

## jUDDI Access Control Enhancements Proposal

<https://issues.apache.org/jira/browse/JUDDI-558>

To summarize, I would like to have jUDDI implement of Role Based Access Control (RBAC) with roles being provided either by the UDDI container or from an external source such as an LDAP group. A default set of global roles must be defined and included and preconfigured with the distro. These roles provide global level permissions into all entities in the registry. Additional role permissions can be added either on a global basis or per entity

### Global Roles

- Admin – all actions
- Manager – can add businesses and delegate permissions
- Auditor – can review audit logs, read all entities, no other implicit permissions
- Service Level Monitoring – can alter the values of tmodels on any entity
- Other, ability for admins to define a new role category and its permission set across all entities, useful for adding external roles (ldap groups)

Permission Sets. Note – I'm probably missing a few here.

### Registry/Node

- Delegate Permissions below
- Add/Remove/Alter businesses, services, binding templates, tmodels
- Delegate permission down
- Cross node federation (subscription)
- Custody transfer?
- Create/Delete tmodels
- Plus everything below

### Per Business

- Alter business entity
- Add services, binding templates, attach tmodels
- Delegate permissions down
- Plus everything below

### Per Service

- Add binding templates
- Attach tmodels on the service, binding templates
- Remove binding templates
- Alter binding templates

### New web service methods

- Permission Check (role, entity/all) (allow/deny, list of global roles)

- Enumerate Permissions (role or entity) equivalent of RSoP
- Add Permission (role, entity/all) explicit allow
- Remove Permission (role, entity/all) implicit deny
- Read audit logs by entity (offset, limit, entity type, entity identifier)
- Read audit logs by user (offset, limit)
- Purge audit logs

#### Proposed Database schema

Role	AppliesToIdentifier	AppliesToType	Read	Update	Delete	Delegate	Audit	Create
Group 1	{some guid}	BUSINESS	X	X	X		X	X

Note, not all columns are present. This idea still needs to be flushed out

While we're at it, we might as well add a new ws endpoint

List<Uri> FindEndpoints (BindingKey)

List<Uri> FindEndpoints (ServiceKey)