Asset Name	Secured Asset Name
1	Edit organization information	EDIT_OWN_ORGANIZATION
2	Create a new user	CREATE_USER_FOR_OWN_ORGANIZATION
3	Edit own user information	EDIT_OWN_USER
4	Edit all users information	EDIT_USER_FOR_OWN_ORGANIZATION
5	Assign user roles	EDIT_ROLE_USER_SETTINGS
6	Edit project settings	EDIT_PROJECT
7	Edit project password and session settings	EDIT_PROJECT_PASSWORD_SESSION
8	Create and edit Project Fields	PROJECT_FIELD
9	Configure mail approvals for organization	APPROVAL_ORGANIZATION_EDIT
10	Configure mail approvals for projects	APPROVAL_PROJECT_EDIT
11	Can be made a mail approver	PROCESS_APPROVALS
12	Create a guest user	CREATE_EXT_USER
13	Unlock any document	CHECK_IN_ANY_DOC_FOR_OWN_ORGANIZATION
14	View Project Participants	CAN_VIEW_PROJECT_PARTICIPANTS
15	Add users	CAN_ADD_PROJECT_PARTICIPANTS
16	Create mail	CREATE_MAIL
17	View organization's project mail	SEARCH_ALL_ORGANIZATIONS_MAIL
18	Upload new documents	CREATE_NEW_CONTROLLED_DOCUMENT
19	Update a document	EDIT_CONTROLLED_DOCUMENT
20	Manually update transmittal attachments	REGISTER_TRANSMITTAL_ATTACHMENTS
21	Create print requests	CREATE_PRINT_REQUEST
22	View print requests	VIEW_PRINT_REQUESTS
23	Run auto-update transmitted documents	AUTO_UPDATE_TRANSMITTED_DOCUMENTS
24	Run a transmittal history report	VIEW_TRANSMITTAL_HISTORY
25	View files using viewer	CAN_ACCESS_VIEWER
26	Mark up files in a Document Review process	CAN_EDIT_MARKUPS

27	Mark up files in the Document Register	CAN_EDIT_MARKUPS_IN_DOC_REGISTER
28	Create/edit a workflow template	CAN_CREATE_WORKFLOW_TEMPLATE
29	Initiate a workflow	CAN_INITIATE_WORKFLOW
30	Create a transmittal	CREATE_TRANSMITTAL
31	Manage related items	MANAGE_RELATED_ITEMS
32	Edit document confidentiality	EDIT_DOCUMENT_CONFIDENTIALITY
33	View Global Directory	VIEW_GLOBAL_DIRECTORY
34	Edit directory visibility	EDIT_DIRECTORY_VISIBILITY
35	Access Bulk Processing	CAN_USE_BULK_PROCESSING
36	Share saved searches	CAN_SHARE_DOC_SAVED_SEARCHES
37	Edit/delete shared saved searches	CAN_EDIT_DOC_SHARED_SAVED_SEARCHES
38	Share saved searches	CAN_SHARE_MAIL_SAVED_SEARCHES
39	Edit/delete shared saved searches	CAN_EDIT_MAIL_SHARED_SAVED_SEARCHES
40	Configure user notification type	CAN_CONFIGURE_USER_NOTIFICATION_TYPE
41	Configure user notification attachments size limit	CAN_CONFIGURE_USER_NOTIFICATION_ATTACHMENTS_SIZE_LIMIT
42	Allow setting of mail number prior to send	ALLOW_ALLOCATE_REAL_MAIL_NUMBERS_PRIOR_TO_SEND
43	Configure user roles	EDIT_ROLE_SECURED_ASSET_SETTINGS
44	Search document register	SEARCH_REGISTERED_DOCUMENTS
45	Edit Field Permissions	EDIT_FIELD_PERMISSIONS
46	Share upload profiles	CAN_SHARE_DOCUMENT_UPLOAD_PROFILE
47	Share saved searches	CAN_SHARE_WORKFLOW_SAVED_SEARCHES
48	Edit/delete shared saved searches	CAN_EDIT_WORKFLOW_SHARED_SAVED_SEARCHES
49	Workflow Administrator	WORKFLOW_ADMINISTRATOR
50	Supplier Documents Administrator	SUPPLIER_DOC_ADMINISTRATOR
51	Make sent mail your Response	MAKE_SENT_MAIL_YOUR_RESPONSE
52	Close-out organization's mail in any thread	CLOSE_OUT_OTHER_USER_MAIL
53	Share saved searches	CAN_SHARE_SUPPLIER_DOC_SAVED_SEARCHES
54	Edit/delete shared saved searches	CAN_EDIT_SUPPLIER_DOC_SHARED_SAVED_SEARCHES
55	Access via Web Services API	CAN_USE_EXTERNAL_API
56	Restore historical document to current version	CAN_RESTORE_HISTORICAL_DOCUMENT_AS_CURRENT
57	Mark documents as No Longer in Use	CAN_MARK_DOCUMENTS_AS_NO_LONGER_IN_USE
58	Configure Access Control	CAN_CONFIGURE_ACCESS_CONTROL
59	Edit user level session time duration	EDIT_USER_SESSION_TIME_DURATION
60	Access via Outlook Plugin	OUTLOOK_PLUGIN
61	Access via 2-Step Verification	ORG_CAN_GRANT_TSV_TO_ROLES
62	Access via Single Sign-On	ORG_CAN_GRANT_SSO_TO_ROLES
63	Review a workflow	CAN_REVIEW_DOCUMENT_APPROVAL_WORKFLOW
64	Configure mail forms	CAN_CONFIGURE_CUSTOM_FIELDS
65	Access Insights	CAN_VIEW_REPORTS
66	Access Models	CAN_ACCESS_BIM
67	Create Model Stack	CAN_CREATE_MODEL_STACKS

68	Create Design Issues	CREATE_DESIGN_ISSUE
69	Create Issue Sets	CREATE_DESIGN_ISSUE_SET
70	Design Issue Administrator	DESIGN_ISSUES_ADMINISTRATION
71	Create a Package	CREATE_PACKAGE
72	Send a Package	SEND_PACKAGE_VERSION
73	Configure Mail Distribution Rules	CONFIGURE_MAIL_ROUTING_RULES
74	Access Dropbox	CAN_ACCESS_DROPBOX
75	Access Box	CAN_ACCESS_BOX
76	Access Office Online	CAN_USE_OFFICE_ONLINE
77	Edit Document Field select-list values on upload/update	CAN_EDIT_DOCUMENT_FIELD_VALUES
78	Access via Mobile Apps	CAN_ACCESS_VIA_MOBILE_APPS
79	Share saved searches	CAN_SHARE_PACKAGE_SAVED_SEARCHES
80	Edit/delete shared saved searches	CAN_EDIT_PACKAGE_SHARED_SAVED_SEARCHES
81	Create private report layouts	CREATE_REPORT_LAYOUTS
82	Create new private reports	CREATE_REPORT_ONLY_SELF
83	Create Project Org reports	CREATE_SHARE_REPORT_PROJECT_ORG
84	Create Project reports	CREATE_SHARE_REPORT_PROJECT
85	Access Reports	CAN_VIEW_BIP_REPORTS
86	Remove Users	CAN_REMOVE_PROJECT_PARTICIPANTS
87	Control Project Directory Visibility	CAN_EDIT_PROJECT_DIRECTORY_VISIBILITY
88	Create placeholders	CAN_CREATE_PLACEHOLDERS
89	Reset 2-Step Verification	CAN_RESET_VERIFICATION_ENROLMENT
90	Export Project Settings	EXPORT_PROJECT_SETTINGS

Examples/Samples

Sample Request

- Provides secured assets information for all the user roles in an organization

Sample request for Role Secured Asset permissions assigned for user roles in an organization

```
https://au1.aconex.com/api/roles
```

- Provides secured assets information for a given user role in an organization

Sample request for Role Secured Asset permissions assigned for a given role name in an organization

```
https://au1.aconex.com/api/roles?role_name=Basic User
```

Sample Response

Response for Role Secured Asset permissions in an organization

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Roles>
    <Role>
        <DefaultRole>true</DefaultRole>
        <NewOrgRole>false</NewOrgRole>
```

```
<OrganizationAdminRole>false</OrganizationAdminRole>
<OwningOrganizationId>1879048492</OwningOrganizationId>
<ProjectId>0</ProjectId>
<RoleId>1879049026</RoleId>
<RoleName>Basic User</RoleName>
<SecuredAssets>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>EDIT_OWN_USER</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>PROCESS_APPROVALS</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>CREATE_EXT_USER</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>CREATE_MAIL</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>SEARCH_ALL_ORGANIZATIONS_MAIL</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>CREATE_NEW_CONTROLLED_DOCUMENT</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>EDIT_CONTROLLED_DOCUMENT</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>REGISTER_TRANSMITTAL_ATTACHMENTS</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>CREATE_PRINT_REQUEST</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>VIEW_PRINT_REQUESTS</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>AUTO_UPDATE_TRANSMITTED_DOCUMENTS</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>VIEW_TRANSMITTAL_HISTORY</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>CAN_ACCESS_VIEWER</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>CAN_EDIT_MARKUPS</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>CAN_INITIATE_WORKFLOW</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
        <Permission>Grant</Permission>
        <SecuredAssetName>CREATE_TRANSMITTAL</SecuredAssetName>
    </SecuredAsset>
    <SecuredAsset>
```

```
                <Permission>Grant</Permission>
                <SecuredAssetName>VIEW_GLOBAL_DIRECTORY</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>CAN_CONFIGURE_USER_NOTIFICATION_TYPE</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>CAN_CONFIGURE_USER_NOTIFICATION_ATTACHMENTS_SIZE_LIMIT</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>SEARCH_REGISTERED_DOCUMENTS</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>EDIT_USER_SESSION_TIME_DURATION</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>CAN_REVIEW_DOCUMENT_APPROVAL_WORKFLOW</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>CAN_ACCESS_BIM</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>CAN_ACCESS_VIA_MOBILE_APPS</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>SEND_PACKAGE_VERSION</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>CREATE_DESIGN_ISSUE</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>CAN_CREATE_PLACEHOLDERS</SecuredAssetName>
            </SecuredAsset>
        </SecuredAssets>
    </Role>
</Roles>
```

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
UNEXPECTED_PARAMETER	Wrong parameter is given	400 Bad Request
ROLE_NAME_MUST_BE_PROVIDED	No role name is given or empty/whitespace is given	400 Bad Request
ROLE_NAME_LENGTH_EXCEEDED	Role Name length is exceeding max limit 20	400 Bad Request

Prerequisites

Required Permissions

- User should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

User Role Search (Project)

Get User Roles and corresponding Secured Asset details

The service returns user roles and their corresponding secured assets for a project.

URL structure

HTTP GET - Role Secured Asset permissions assigned to a user role in a project
`HTTP GET: https://{hostname}/api/roles/projects/{project_id}?queryparams`

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
project_id	string	1	Project id of the project admin
role_name	string(20)	0..1	Optional. If provided secured assets will be filtered based on the role name eg: role_name=Basic User

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Notes
Roles	Group	1	List of User Roles in a project
*Role	Attribute	1..n	A specific user role in a project
**DefaultRole	Attribute Boolean	1	Describes user role is default in an project or not
**NewOrgRole	Attribute Boolean	1	Describes whether a user role is a new organization role or not
**OrganizationAdminRole	Attribute Boolean	1	Describes if current user role is an organization admin or not
**OwningOrganizationId	Attribute Long	1	User Role's owning organization id
**ProjectId	Attribute Long	1	Project Id provided in path parameter
**RoleId	Attribute Integer	1	Provides id of the user role
**RoleName	Attribute String	1	Name of the user role
**SecuredAssets	Group	1..n	List of secured assets related to a user role
***SecuredAsset	Attribute	1	Action intended to be performed on an asset

****Permission	Attribute String	1	Describes the permission Grant to secured asset in context of a user role Permissions are: • `Grant` • `Deny` • `N/A`
****SecuredAssetName	Attribute String	1	Name of the secured title

---

Role Secured Asset Names with UI Mapping:

The tag value of `<SecuredAssetName></SecuredAssetName>` can be mapped to the UI using the below table

S.No	UI Secured Asset Name	Secured Asset Name
1	Edit organization information	EDIT_OWN_ORGANIZATION
2	Create a new user	CREATE_USER_FOR_OWN_ORGANIZATION
3	Edit own user information	EDIT_OWN_USER
4	Edit all users information	EDIT_USER_FOR_OWN_ORGANIZATION
5	Assign user roles	EDIT_ROLE_USER_SETTINGS
6	Edit project settings	EDIT_PROJECT
7	Edit project password and session settings	EDIT_PROJECT_PASSWORD_SESSION
8	Create and edit Project Fields	PROJECT_FIELD
9	Configure mail approvals for organization	APPROVAL_ORGANIZATION_EDIT
10	Configure mail approvals for projects	APPROVAL_PROJECT_EDIT
11	Can be made a mail approver	PROCESS_APPROVALS
12	Create a guest user	CREATE_EXT_USER
13	Unlock any document	CHECK_IN_ANY_DOC_FOR_OWN_ORGANIZATION
14	View Project Participants	CAN_VIEW_PROJECT_PARTICIPANTS
15	Add users	CAN_ADD_PROJECT_PARTICIPANTS
16	Create mail	CREATE_MAIL
17	View organization's project mail	SEARCH_ALL_ORGANIZATIONS_MAIL
18	Upload new documents	CREATE_NEW_CONTROLLED_DOCUMENT
19	Update a document	EDIT_CONTROLLED_DOCUMENT
20	Manually update transmittal attachments	REGISTER_TRANSMITTAL_ATTACHMENTS
21	Create print requests	CREATE_PRINT_REQUEST
22	View print requests	VIEW_PRINT_REQUESTS
23	Run auto-update transmitted documents	AUTO_UPDATE_TRANSMITTED_DOCUMENTS
24	Run a transmittal history report	VIEW_TRANSMITTAL_HISTORY
25	View files using viewer	CAN_ACCESS_VIEWER
26	Mark up files in a Document Review process	CAN_EDIT_MARKUPS
27	Mark up files in the Document Register	CAN_EDIT_MARKUPS_IN_DOC_REGISTER
28	Create/edit a workflow template	CAN_CREATE_WORKFLOW_TEMPLATE
29	Initiate a workflow	CAN_INITIATE_WORKFLOW

30	Create a transmittal	CREATE_TRANSMITTAL
31	Manage related items	MANAGE_RELATED_ITEMS
32	Edit document confidentiality	EDIT_DOCUMENT_CONFIDENTIALITY
33	View Global Directory	VIEW_GLOBAL_DIRECTORY
34	Edit directory visibility	EDIT_DIRECTORY_VISIBILITY
35	Access Bulk Processing	CAN_USE_BULK_PROCESSING
36	Share saved searches	CAN_SHARE_DOC_SAVED_SEARCHES
37	Edit/delete shared saved searches	CAN_EDIT_DOC_SHARED_SAVED_SEARCHES
38	Share saved searches	CAN_SHARE_MAIL_SAVED_SEARCHES
39	Edit/delete shared saved searches	CAN_EDIT_MAIL_SHARED_SAVED_SEARCHES
40	Configure user notification type	CAN_CONFIGURE_USER_NOTIFICATION_TYPE
41	Configure user notification attachments size limit	CAN_CONFIGURE_USER_NOTIFICATION_ATTACHMENTS_SIZE_LIMIT
42	Allow setting of mail number prior to send	ALLOW_ALLOCATE_REAL_MAIL_NUMBERS_PRIOR_TO_SEND
43	Configure user roles	EDIT_ROLE_SECURED_ASSET_SETTINGS
44	Search document register	SEARCH_REGISTERED_DOCUMENTS
45	Edit Field Permissions	EDIT_FIELD_PERMISSIONS
46	Share upload profiles	CAN_SHARE_DOCUMENT_UPLOAD_PROFILE
47	Share saved searches	CAN_SHARE_WORKFLOW_SAVED_SEARCHES
48	Edit/delete shared saved searches	CAN_EDIT_WORKFLOW_SHARED_SAVED_SEARCHES
49	Workflow Administrator	WORKFLOW_ADMINISTRATOR
50	Supplier Documents Administrator	SUPPLIER_DOC_ADMINISTRATOR
51	Make sent mail your Response	MAKE_SENT_MAIL_YOUR_RESPONSE
52	Close-out organization's mail in any thread	CLOSE_OUT_OTHER_USER_MAIL
53	Share saved searches	CAN_SHARE_SUPPLIER_DOC_SAVED_SEARCHES
54	Edit/delete shared saved searches	CAN_EDIT_SUPPLIER_DOC_SHARED_SAVED_SEARCHES
55	Access via Web Services API	CAN_USE_EXTERNAL_API
56	Restore historical document to current version	CAN_RESTORE_HISTORICAL_DOCUMENT_AS_CURRENT
57	Mark documents as No Longer in Use	CAN_MARK_DOCUMENTS_AS_NO_LONGER_IN_USE
58	Configure Access Control	CAN_CONFIGURE_ACCESS_CONTROL
59	Edit user level session time duration	EDIT_USER_SESSION_TIME_DURATION
60	Access via Outlook Plugin	OUTLOOK_PLUGIN
61	Access via 2-Step Verification	ORG_CAN_GRANT_TSV_TO_ROLES
62	Access via Single Sign-On	ORG_CAN_GRANT_SSO_TO_ROLES
63	Review a workflow	CAN_REVIEW_DOCUMENT_APPROVAL_WORKFLOW
64	Configure mail forms	CAN_CONFIGURE_CUSTOM_FIELDS
65	Access Insights	CAN_VIEW_REPORTS
66	Access Models	CAN_ACCESS_BIM
67	Create Model Stack	CAN_CREATE_MODEL_STACKS
68	Create Design Issues	CREATE_DESIGN_ISSUE
69	Create Issue Sets	CREATE_DESIGN_ISSUE_SET
70	Design Issue Administrator	DESIGN_ISSUES_ADMINISTRATION

71	Create a Package	CREATE_PACKAGE
72	Send a Package	SEND_PACKAGE_VERSION
73	Configure Mail Distribution Rules	CONFIGURE_MAIL_ROUTING_RULES
74	Access Dropbox	CAN_ACCESS_DROPBOX
75	Access Box	CAN_ACCESS_BOX
76	Access Office Online	CAN_USE_OFFICE_ONLINE
77	Edit Document Field select-list values on upload/update	CAN_EDIT_DOCUMENT_FIELD_VALUES
78	Access via Mobile Apps	CAN_ACCESS_VIA_MOBILE_APPS
79	Share saved searches	CAN_SHARE_PACKAGE_SAVED_SEARCHES
80	Edit/delete shared saved searches	CAN_EDIT_PACKAGE_SHARED_SAVED_SEARCHES
81	Create private report layouts	CREATE_REPORT_LAYOUTS
82	Create new private reports	CREATE_REPORT_ONLY_SELF
83	Create Project Org reports	CREATE_SHARE_REPORT_PROJECT_ORG
84	Create Project reports	CREATE_SHARE_REPORT_PROJECT
85	Access Reports	CAN_VIEW_BIP_REPORTS
86	Remove Users	CAN_REMOVE_PROJECT_PARTICIPANTS
87	Control Project Directory Visibility	CAN_EDIT_PROJECT_DIRECTORY_VISIBILITY
88	Create placeholders	CAN_CREATE_PLACEHOLDERS
89	Reset 2-Step Verification	CAN_RESET_VERIFICATION_ENROLMENT
90	Export Project Settings	EXPORT_PROJECT_SETTINGS

Examples/Samples

Sample Request

- Provides secured assets information for all the user roles in a project

Sample request for Role Secured Asset permissions assigned for a role in a project
`https://au1.aconex.com/api/roles/projects/1879048400`

- Provides secured assets information for a given user role in a project

Sample request for Role Secured Asset permissions assigned for a given role name in a project
`https://au1.aconex.com/api/roles/projects/1879048400?role_name=Basic User`

Sample Response

Response for Role Secured Asset permissions in a project

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Roles>
    <Role>
        <DefaultRole>false</DefaultRole>
        <NewOrgRole>true</NewOrgRole>
        <OrganizationAdminRole>false</OrganizationAdminRole>
        <OwningOrganizationId>1879048492</OwningOrganizationId>
        <ProjectId>1879048400</ProjectId>
        <RoleId>1879049114</RoleId>
        <RoleName>Contract Admin</RoleName>
        <SecuredAssets>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <securedAsset>VIEW_GLOBAL_DIRECTORY</securedAsset>
                <SecuredAssetName>VIEW_GLOBAL_DIRECTORY</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <securedAsset>CAN_CONFIGURE_USER_NOTIFICATION_TYPE</securedAsset>
                <SecuredAssetName>CAN_CONFIGURE_USER_NOTIFICATION_TYPE</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <securedAsset>CAN_CONFIGURE_USER_NOTIFICATION_ATTACHMENTS_SIZE_LIMIT</securedAsset>
                <SecuredAssetName>CAN_CONFIGURE_USER_NOTIFICATION_ATTACHMENTS_SIZE_LIMIT</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <securedAsset>SEARCH_REGISTERED_DOCUMENTS</securedAsset>
                <SecuredAssetName>SEARCH_REGISTERED_DOCUMENTS</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <securedAsset>EDIT_USER_SESSION_TIME_DURATION</securedAsset>
                <SecuredAssetName>EDIT_USER_SESSION_TIME_DURATION</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <securedAsset>CAN_ACCESS_VIA_MOBILE_APPS</securedAsset>
                <SecuredAssetName>CAN_ACCESS_VIA_MOBILE_APPS</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <securedAsset>SEND_PACKAGE_VERSION</securedAsset>
                <SecuredAssetName>SEND_PACKAGE_VERSION</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <securedAsset>CAN_CREATE_PLACEHOLDERS</securedAsset>
                <SecuredAssetName>CAN_CREATE_PLACEHOLDERS</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>N/A</Permission>
                <securedAsset>EDIT_ROLE_USER_SETTINGS</securedAsset>
                <SecuredAssetName>EDIT_ROLE_USER_SETTINGS</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>N/A</Permission>
                <securedAsset>EDIT_ROLE_SECURED_ASSET_SETTINGS</securedAsset>
                <SecuredAssetName>EDIT_ROLE_SECURED_ASSET_SETTINGS</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>N/A</Permission>
                <securedAsset>CAN_USE_EXTERNAL_API</securedAsset>
                <SecuredAssetName>CAN_USE_EXTERNAL_API</SecuredAssetName>
            </SecuredAsset>
            <SecuredAsset>
                <Permission>N/A</Permission>
                <securedAsset>SEARCH_ALL_ORGANIZATIONS_MAIL</securedAsset>
                <SecuredAssetName>SEARCH_ALL_ORGANIZATIONS_MAIL</SecuredAssetName>
            </SecuredAsset>
```

```
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CREATE_MAIL</securedAsset>
    <SecuredAssetName>CREATE_MAIL</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>MAKE_SENT_MAIL_YOUR_RESPONSE</securedAsset>
    <SecuredAssetName>MAKE_SENT_MAIL_YOUR_RESPONSE</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CLOSE_OUT_OTHER_USER_MAIL</securedAsset>
    <SecuredAssetName>CLOSE_OUT_OTHER_USER_MAIL</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>VIEW_ORG_CONFIDENTIAL_PROJECT_MAIL</securedAsset>
    <SecuredAssetName>VIEW_ORG_CONFIDENTIAL_PROJECT_MAIL</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>PROCESS_APPROVALS</securedAsset>
    <SecuredAssetName>PROCESS_APPROVALS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CREATE_TRANSMITTAL</securedAsset>
    <SecuredAssetName>CREATE_TRANSMITTAL</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>AUTO_UPDATE_TRANSMITTED_DOCUMENTS</securedAsset>
    <SecuredAssetName>AUTO_UPDATE_TRANSMITTED_DOCUMENTS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CREATE_NEW_CONTROLLED_DOCUMENT</securedAsset>
    <SecuredAssetName>CREATE_NEW_CONTROLLED_DOCUMENT</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>EDIT_CONTROLLED_DOCUMENT</securedAsset>
    <SecuredAssetName>EDIT_CONTROLLED_DOCUMENT</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_USE_BULK_PROCESSING</securedAsset>
    <SecuredAssetName>CAN_USE_BULK_PROCESSING</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_RESTORE_HISTORICAL_DOCUMENT_AS_CURRENT</securedAsset>
    <SecuredAssetName>CAN_RESTORE_HISTORICAL_DOCUMENT_AS_CURRENT</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_MARK_DOCUMENTS_AS_NO_LONGER_IN_USE</securedAsset>
    <SecuredAssetName>CAN_MARK_DOCUMENTS_AS_NO_LONGER_IN_USE</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>VIEW_ORG_CONFIDENTIAL_DOCUMENTS</securedAsset>
    <SecuredAssetName>VIEW_ORG_CONFIDENTIAL_DOCUMENTS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>MANAGE_RELATED_ITEMS</securedAsset>
    <SecuredAssetName>MANAGE_RELATED_ITEMS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
```

```
    <Permission>N/A</Permission>
    <securedAsset>CAN_ACCESS_BOX</securedAsset>
    <SecuredAssetName>CAN_ACCESS_BOX</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_ACCESS_DROPBOX</securedAsset>
    <SecuredAssetName>CAN_ACCESS_DROPBOX</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_USE_OFFICE_ONLINE</securedAsset>
    <SecuredAssetName>CAN_USE_OFFICE_ONLINE</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_EDIT_MARKUPS</securedAsset>
    <SecuredAssetName>CAN_EDIT_MARKUPS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_EDIT_MARKUPS_IN_DOC_REGISTER</securedAsset>
    <SecuredAssetName>CAN_EDIT_MARKUPS_IN_DOC_REGISTER</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_REVIEW_DOCUMENT_APPROVAL_WORKFLOW</securedAsset>
    <SecuredAssetName>CAN_REVIEW_DOCUMENT_APPROVAL_WORKFLOW</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_INITIATE_WORKFLOW</securedAsset>
    <SecuredAssetName>CAN_INITIATE_WORKFLOW</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_CREATE_WORKFLOW_TEMPLATE</securedAsset>
    <SecuredAssetName>CAN_CREATE_WORKFLOW_TEMPLATE</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>WORKFLOW_ADMINISTRATOR</securedAsset>
    <SecuredAssetName>WORKFLOW_ADMINISTRATOR</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>EXPORT_PROJECT_SETTINGS</securedAsset>
    <SecuredAssetName>EXPORT_PROJECT_SETTINGS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>PROJECT_FIELD</securedAsset>
    <SecuredAssetName>PROJECT_FIELD</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>READ_PROJECT_FIELD</securedAsset>
    <SecuredAssetName>READ_PROJECT_FIELD</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_INLINE_EDIT_PROJECT_FIELD_VALUES</securedAsset>
    <SecuredAssetName>CAN_INLINE_EDIT_PROJECT_FIELD_VALUES</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>EDIT_PROJECT</securedAsset>
    <SecuredAssetName>EDIT_PROJECT</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
```

```
    <securedAsset>CAN_CONFIGURE_CUSTOM_FIELDS</securedAsset>
    <SecuredAssetName>CAN_CONFIGURE_CUSTOM_FIELDS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>EDIT_FIELD_PERMISSIONS</securedAsset>
    <SecuredAssetName>EDIT_FIELD_PERMISSIONS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_EDIT_DOCUMENT_FIELD_VALUES</securedAsset>
    <SecuredAssetName>CAN_EDIT_DOCUMENT_FIELD_VALUES</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CONFIGURE_MAIL_ROUTING_RULES</securedAsset>
    <SecuredAssetName>CONFIGURE_MAIL_ROUTING_RULES</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CASCADING_METADATA</securedAsset>
    <SecuredAssetName>CASCADING_METADATA</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_VIEW_PROJECT_PARTICIPANTS</securedAsset>
    <SecuredAssetName>CAN_VIEW_PROJECT_PARTICIPANTS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_EDIT_PROJECT_DIRECTORY_VISIBILITY</securedAsset>
    <SecuredAssetName>CAN_EDIT_PROJECT_DIRECTORY_VISIBILITY</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_ADD_PROJECT_PARTICIPANTS</securedAsset>
    <SecuredAssetName>CAN_ADD_PROJECT_PARTICIPANTS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_REMOVE_PROJECT_PARTICIPANTS</securedAsset>
    <SecuredAssetName>CAN_REMOVE_PROJECT_PARTICIPANTS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_CONFIGURE_ACCESS_CONTROL</securedAsset>
    <SecuredAssetName>CAN_CONFIGURE_ACCESS_CONTROL</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_ACCESS_BIM</securedAsset>
    <SecuredAssetName>CAN_ACCESS_BIM</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_CREATE_MODEL_STACKS</securedAsset>
    <SecuredAssetName>CAN_CREATE_MODEL_STACKS</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CREATE_PACKAGE</securedAsset>
    <SecuredAssetName>CREATE_PACKAGE</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_SHARE_PACKAGE_SAVED_SEARCHES</securedAsset>
    <SecuredAssetName>CAN_SHARE_PACKAGE_SAVED_SEARCHES</SecuredAssetName>
</SecuredAsset>
<SecuredAsset>
    <Permission>N/A</Permission>
    <securedAsset>CAN_EDIT_PACKAGE_SHARED_SAVED_SEARCHES</securedAsset>
```

```
            <SecuredAssetName>CAN_EDIT_PACKAGE_SHARED_SAVED_SEARCHES</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>SUPPLIER_DOC_ADMINISTRATOR</securedAsset>
            <SecuredAssetName>SUPPLIER_DOC_ADMINISTRATOR</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>CAN_VIEW_ORG_TENDERS</securedAsset>
            <SecuredAssetName>CAN_VIEW_ORG_TENDERS</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>CAN_CREATE_TENDER_RESPONSE</securedAsset>
            <SecuredAssetName>CAN_CREATE_TENDER_RESPONSE</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>CAN_CREATE_TENDER_INVITATION</securedAsset>
            <SecuredAssetName>CAN_CREATE_TENDER_INVITATION</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>CAN_CREATE_TENDER_ADDENDUM</securedAsset>
            <SecuredAssetName>CAN_CREATE_TENDER_ADDENDUM</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>CAN_USE_ASSET_REGISTER</securedAsset>
            <SecuredAssetName>CAN_USE_ASSET_REGISTER</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>CAN_ADMIN_ASSET_REGISTER</securedAsset>
            <SecuredAssetName>CAN_ADMIN_ASSET_REGISTER</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>CAN_CREATE_ASSETS</securedAsset>
            <SecuredAssetName>CAN_CREATE_ASSETS</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>SUBMIT_HANDOVER_CONTENT</securedAsset>
            <SecuredAssetName>SUBMIT_HANDOVER_CONTENT</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>REVIEW_HANDOVER_CONTENT</securedAsset>
            <SecuredAssetName>REVIEW_HANDOVER_CONTENT</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>CREATE_AND_EDIT_HANDOVER_MANUALS</securedAsset>
            <SecuredAssetName>CREATE_AND_EDIT_HANDOVER_MANUALS</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>SHARE_DOCUMENT</securedAsset>
            <SecuredAssetName>SHARE_DOCUMENT</SecuredAssetName>
        </SecuredAsset>
        <SecuredAsset>
            <Permission>N/A</Permission>
            <securedAsset>SHARE_DOCUMENT_TO_ALL</securedAsset>
            <SecuredAssetName>SHARE_DOCUMENT_TO_ALL</SecuredAssetName>
        </SecuredAsset>
    </SecuredAssets>
  </Role>
</Roles>
```

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
UNEXPECTED_PARAMETER	Wrong parameter is given	400 Bad Request
ROLE_NAME_MUST_BE_PROVIDED	No role name is given or empty/whitespace is given	400 Bad Request
ROLE_NAME_LENGTH_EXCEEDED	Role Name length is exceeding max limit 20	400 Bad Request

Prerequisites

Required Permissions

- User should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

User Search (User Role – Organization)

Get Users assigned to a User Role

The service returns users assigned to a user role in an organization

URL structure

HTTP GET - Users Assigned to a User Role - Organization Admin
`HTTP GET: https://{hostname}/api/roles/users?queryparams`

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
role_name	string(20)	1	Provides list of users assigned to a user role eg: role_name=Basic User
page_number	string	1	Optional. A default value is set to **1**
page_size	string	1	Optional. A default value is set to **1000**

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type	Cardinality	Notes
Role-Users	Group	1	List of users assigned to a user role

*Role	Attribute	1	User role that has been given in the query parameter
**DefaultRole	Attribute Boolean	1	Describes whether user role is default in an organization or not
**NewOrgRole	Attribute Boolean	1	*Describes whether a user role is a new organization role or not
**OrganizationAdminRole	Attribute Boolean	1	Describes whether current user role is an organization admin or not
**OwningOrganizationId	Attribute Long	1	User Role's owning organization id
**ProjectId	Attribute Long	1	Default value is 0, as user roles are fetched from organization
**Id	Attribute Integer	1	Provides id of the user role
**Name	Attribute String	1	Name of the user role
**Users	Group	0..n	Grouping of users for the given user role
***User	Attribute	1	User assigned with the given user role
****Email	Attribute String	1	Email of the user
****Mobile	Attribute String	0..1	Mobile number of the user
****FirstName	Attribute String	1	First name of the user
****UserId	Attribute Long	1	Id of the user
****LastName	Attribute String	1	Last name of the user
****MiddleName	Attribute String	0..1	Middle name of the user
****UserTitle	Attribute String	1	User title of the user
****UserName	Attribute String	1	Username of the user

Examples/Samples

Sample Requests

- Provides users for all available user roles in an organization

```
https://au1.aconex.com/api/roles/users
```

- Provides users for a given user role in an organization

```
https://au1.aconex.com/api/roles/users?role_name=Basic User
```

Sample Response

Users Assigned to Role Response - Organization Admin

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<RoleUsers TotalResultsOnPage="2" TotalResults="58" TotalPages="29" PageSize="2" CurrentPage="1">
    <SearchResults>
        <Role>
            <DefaultRole>true</DefaultRole>
            <NewOrgRole>true</NewOrgRole>
            <OrganizationAdminRole>false</OrganizationAdminRole>
            <OwningOrganizationId>1</OwningOrganizationId>
            <ProjectId>0</ProjectId>
            <Id>17</Id>
            <Name>2 - Basic +</Name>
            <Users>
                <User>
                    <Email>cegbu_automations@mailac.custhelp.com</Email>
                    <Mobile>999999999</Mobile>
                    <FirstName>Aconex</FirstName>
                    <UserId>1</UserId>
                    <LastName>Administrator</LastName>
                    <MiddleName></MiddleName>
                    <UserTitle>Mr</UserTitle>
                    <UserName>acnxAdmin</UserName>
                </User>
                <User>
                    <Email>abhishek.gupta@abc.com</Email>
                    <Mobile>9999999</Mobile>
                    <FirstName>Abhishek</FirstName>
                    <UserId>1879053194</UserId>
                    <LastName>Gupta</LastName>
                    <MiddleName></MiddleName>
                    <UserTitle>Mr</UserTitle>
                    <UserName>a.gupta</UserName>
                </User>
            </Users>
        </Role>
    </SearchResults>
</RoleUsers>
```

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
UNEXPECTED_PARAMETER	Wrong parameter is given	400 Bad Request
ROLE_NAME_MUST_BE_PROVIDED	No role name is given or empty/whitespace is given	400 Bad Request
ROLE_NAME_LENGTH_EXCEEDED	Role Name length is exceeding max limit 20	400 Bad Request

Prerequisites

Required Permissions

- User should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

User Search (User Role – Project)

Get Users assigned to a User Role in a project

The service returns users assigned to a user role in a project

URL structure

HTTP GET - Users Assigned to a Role Name - Organization Admin
`HTTP GET: https://{hostname}/api/roles/users/projects/{project_id}?queryparams`

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
project_id	string	1	Project id of the project admin
role_name	string(20)	1	Provides list of users assigned to a user role eg: role_name=Basic User
page_number	string	1	Optional. A default value is set to **1**
page_size	string	1	Optional. A default value is set to **1000**

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type	Cardinality	Notes
RoleUsers	Group	1	List of users assigned to a user role
*Role	Attribute	1	User role that has been given in the query parameter
**DefaultRole	Attribute Boolean	1	Describes whether user role is default in a project or not
**NewOrgRole	Attribute Boolean	1	*Describes whether a user role is a new role or not
**OrganizationAdminRole	Attribute Boolean	1	Describes whether current user role is a project admin or not
**OwningOrganizationId	Attribute Long	1	User Role's owning organization id
**ProjectId	Attribute Long	1	Project Id provided as in path parameter
**Id	Attribute Integer	1	Provides id of the user role
**Name	Attribute String	1	Name of the user role
**Users	Group	0..n	Grouping of users for the given user role
***User	Attribute	1	User assigned with the given user role
****Email	Attribute String	1	Email of the user
****Mobile	Attribute String	0..1	Mobile number of the user
****FirstName	Attribute String	1	First name of the user
****UserId	Attribute Long	1	Id of the user
****LastName	Attribute String	1	Last name of the user
****MiddleName	Attribute String	0..1	Middle name of the user

****UserTitle	Attribute String	1	User title of the user
****UserName	Attribute String	1	Username of the user

Examples/Samples

Sample Requests

Provides users for a given user role in a project

Sample Request for users assigned to a given role name in a project

```
https://au1.aconex.com/api/roles/users/projects/1879048400?page_number=1&page_size=1000&role_name=Basic User
```

Sample Response

Users assigned to a Role response - Project Admin

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<RoleUsers TotalResultsOnPage="5" TotalResults="5" TotalPages="1" PageSize="1000" CurrentPage="1">
    <SearchResults>
        <Role>
            <DefaultRole>false</DefaultRole>
            <NewOrgRole>true</NewOrgRole>
            <OrganizationAdminRole>false</OrganizationAdminRole>
            <OwningOrganizationId>1879048492</OwningOrganizationId>
            <ProjectId>1879048400</ProjectId>
            <Id>1879049114</Id>
            <Name>Contract Admin</Name>
            <Users>
                <User>
                    <Email>blackhole@aconex.com</Email>
                    <Mobile></Mobile>
                    <FirstName>Document</FirstName>
                    <UserId>1879049121</UserId>
                    <LastName>Controller</LastName>
                    <MiddleName></MiddleName>
                    <UserTitle></UserTitle>
                    <UserName>dcontroller</UserName>
                </User>
                <User>
                    <Email>blackhole@aconex.com</Email>
                    <Mobile>0412 333 222</Mobile>
                    <FirstName>Patrick</FirstName>
                    <UserId>1879049107</UserId>
                    <LastName>O'Leary</LastName>
                    <MiddleName></MiddleName>
                    <UserTitle>Mr</UserTitle>
                    <UserName>poleary</UserName>
                </User>
                <User>
                    <Email>blackhole@aconex.com</Email>
                    <Mobile></Mobile>
                    <FirstName>Tim</FirstName>
                    <UserId>1879049123</UserId>
                    <LastName>Yeung</LastName>
                    <MiddleName></MiddleName>
                    <UserTitle>Mr</UserTitle>
                    <UserName>tyeung</UserName>
                </User>
            </Users>
        </Role>
        <Role>
            <DefaultRole>false</DefaultRole>
```

```
            <NewOrgRole>false</NewOrgRole>
            <OrganizationAdminRole>false</OrganizationAdminRole>
            <OwningOrganizationId>1879048492</OwningOrganizationId>
            <ProjectId>1879048400</ProjectId>
            <Id>1879049294</Id>
            <Name>External API</Name>
            <Users>
                <User>
                    <Email>blackhole@aconex.com</Email>
                    <Mobile>0412 333 222</Mobile>
                    <FirstName>Patrick</FirstName>
                    <UserId>1879049107</UserId>
                    <LastName>O'Leary</LastName>
                    <MiddleName></MiddleName>
                    <UserTitle>Mr</UserTitle>
                    <UserName>poleary</UserName>
                </User>
                <User>
                    <Email>blackhole@aconex.com</Email>
                    <Mobile></Mobile>
                    <FirstName>Tim</FirstName>
                    <UserId>1879049123</UserId>
                    <LastName>Yeung</LastName>
                    <MiddleName></MiddleName>
                    <UserTitle>Mr</UserTitle>
                    <UserName>tyeung</UserName>
                </User>
            </Users>
        </Role>
    </SearchResults>
</RoleUsers>
```

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
UNEXPECTED_PARAMETER	Wrong parameter is given	400 Bad Request
ROLE_NAME_MUST_BE_PROVIDED	No role name is given or empty/whitespace is given	400 Bad Request
ROLE_NAME_LENGTH_EXCEEDED	Role Name length is exceeding max limit 20	400 Bad Request

---

Prerequisites

Required Permissions

- User should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

User Entitlements (Organization)

Get User Entitlements assigned to a User in an organization

The service returns user entitlements assigned to a user in an organization

URL structure

HTTP GET - User Entitlements Assigned to a user

```
HTTP GET: https://{hostname}/api/roles/user?queryparams
```

Parameters

Parameters	Type	Cardinality	Notes
user_id	string	1	Provides list of user entitlements assigned to a user provided user id eg: user_id=123456

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type	Cardinality	Notes
UserRoles	Group	1	List of user entitlements/roles assigned to a user
*User	Attribute	1	User that has been given in the query parameter
**Email	Attribute String	1	Email of the user
**Mobile	Attribute String	1	Mobile number of the user
**FirstName	Attribute String	1	First name of the user
**MiddleName	Attribute String	1	Middle name of the user
**LastName	Attribute String	1	Last name of the user
**UserTitle	Attribute String	1	Title of the user (Mr/Ms/Mrs)
**UserId	Attribute Long	1	User Id of the user
**UserName	Attribute String	1	Username of the user
**Roles	Group	0..n	List of assigned entitlements/roles to a user
***Role	Attribute	1	Entitlement/Role assigned to a user
****DefaultRole	Attribute Boolean	1	Describes whether user role is default in an organization or not
****NewOrgRole	Attribute Boolean	1	Describes whether a user role is a new organization role or not
****OrganizationAdminRole	Attribute Boolean	1	Describes whether current user role is an organization admin or not
****OwningOrganizationId	Attribute Long	1	User Role's owning organization id
****ProjectId	Attribute Long	1	Default value is 0, as user roles are fetched from organization
****RoleId	Attribute Integer	1	Provides id of the user role

****RoleName	Attribute String	1	Name of the user role

Examples/Samples

Sample Requests

Provides user entitlements for a given user id in an organization

Sample request for User Entitlement in an organization
`https://au1.aconex.com/api/roles/user?user_id=1234567890`

Sample Response

Response for User Entitlements API

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<UserRoles>
    <User>
        <Email>blackhole@aconex.com</Email>
        <Mobile>0412 333 222</Mobile>
        <FirstName>Patrick</FirstName>
        <UserId>1879049107</UserId>
        <LastName>O'Leary</LastName>
        <MiddleName></MiddleName>
        <Roles>
            <Role>
                <DefaultRole>false</DefaultRole>
                <NewOrgRole>false</NewOrgRole>
                <OrganizationAdminRole>false</OrganizationAdminRole>
                <OwningOrganizationId>1879048492</OwningOrganizationId>
                <ProjectId>1879048400</ProjectId>
                <RoleId>1879049294</RoleId>
                <RoleName>External API</RoleName>
            </Role>
            <Role>
                <DefaultRole>false</DefaultRole>
                <NewOrgRole>false</NewOrgRole>
                <OrganizationAdminRole>false</OrganizationAdminRole>
                <OwningOrganizationId>1879048492</OwningOrganizationId>
                <ProjectId>0</ProjectId>
                <RoleId>1879049231</RoleId>
                <RoleName>Bulk Processing</RoleName>
            </Role>
            <Role>
                <DefaultRole>false</DefaultRole>
                <NewOrgRole>true</NewOrgRole>
                <OrganizationAdminRole>false</OrganizationAdminRole>
                <OwningOrganizationId>1879048492</OwningOrganizationId>
                <ProjectId>1879048400</ProjectId>
                <RoleId>1879049114</RoleId>
                <RoleName>Contract Admin</RoleName>
            </Role>
            <Role>
                <DefaultRole>false</DefaultRole>
                <NewOrgRole>false</NewOrgRole>
                <OrganizationAdminRole>true</OrganizationAdminRole>
                <OwningOrganizationId>1879048492</OwningOrganizationId>
                <ProjectId>0</ProjectId>
                <RoleId>1879049027</RoleId>
                <RoleName>Org Admin</RoleName>
            </Role>
        </Roles>
        <UserTitle>Mr</UserTitle>
        <UserName>poleary</UserName>
    </User>
</UserRoles>
```

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
UNEXPECTED_PARAMETER	Wrong parameter is given	400 Bad Request
INVALID_PARAMETER_VALUE	The request parameter userId contains an incorrect or unknown value	400 Bad Request

USER_ID_MUST_BE_PROVIDED	User id must Be Provided	400 Bad Request

---

Prerequisites

Required Permissions

- User should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

User Entitlements (Project)

Get User Entitlements assigned to a User in a project

The service returns user entitlements assigned to a user in a project

URL structure

HTTP GET - User Entitlements Assigned to a user for a project admin

```
HTTP GET: https://{hostname}/api/roles/user/projects/{project_id}?queryparams
```

Parameters

Parameters	Type	Cardinality	Notes
project_id	string	1	Project id of the project admin
user_id	string	1	Provides list of user entitlements assigned to a user provided user id eg: user_id=123456

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type	Cardinality	Notes
UserRoles	Group	1	List of user entitlements/roles assigned to a user
*User	Attribute	1	User that has been given in the query parameter
**Email	Attribute String	1	Email of the user
**Mobile	Attribute String	1	Mobile number of the user
**FirstName	Attribute String	1	First name of the user
**MiddleName	Attribute String	1	Middle name of the user
**LastName	Attribute String	1	Last name of the user
**UserTitle	Attribute String	1	Title of the user (Mr/Ms/Mrs)

**UserId	Attribute Long	1	User Id of the user
**UserName	Attribute String	1	Username of the user
**Roles	Group	0..n	List of assigned entitlements/roles to a user
***Role	Attribute	1	Entitlement/Role assigned to a user
****DefaultRole	Attribute Boolean	1	Describes whether user role is default in a project or not
****NewOrgRole	Attribute Boolean	1	Describes whether a user role is a new organization role or not
****OrganizationAdminRole	Attribute Boolean	1	Describes whether current user role is a project admin or not
****OwningOrganizationId	Attribute Long	1	User Role's owning organization id
****ProjectId	Attribute Long	1	ProjectId as provided in the path parameters
****RoleId	Attribute Integer	1	Provides id of the user role
****RoleName	Attribute String	1	Name of the user role

Examples/Samples

Sample Requests

Provides user entitlements for a given user id in a project

Sample request for User Entitlement in a project
`https://au1.aconex.com/api/roles/user/projects/123456789?user_id=1234567890`

Sample Response

Response for User Entitlements API


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<UserRoles>
    <User>
        <Email>blackhole@aconex.com</Email>
        <Mobile></Mobile>
        <FirstName>Kim</FirstName>
        <UserId>1234567890</UserId>
        <LastName>Nga</LastName>
        <MiddleName></MiddleName>
        <Roles>
            <Role>
                <DefaultRole>true</DefaultRole>
                <NewOrgRole>true</NewOrgRole>
                <OrganizationAdminRole>false</OrganizationAdminRole>
                <OwningOrganizationId>1</OwningOrganizationId>
                <ProjectId>0</ProjectId>
                <RoleId>1879048195</RoleId>
                <RoleName>1 - Basic</RoleName>
            </Role>
            <Role>
                <DefaultRole>true</DefaultRole>
                <NewOrgRole>true</NewOrgRole>
                <OrganizationAdminRole>false</OrganizationAdminRole>
                <OwningOrganizationId>1</OwningOrganizationId>
                <ProjectId>0</ProjectId>
                <RoleId>1879048195</RoleId>
                <RoleName>1 - Basic</RoleName>
            </Role>
            <Role>
                <DefaultRole>true</DefaultRole>
                <NewOrgRole>true</NewOrgRole>
                <OrganizationAdminRole>false</OrganizationAdminRole>
                <OwningOrganizationId>1</OwningOrganizationId>
                <ProjectId>0</ProjectId>
                <RoleId>1879048195</RoleId>
                <RoleName>1 - Basic</RoleName>
            </Role>
            <Role>
                <DefaultRole>true</DefaultRole>
                <NewOrgRole>true</NewOrgRole>
                <OrganizationAdminRole>false</OrganizationAdminRole>
                <OwningOrganizationId>1</OwningOrganizationId>
                <ProjectId>0</ProjectId>
                <RoleId>1879048195</RoleId>
                <RoleName>1 - Basic</RoleName>
            </Role>
            <Role>
                <DefaultRole>true</DefaultRole>
                <NewOrgRole>true</NewOrgRole>
                <OrganizationAdminRole>false</OrganizationAdminRole>
                <OwningOrganizationId>1</OwningOrganizationId>
                <ProjectId>0</ProjectId>
                <RoleId>1879048195</RoleId>
                <RoleName>1 - Basic</RoleName>
            </Role>
        </Roles>
        <UserTitle>Ms</UserTitle>
        <UserName>knga</UserName>
    </User>
</UserRoles>
```


Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
UNEXPECTED_PARAMETER	Wrong parameter is given	400 Bad Request
INVALID_PARAMETER_VALUE	The request parameter userId contains an incorrect or unknown value	400 Bad Request
USER_ID_MUST_BE_PROVIDED	User id must Be Provided	400 Bad Request

---

Prerequisites

Required Permissions

- User should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Create User Role (Organization)

Create a user role in an organization

The service creates a user role in an organization with all role secured assets permissions as **N/A**

URL structure

HTTP POST - Create a user role in an organization
`HTTP POST: https://{hostname}/api/roles?queryparams`

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
role_name	string(20)	1	A role name should be provided eg: role_name=Basic User
assign_role	boolean	0..1	Optional. Default value is **false**

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **201**

Examples/Samples

Sample Request

- Create a user role in an organization

Sample request for creating a user role in organization

```
https://au1.aconex.com/api/roles?role_name=Basic User
```

- Create a user role in an organization with the given role name as default role

Sample request for creating a user role as default role in an organization

```
https://au1.aconex.com/api/roles?role_name=Basic User&assign_role=true
```

Sample Response

Response for creating a user role in an organization - Empty response

---

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
UNEXPECTED_PARAMETER	Wrong parameter is given	400 Bad Request
ROLE_NAME_MUST_BE_PROVIDED	No role name is given or empty/whitespace is given	400 Bad Request
ROLE_NAME_LENGTH_EXCEEDED	Role Name length is exceeding max limit 20	400 Bad Request

---

Prerequisites

Required Permissions

- User should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Create User Role (Project)

Create a user role in a project

The service creates a user role in a project with all role secured assets permissions as **N/A**

URL structure

HTTP POST - Create a user role in a project

```
HTTP POST: https://{hostname}/api/roles/projects/{project_id}?queryparams
```

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
project_id	string	1	Project id of the project admin
role_name	string(20)	1	A role name should be provided eg: role_name=Basic User
assign_role	boolean	0..1	Optional. Default value is **false**

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **201**

Examples/Samples

Sample Request

- Create a user role in a project

Sample request for creating a user role in project
`https://au1.aconex.com/api/roles/projects/1234567?role_name=Basic User`

- Create a user role in a project with the given role name as default role

Sample request for creating a user role as default role in project
`https://au1.aconex.com/api/roles/projects/1234567?role_name=Basic User&assign_role=true`

Sample Response

Response for creating a user role in a project - Empty response

---

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
UNEXPECTED_PARAMETER	Wrong parameter is given	400 Bad Request
ROLE_NAME_MUST_BE_PROVIDED	No role name is given or empty/whitespace is given	400 Bad Request
ROLE_NAME_LENGTH_EXCEEDED	Role Name length is exceeding max limit 20	400 Bad Request

---

Prerequisites

Required Permissions

- Should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Update User Role (Organization)

Update User Role Name and properties in an organization

The service updates user role name and properties

URL structure

HTTP PATCH - Update User Role name and properties in an organization

```
HTTP PATCH: https://{hostname}/api/roles
```

Parameters

Parameters	Type(maxlength)	Cardinality	Notes

Input Payload Template

Input Payload template to Update user role name and properties

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Role>
    <RoleId></RoleId>
    <RoleName></RoleName>
    <DefaultRole></DefaultRole>
</Role>
```

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Notes
Role	Attribute	1	A specific user role in an organization
*RoleId	Attribute Integer	1	Provides id of the user role
*RoleName	Attribute String	1	Name of the user role
*DefaultRole	Attribute Boolean	1	Specifies if the role should be set to default or not

Expected Response

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **200**

Examples/Samples

Sample Request

Sample request for updating User Role name and properties in an organization

```
HTTP PATCH https://au1.aconex.com/api/roles
Content-Type: application/xml;boundary="a1a1"

--a1a1

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Role>
    <RoleId>1879049312</RoleId>
    <RoleName>created_role</RoleName>
        <DefaultRole>false</DefaultRole>
</Role>
```

Sample Response

Response for updating User Role name and properties in an organization - Empty response

---

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
ROLE_NAME_MUST_BE_PROVIDED	No role name is given or empty/whitespace is given	400 Bad Request
ROLE_NAME_LENGTH_EXCEEDED	Role Name length is exceeding max limit 20	400 Bad Request
ROLE_ID_MUST_BE_PROVIDED	Role Id must be provided in the input XML payload	400 Bad Request

---

Prerequisites

Required Permissions

- Should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Update User Role (Project)

Update User Role Name and properties in a project

The service updates user role name and properties

URL structure

HTTP PATCH - Update User Role name and properties in a project

```
HTTP PATCH: https://{hostname}/api/roles/projects/{project_id}
```

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
project_id	string	1	Project id of the project admin

Input Payload Template

Input Payload template to Update user role name and properties

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Role>
    <RoleId></RoleId>
    <RoleName></RoleName>
    <DefaultRole></DefaultRole>
</Role>
```

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Notes
Role	Attribute	1	A specific user role in a project
*RoleId	Attribute Integer	1	Provides id of the user role
*RoleName	Attribute String	1	Name of the user role
*DefaultRole	Attribute Boolean	1	Specifies if the role should be set to default or not

Expected Response

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **200**

Examples/Samples

Sample Request

Sample request for updating User Role name and properties in a project

```
HTTP PATCH https://au1.aconex.com/api/roles/projects/1234567890
Content-Type: application/xml;boundary="a1a1"

--a1a1

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Role>
    <RoleId>1879049312</RoleId>
    <RoleName>created_role</RoleName>
    <DefaultRole>false</DefaultRole>
</Role>
```

Sample Response

Response for updating User Role name and properties in a project - Empty response

---

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
ROLE_NAME_MUST_BE_PROVIDED	No role name is given or empty/whitespace is given	400 Bad Request
ROLE_NAME_LENGTH_EXCEEDED	Role Name length is exceeding max limit 20	400 Bad Request
ROLE_ID_MUST_BE_PROVIDED	Role Id must be provided in the input XML payload	400 Bad Request

---

Prerequisites

Required Permissions

- Should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Update Secured Asset permissions (Organization)

Update Secured Asset permissions of a user role in an organization

The service updates secured asset permissions for a given user role

URL structure

HTTP PUT - Update Secured Asset permissions in an organization

```
HTTP PUT: https://{hostname}/api/roles
```

Parameters

Parameters	Type(maxlength)	Cardinality	Notes

Input Payload Template

Input Payload Template to Update Secured Asset permissions

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Roles>
        <Role>
                <RoleId></RoleId>
                <RoleName></RoleName>
                <OwningOrganizationId></OwningOrganizationId>
                <ProjectId></ProjectId>
                <SecuredAssets>
                        <SecuredAsset>
                                <Permission></Permission>
                                <SecuredAssetName></SecuredAssetName>
                        </SecuredAsset>
                </SecuredAssets>
        </Role>
</Roles>
```

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type (maxlength)	Cardinality	Constraints	Notes
Roles	Group	1		List of User Role in an organization
*Role	Attribute	1	• Should not be null	A specific user role in an organization
**RoleId	Attribute Integer	1	• Should not be null • Minimum value should be 1	Provides id of the user role
**RoleName	Attribute String	1	• Should not be null • Whitespace strings not allowed	Name of the user role
**OwningOrganizationId	Attribute Long	1		User Role's owning organization id
**ProjectId	Attribute Long	1		Default value is 0, as user roles are fetched from organization
**SecuredAssets	Group	1..n		List of secured assets related to a user role
***SecuredAsset	Attribute	1		Action intended to be performed on an asset

****Permission	Attribute
	
	String
		1	• Should not be null
			• Whitespace strings not allowed
			• Accepts only:
			  • `Grant`
			  • `Deny`
			  • `N/A`
				Describes the permission Grant to secured asset in context of a user role
				
				Permissions are:
				• `Grant`
				• `Deny`
				• `N/A`

****SecuredAssetName	Attribute String	1	• Should not be null • Whitespace strings not allowed	Name of the secured title

Role Secured Asset Names with UI Mapping:

When an update request is being sent, the tag `<SecuredAssetName>` name must be populated according the the column **Secured Asset Name** given in the table below.

S.No	UI Secured Asset Name	Secured Asset Name
1	Edit organization information	EDIT_OWN_ORGANIZATION
2	Create a new user	CREATE_USER_FOR_OWN_ORGANIZATION
3	Edit own user information	EDIT_OWN_USER
4	Edit all users information	EDIT_USER_FOR_OWN_ORGANIZATION
5	Assign user roles	EDIT_ROLE_USER_SETTINGS
6	Edit project settings	EDIT_PROJECT
7	Edit project password and session settings	EDIT_PROJECT_PASSWORD_SESSION
8	Create and edit Project Fields	PROJECT_FIELD
9	Configure mail approvals for organization	APPROVAL_ORGANIZATION_EDIT
10	Configure mail approvals for projects	APPROVAL_PROJECT_EDIT
11	Can be made a mail approver	PROCESS_APPROVALS
12	Create a guest user	CREATE_EXT_USER
13	Unlock any document	CHECK_IN_ANY_DOC_FOR_OWN_ORGANIZATION
14	View Project Participants	CAN_VIEW_PROJECT_PARTICIPANTS
15	Add users	CAN_ADD_PROJECT_PARTICIPANTS
16	Create mail	CREATE_MAIL
17	View organization's project mail	SEARCH_ALL_ORGANIZATIONS_MAIL
18	Upload new documents	CREATE_NEW_CONTROLLED_DOCUMENT
19	Update a document	EDIT_CONTROLLED_DOCUMENT
20	Manually update transmittal attachments	REGISTER_TRANSMITTAL_ATTACHMENTS
21	Create print requests	CREATE_PRINT_REQUEST
22	View print requests	VIEW_PRINT_REQUESTS
23	Run auto-update transmitted documents	AUTO_UPDATE_TRANSMITTED_DOCUMENTS
24	Run a transmittal history report	VIEW_TRANSMITTAL_HISTORY
25	View files using viewer	CAN_ACCESS_VIEWER
26	Mark up files in a Document Review process	CAN_EDIT_MARKUPS
27	Mark up files in the Document Register	CAN_EDIT_MARKUPS_IN_DOC_REGISTER
28	Create/edit a workflow template	CAN_CREATE_WORKFLOW_TEMPLATE
29	Initiate a workflow	CAN_INITIATE_WORKFLOW
30	Create a transmittal	CREATE_TRANSMITTAL
31	Manage related items	MANAGE_RELATED_ITEMS
32	Edit document confidentiality	EDIT_DOCUMENT_CONFIDENTIALITY
33	View Global Directory	VIEW_GLOBAL_DIRECTORY
34	Edit directory visibility	EDIT_DIRECTORY_VISIBILITY
35	Access Bulk Processing	CAN_USE_BULK_PROCESSING
36	Share saved searches	CAN_SHARE_DOC_SAVED_SEARCHES
37	Edit/delete shared saved searches	CAN_EDIT_DOC_SHARED_SAVED_SEARCHES

38	Share saved searches	CAN_SHARE_MAIL_SAVED_SEARCHES
39	Edit/delete shared saved searches	CAN_EDIT_MAIL_SHARED_SAVED_SEARCHES
40	Configure user notification type	CAN_CONFIGURE_USER_NOTIFICATION_TYPE
41	Configure user notification attachments size limit	CAN_CONFIGURE_USER_NOTIFICATION_ATTACHMENTS_SIZE_LIMIT
42	Allow setting of mail number prior to send	ALLOW_ALLOCATE_REAL_MAIL_NUMBERS_PRIOR_TO_SEND
43	Configure user roles	EDIT_ROLE_SECURED_ASSET_SETTINGS
44	Search document register	SEARCH_REGISTERED_DOCUMENTS
45	Edit Field Permissions	EDIT_FIELD_PERMISSIONS
46	Share upload profiles	CAN_SHARE_DOCUMENT_UPLOAD_PROFILE
47	Share saved searches	CAN_SHARE_WORKFLOW_SAVED_SEARCHES
48	Edit/delete shared saved searches	CAN_EDIT_WORKFLOW_SHARED_SAVED_SEARCHES
49	Workflow Administrator	WORKFLOW_ADMINISTRATOR
50	Supplier Documents Administrator	SUPPLIER_DOC_ADMINISTRATOR
51	Make sent mail your Response	MAKE_SENT_MAIL_YOUR_RESPONSE
52	Close-out organization's mail in any thread	CLOSE_OUT_OTHER_USER_MAIL
53	Share saved searches	CAN_SHARE_SUPPLIER_DOC_SAVED_SEARCHES
54	Edit/delete shared saved searches	CAN_EDIT_SUPPLIER_DOC_SHARED_SAVED_SEARCHES
55	Access via Web Services API	CAN_USE_EXTERNAL_API
56	Restore historical document to current version	CAN_RESTORE_HISTORICAL_DOCUMENT_AS_CURRENT
57	Mark documents as No Longer in Use	CAN_MARK_DOCUMENTS_AS_NO_LONGER_IN_USE
58	Configure Access Control	CAN_CONFIGURE_ACCESS_CONTROL
59	Edit user level session time duration	EDIT_USER_SESSION_TIME_DURATION
60	Access via Outlook Plugin	OUTLOOK_PLUGIN
61	Access via 2-Step Verification	ORG_CAN_GRANT_TSV_TO_ROLES
62	Access via Single Sign-On	ORG_CAN_GRANT_SSO_TO_ROLES
63	Review a workflow	CAN_REVIEW_DOCUMENT_APPROVAL_WORKFLOW
64	Configure mail forms	CAN_CONFIGURE_CUSTOM_FIELDS
65	Access Insights	CAN_VIEW_REPORTS
66	Access Models	CAN_ACCESS_BIM
67	Create Model Stack	CAN_CREATE_MODEL_STACKS
68	Create Design Issues	CREATE_DESIGN_ISSUE
69	Create Issue Sets	CREATE_DESIGN_ISSUE_SET
70	Design Issue Administrator	DESIGN_ISSUES_ADMINISTRATION
71	Create a Package	CREATE_PACKAGE
72	Send a Package	SEND_PACKAGE_VERSION
73	Configure Mail Distribution Rules	CONFIGURE_MAIL_ROUTING_RULES
74	Access Dropbox	CAN_ACCESS_DROPBOX
75	Access Box	CAN_ACCESS_BOX
76	Access Office Online	CAN_USE_OFFICE_ONLINE
77	Edit Document Field select-list values on upload/update	CAN_EDIT_DOCUMENT_FIELD_VALUES
78	Access via Mobile Apps	CAN_ACCESS_VIA_MOBILE_APPS

79	Share saved searches	CAN_SHARE_PACKAGE_SAVED_SEARCHES
80	Edit/delete shared saved searches	CAN_EDIT_PACKAGE_SHARED_SAVED_SEARCHES
81	Create private report layouts	CREATE_REPORT_LAYOUTS
82	Create new private reports	CREATE_REPORT_ONLY_SELF
83	Create Project Org reports	CREATE_SHARE_REPORT_PROJECT_ORG
84	Create Project reports	CREATE_SHARE_REPORT_PROJECT
85	Access Reports	CAN_VIEW_BIP_REPORTS
86	Remove Users	CAN_REMOVE_PROJECT_PARTICIPANTS
87	Control Project Directory Visibility	CAN_EDIT_PROJECT_DIRECTORY_VISIBILITY
88	Create placeholders	CAN_CREATE_PLACEHOLDERS
89	Reset 2-Step Verification	CAN_RESET_VERIFICATION_ENROLMENT
90	Export Project Settings	EXPORT_PROJECT_SETTINGS

For example if you are trying to update Secured Asset **Create a new user** , the value that needs to be sent in XML payload should be **CREATE_USER_FOR_OWN_ORGANIZATION**

Input Payload

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Roles>
        <Role>
                <RoleId>1879049026</RoleId>
                <RoleName>Basic User</RoleName>
                <OwningOrganizationId>1879048492</OwningOrganizationId>
                <ProjectId>0</ProjectId>
                <SecuredAssets>
                        <SecuredAsset>
                                <Permission>Grant</Permission>
                                <SecuredAssetName>CREATE_USER_FOR_OWN_ORGANIZATION</SecuredAssetName>
                        </SecuredAsset>
                </SecuredAssets>
        </Role>
</Roles>
```

Expected Response

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **200**

Examples/Samples

Sample Request

Sample request for updating Secured Asset Permissions for a user role in an organization

```
HTTP PUT https://au1.aconex.com/api/roles
Content-Type: application/xml;boundary="a1a1"

--a1a1

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Roles>
        <Role>
                <RoleId>1879049026</RoleId>
                <RoleName>Basic User</RoleName>
                <OwningOrganizationId>1879048492</OwningOrganizationId>
                <ProjectId>0</ProjectId>
                <SecuredAssets>
                        <SecuredAsset>
                                <Permission>Grant</Permission>
                                <SecuredAssetName>EDIT_OWN_USER</SecuredAssetName>
                        </SecuredAsset>
                        <SecuredAsset>
                                <Permission>Grant</Permission>
                                <SecuredAssetName>PROCESS_APPROVALS</SecuredAssetName>
                        </SecuredAsset>
                        <SecuredAsset>
                                <Permission>Grant</Permission>
                                <SecuredAssetName>CREATE_EXT_USER</SecuredAssetName>
                        </SecuredAsset>
                        <SecuredAsset>
                                <Permission>Grant</Permission>
                                <SecuredAssetName>CREATE_MAIL</SecuredAssetName>
                        </SecuredAsset>
                </SecuredAssets>
        </Role>
</Roles>
```

Sample Response

Response for updating Secured Asset permissions for a user role in an organization - Empty response

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
CONSTRAINT_VIOLATION	Input bean has constraint violations	400 Bad Request

Prerequisites

Required Permissions

- Should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Update Secured Asset permissions (Project)

Update Secured Asset permissions of a user role in a project

The service updates secured asset permissions for a given user role

URL structure

HTTP PUT - Update Secured Asset permissions in a project

```
HTTP PUT: https://{hostname}/api/roles/projects/{project_id}
```

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
project_id	string	1	Project id of the project admin

Input Payload Template

Input Payload Template to Update Secured Asset permissions

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Roles>
        <Role>
                <RoleId></RoleId>
                <RoleName></RoleName>
                <OwningOrganizationId></OwningOrganizationId>
                <ProjectId></ProjectId>
                <SecuredAssets>
                        <SecuredAsset>
                                <Permission></Permission>
                                <SecuredAssetName></SecuredAssetName>
                        </SecuredAsset>
                </SecuredAssets>
        </Role>
</Roles>
```

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type (maxlength)	Cardinality	Constraints	Notes
Roles	Group	1		List of User Role in a project
*Role	Attribute	1	• Should not be null	A specific user role in a project
**RoleId	Attribute Integer	1	• Should not be null • Minimum value should be 1	Provides id of the user role

**RoleName	Attribute String	1	• Should not be null • Whitespace strings not allowed	Name of the user role
**OwningOrganizationId	Attribute Long	1		User Role's owning organization id
**ProjectId	Attribute Long	1		Project id from the path parameter is only considered
**SecuredAssets	Group	1..n		List of secured assets related to a user role
***SecuredAsset	Attribute	1		Action intended to be performed on an asset

****Permission	Attribute
	
	String
		1	• Should not be null
			• Whitespace strings not allowed
			• Accepts only:
			  • `Grant`
			  • `Deny`
			  • `N/A`
				Describes the permission Grant to secured asset in context of a user role
				
				Permissions are:
				• `Grant`
				• `Deny`
				• `N/A`

****SecuredAssetName	Attribute String	1	• Should not be null • Whitespace strings not allowed	Name of the secured title

Role Secured Asset Names with UI Mapping:

When an update request is being sent, the tag <`SecuredAssetName`> name must be populated according the the column **Secured Asset Name** given in the table below.

S.No	UI Secured Asset Name	Secured Asset Name
1	Edit organization information	EDIT_OWN_ORGANIZATION
2	Create a new user	CREATE_USER_FOR_OWN_ORGANIZATION
3	Edit own user information	EDIT_OWN_USER
4	Edit all users information	EDIT_USER_FOR_OWN_ORGANIZATION
5	Assign user roles	EDIT_ROLE_USER_SETTINGS
6	Edit project settings	EDIT_PROJECT
7	Edit project password and session settings	EDIT_PROJECT_PASSWORD_SESSION
8	Create and edit Project Fields	PROJECT_FIELD
9	Configure mail approvals for organization	APPROVAL_ORGANIZATION_EDIT
10	Configure mail approvals for projects	APPROVAL_PROJECT_EDIT
11	Can be made a mail approver	PROCESS_APPROVALS
12	Create a guest user	CREATE_EXT_USER
13	Unlock any document	CHECK_IN_ANY_DOC_FOR_OWN_ORGANIZATION
14	View Project Participants	CAN_VIEW_PROJECT_PARTICIPANTS
15	Add users	CAN_ADD_PROJECT_PARTICIPANTS
16	Create mail	CREATE_MAIL
17	View organization's project mail	SEARCH_ALL_ORGANIZATIONS_MAIL
18	Upload new documents	CREATE_NEW_CONTROLLED_DOCUMENT
19	Update a document	EDIT_CONTROLLED_DOCUMENT
20	Manually update transmittal attachments	REGISTER_TRANSMITTAL_ATTACHMENTS

21	Create print requests	CREATE_PRINT_REQUEST
22	View print requests	VIEW_PRINT_REQUESTS
23	Run auto-update transmitted documents	AUTO_UPDATE_TRANSMITTED_DOCUMENTS
24	Run a transmittal history report	VIEW_TRANSMITTAL_HISTORY
25	View files using viewer	CAN_ACCESS_VIEWER
26	Mark up files in a Document Review process	CAN_EDIT_MARKUPS
27	Mark up files in the Document Register	CAN_EDIT_MARKUPS_IN_DOC_REGISTER
28	Create/edit a workflow template	CAN_CREATE_WORKFLOW_TEMPLATE
29	Initiate a workflow	CAN_INITIATE_WORKFLOW
30	Create a transmittal	CREATE_TRANSMITTAL
31	Manage related items	MANAGE_RELATED_ITEMS
32	Edit document confidentiality	EDIT_DOCUMENT_CONFIDENTIALITY
33	View Global Directory	VIEW_GLOBAL_DIRECTORY
34	Edit directory visibility	EDIT_DIRECTORY_VISIBILITY
35	Access Bulk Processing	CAN_USE_BULK_PROCESSING
36	Share saved searches	CAN_SHARE_DOC_SAVED_SEARCHES
37	Edit/delete shared saved searches	CAN_EDIT_DOC_SHARED_SAVED_SEARCHES
38	Share saved searches	CAN_SHARE_MAIL_SAVED_SEARCHES
39	Edit/delete shared saved searches	CAN_EDIT_MAIL_SHARED_SAVED_SEARCHES
40	Configure user notification type	CAN_CONFIGURE_USER_NOTIFICATION_TYPE
41	Configure user notification attachments size limit	CAN_CONFIGURE_USER_NOTIFICATION_ATTACHMENTS_SIZE_LIMIT
42	Allow setting of mail number prior to send	ALLOW_ALLOCATE_REAL_MAIL_NUMBERS_PRIOR_TO_SEND
43	Configure user roles	EDIT_ROLE_SECURED_ASSET_SETTINGS
44	Search document register	SEARCH_REGISTERED_DOCUMENTS
45	Edit Field Permissions	EDIT_FIELD_PERMISSIONS
46	Share upload profiles	CAN_SHARE_DOCUMENT_UPLOAD_PROFILE
47	Share saved searches	CAN_SHARE_WORKFLOW_SAVED_SEARCHES
48	Edit/delete shared saved searches	CAN_EDIT_WORKFLOW_SHARED_SAVED_SEARCHES
49	Workflow Administrator	WORKFLOW_ADMINISTRATOR
50	Supplier Documents Administrator	SUPPLIER_DOC_ADMINISTRATOR
51	Make sent mail your Response	MAKE_SENT_MAIL_YOUR_RESPONSE
52	Close-out organization's mail in any thread	CLOSE_OUT_OTHER_USER_MAIL
53	Share saved searches	CAN_SHARE_SUPPLIER_DOC_SAVED_SEARCHES
54	Edit/delete shared saved searches	CAN_EDIT_SUPPLIER_DOC_SHARED_SAVED_SEARCHES
55	Access via Web Services API	CAN_USE_EXTERNAL_API
56	Restore historical document to current version	CAN_RESTORE_HISTORICAL_DOCUMENT_AS_CURRENT
57	Mark documents as No Longer in Use	CAN_MARK_DOCUMENTS_AS_NO_LONGER_IN_USE
58	Configure Access Control	CAN_CONFIGURE_ACCESS_CONTROL
59	Edit user level session time duration	EDIT_USER_SESSION_TIME_DURATION
60	Access via Outlook Plugin	OUTLOOK_PLUGIN
61	Access via 2-Step Verification	ORG_CAN_GRANT_TSV_TO_ROLES

62	Access via Single Sign-On	ORG_CAN_GRANT_SSO_TO_ROLES
63	Review a workflow	CAN_REVIEW_DOCUMENT_APPROVAL_WORKFLOW
64	Configure mail forms	CAN_CONFIGURE_CUSTOM_FIELDS
65	Access Insights	CAN_VIEW_REPORTS
66	Access Models	CAN_ACCESS_BIM
67	Create Model Stack	CAN_CREATE_MODEL_STACKS
68	Create Design Issues	CREATE_DESIGN_ISSUE
69	Create Issue Sets	CREATE_DESIGN_ISSUE_SET
70	Design Issue Administrator	DESIGN_ISSUES_ADMINISTRATION
71	Create a Package	CREATE_PACKAGE
72	Send a Package	SEND_PACKAGE_VERSION
73	Configure Mail Distribution Rules	CONFIGURE_MAIL_ROUTING_RULES
74	Access Dropbox	CAN_ACCESS_DROPBOX
75	Access Box	CAN_ACCESS_BOX
76	Access Office Online	CAN_USE_OFFICE_ONLINE
77	Edit Document Field select-list values on upload/update	CAN_EDIT_DOCUMENT_FIELD_VALUES
78	Access via Mobile Apps	CAN_ACCESS_VIA_MOBILE_APPS
79	Share saved searches	CAN_SHARE_PACKAGE_SAVED_SEARCHES
80	Edit/delete shared saved searches	CAN_EDIT_PACKAGE_SHARED_SAVED_SEARCHES
81	Create private report layouts	CREATE_REPORT_LAYOUTS
82	Create new private reports	CREATE_REPORT_ONLY_SELF
83	Create Project Org reports	CREATE_SHARE_REPORT_PROJECT_ORG
84	Create Project reports	CREATE_SHARE_REPORT_PROJECT
85	Access Reports	CAN_VIEW_BIP_REPORTS
86	Remove Users	CAN_REMOVE_PROJECT_PARTICIPANTS
87	Control Project Directory Visibility	CAN_EDIT_PROJECT_DIRECTORY_VISIBILITY
88	Create placeholders	CAN_CREATE_PLACEHOLDERS
89	Reset 2-Step Verification	CAN_RESET_VERIFICATION_ENROLMENT
90	Export Project Settings	EXPORT_PROJECT_SETTINGS

For example if you are trying to update Secured Asset **Create a new user** , the value that needs to be sent in XML payload should be **CREATE_USER_FOR_OWN_ORGANIZATION**
Input Payload

Input payload

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Roles>
    <Role>
        <RoleId>1879049026</RoleId>
        <RoleName>Basic User</RoleName>
        <OwningOrganizationId>1879048492</OwningOrganizationId>
        <ProjectId>1234567890</ProjectId>
        <SecuredAssets>
            <SecuredAsset>
                <Permission>Grant</Permission>
                <SecuredAssetName>CREATE_USER_FOR_OWN_ORGANIZATION</SecuredAssetName>
            </SecuredAsset>
        </SecuredAssets>
    </Role>
</Roles>
```

Expected Response

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **200**

Examples/Samples

Sample Request

Sample request for updating Secured Asset Permissions for a user role in a project

```
HTTP PUT https://au1.aconex.com/api/roles/projects/1234567890
Content-Type: application/xml;boundary="a1a1"

--a1a1

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Roles>
        <Role>
                <RoleId>1879049026</RoleId>
                <RoleName>Basic User</RoleName>
                <OwningOrganizationId>1879048492</OwningOrganizationId>
                <ProjectId>1234567890</ProjectId>
                <SecuredAssets>
                        <SecuredAsset>
                                <Permission>Grant</Permission>
                                <SecuredAssetName>EDIT_OWN_USER</SecuredAssetName>
                        </SecuredAsset>
                        <SecuredAsset>
                                <Permission>Grant</Permission>
                                <SecuredAssetName>PROCESS_APPROVALS</SecuredAssetName>
                        </SecuredAsset>
                        <SecuredAsset>
                                <Permission>Grant</Permission>
                                <SecuredAssetName>CREATE_EXT_USER</SecuredAssetName>
                        </SecuredAsset>
                        <SecuredAsset>
                                <Permission>Grant</Permission>
                                <SecuredAssetName>CREATE_MAIL</SecuredAssetName>
                        </SecuredAsset>
                </SecuredAssets>
        </Role>
</Roles>
```

Sample Response

Response for updating Secured Asset permissions for a user role in a project - Empty response

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
CONSTRAINT_VIOLATION	Input bean has constraint violations	400 Bad Request

Prerequisites

Required Permissions

- Should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Update Users assigned to User Role (Organization)

Update users assigned to a user role in an organization

The service updates assignment/removal of users assigned to a user role in an organization.

URL structure

HTTP PUT - Update users assigned to a user role in an organization

```
HTTP PUT: https://{hostname}/api/roles/userrole
```

Parameters

Parameters	Type(maxlength)	Cardinality	Notes

Input Payload Template

Input Payload template to Update users assigned to user role

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Users>
        <User>
                <UserId></UserId>
                <Roles>
                        <Role>
                                <RoleId></RoleId>
                                <AssignRole></AssignRole>
                        </Role>
                </Roles>
        </User>
</Users>
```

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Constraint	Notes
Users	Attribute	1..n		List of users whose roles needs to be updated
*User	Attribute	1.	• Should not be null	
**UserId	String	1	• Should not be null • Minimum value should be 1	
**Roles	Attribute	1..n		List of roles assigned to a user that needs to be updated
***Role	Attribute	1	• Should not be null	
****RoleId	String	1	• Should not be null • Whitespace strings not allowed	

****AssignRole	Boolean	1	• Should not be null	Provide true/false. • true - Assigns the role to user • false - Removes the role from user

Expected Response

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **200**

Examples/Samples

Sample Request

Sample request for updating users assigned to an user role in an organization

```
HTTP PUT https://au1.aconex.com/api/roles/userrole
Content-Type: application/xml;boundary="a1a1"

--a1a1

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Users>
        <User>
                <UserId>1879049248</UserId>
                <Roles>
                        <Role>
                                <RoleId>1879048193</RoleId>
                                <AssignRole>true</AssignRole>
                        </Role>
                        <Role>
                                <RoleId>1879048195</RoleId>
                                <AssignRole>true</AssignRole>
                        </Role>
                </Roles>
        </User>
        <User>
                <UserId>1879049452</UserId>
                <Roles>
                        <Role>
                                <RoleId>1879048195</RoleId>
                                <AssignRole>true</AssignRole>
                        </Role>
            <Role>
                                <RoleId>1879048207</RoleId>
                                <AssignRole>false</AssignRole>
                        </Role>
                </Roles>
        </User>
</Users>
```

Sample Response

Response for updating users assigned to user role in an organization - Empty response

---

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code

LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
CONSTRAINT_VIOLATION	Input bean has constraint violations	400 Bad Request

---

Prerequisites

Required Permissions

- Should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Update Users assigned to User Role (Project)

Update users assigned to a user role in a project

The service updates assignment/removal of users assigned to a user role in a project.

URL structure

HTTP PUT - Update users assigned to a user role in a project

```
HTTP PUT: https://{hostname}/api/roles/userrole/projects/{project_id}
```

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
project_id	string	1	

Input Payload Template

Input Payload template to Update users assigned to user role

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Users>
        <User>
                <UserId></UserId>
                <Roles>
                        <Role>
                                <RoleId></RoleId>
                                <AssignRole></AssignRole>
                        </Role>
                </Roles>
        </User>
</Users>
```

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Constraint	Notes
Users	Attribute	1..n		List of users whose roles needs to be updated
*User	Attribute	1.	• Should not be null	
**UserId	String	1	• Should not be null • Minimum value should be 1	
**Roles	Attribute	1..n		List of roles assigned to a user that needs to be updated
***Role	Attribute	1	• Should not be null	
****RoleId	String	1	• Should not be null • Whitespace strings not allowed	
****AssignRole	Boolean	1	• Should not be null	Provide true/false. • true - Assigns the role to user • false - Removes the role from user

Expected Response

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **200**

Examples/Samples

Sample Request

Sample request for updating users assigned to an user role in a project

```
HTTP PUT https://au1.aconex.com/api/roles/userrole/projects/1234567
Content-Type: application/xml;boundary="a1a1"

--a1a1

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Users>
        <User>
                <UserId>1879049248</UserId>
                <Roles>
                        <Role>
                                <RoleId>1879048193</RoleId>
                                <AssignRole>true</AssignRole>
                        </Role>
                        <Role>
                                <RoleId>1879048195</RoleId>
                                <AssignRole>true</AssignRole>
                        </Role>
                </Roles>
        </User>
        <User>
                <UserId>1879049452</UserId>
                <Roles>
                        <Role>
                                <RoleId>1879048195</RoleId>
                                <AssignRole>true</AssignRole>
                        </Role>
            <Role>
                                <RoleId>1879048207</RoleId>
                                <AssignRole>false</AssignRole>
                        </Role>
                </Roles>
        </User>
</Users>
```

Sample Response

Response for updating users assigned to user role in a project - Empty response

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
CONSTRAINT_VIOLATION	Input bean has constraint violations	400 Bad Request

Prerequisites

Required Permissions

- Should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Delete User Role (Organization)

Deletes a user role in an organization

The service deletes a user role in an organization and disposes the role name which has been granted to the users

URL structure

HTTP POST - Delete a user role in an organization
`HTTP DELETE: https://{hostname}/api/roles/{role_id}`

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
role_id	integer	1	Role Id of the user role

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **200**

Examples/Samples

Sample Request

- Delete a user role in an organization

Sample request for deleting a user role in organization
`https://au1.aconex.com/api/roles/1234567`

Sample Response

Response for deleting a user role in an organization - Empty response

---

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
ROLE_NOT_FOUND	Role not found with given role id	400 Bad Request

Prerequisites

Required Permissions

- User should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs

Delete User Role (Project)

Delete a user role in a project

The service deletes a user role in a project and disposes the role name which has been granted to the users

URL structure

HTTP POST - Delete a user role in a project
`HTTP DELETE: https://{hostname}/api/roles/projects/{project_id}/{role_id}`

Parameters

Parameters	Type(maxlength)	Cardinality	Notes
project_id	string	1	
role_id	integer	1	Role Id of the user role

Expected Response

Cardinality refers to the number of repetitions a field can have. A cardinality that allows zero (0) means the field is optional, and may not appear in the response.

The number of *'s indicate the parent-child depth.

Element	Type(maxlength)	Cardinality	Notes

An empty response body with HTTP status code **200**

Examples/Samples

Sample Request

- Delete a user role in a project

Sample request for deleting a user role in project
`https://au1.aconex.com/api/roles/projects/987654/1234567`

Sample Response

Response for deleting a user role in a project - Empty response

Error Codes Specific to the Service

Status Code	Description	HTTP Status Code
LOGIN_FAILED	Login failed - username or password incorrect	401 Unauthorized
ACCESS FAILED FOR ORG	Organization not permitted to use API	401 Unauthorized
ROLE_NOT_FOUND	Role not found with given role id	400 Bad Request

Prerequisites

Required Permissions

- User should have **EDIT_ROLE_ACCESS**

Preferences/Module Setup

Not applicable

Related APIs