CHAPTER 6

Permissions

Entity Permissions

The Self Service Catalog deploys permissions for entities as part of the entity. When permissions are removed from the entity in its Home site, the application does not leave behind deletion stubs (or a transaction log) that Self Service Catalog may use to replicate this removal. For example, when the permission to order a service is removed from an Organizational Unit on a Service Definition, Service Portal does not retain this fact, it simply removes the permission data.

A user must be granted a role that includes the import and deploy capabilities in order to import. When you deploy a service whose permissions have been changed, all associations between the service definition and its permissions are dropped in the target site and recreated according to the permissions in effect in the source site. Any deleted permissions will be reflected. However, if the permission was granted to a custom role or group, and the role or group was deleted from the source site, the role or group will still exist in the target site. Self Service Catalog cannot propagate entity deletions.

Editing Security Access

TES Services

To edit (grant/revoke) security access for TES services for an individual user:

Step 1 Log in to the Cisco Service Portal as *Admin* and navigate to the Organization Designer.

Step 2 Click the **People** page and add the same roles that are used in StTES_SERVICES for the exposed function.

To edit (grant/revoke) security access for TES services for a Group or Org Unit:

Security roles can be assigned to groups or org units.

If a user belongs to the group or org unit that contains roles with access to TES services, then the user would have access to that TES service.

To edit (grant/revoke) security access for TES services in the Cisco Service Portal service level:

Step 1 Log in to the Cisco Service Portal as *Admin* and navigate to the Service Designer.

Service Portal allows service designers and site administrators to establish authorizations at several levels:

- Site. Authorizations at the site-level establish the default authorization structure for all services for the site. These authorizations are maintained in the Administration module>Authorizations page, or by selecting the Site (top-most) node in the Service Designer>Catalog component.
- Organizational Unit. Authorizations at the organizational unit level establish the authorization structure for the departmental authorization and review by the current organization. The specified structure can be set to either override or supplement site-wide authorization. Organizational unit authorizations are maintained via the Organization Designer module>Org Units tab>Authorization link.
- Service Group. Authorizations at the service group level establish the authorization structure for the service group. This structure can be set to either override or supplement the site authorization structure. Authorizations for service groups are maintained by selecting the Service Group in the Service Catalog of Service Designer and clicking on the Authorizations tab.
- Service. Authorizations at the individual service level establish the authorization structure for that service.

  Service-level authorizations are maintained via the Authorizations tab for the selected service.

Step 2 To expose a TES function, create a new entry in the permission that has access to the TES services.

The entries for each service **Launch**, **Rerun**, **Cancel**, **Hold**, and **Resume** display.

StTES_JOBS

To edit (grand/revoke) security access for StTES_JOBS standard in the Service Item Manager level:

Step 1 Log in to the Cisco Service Portal as *Admin* and navigate to the **Organization Designer**.

Step 2 Select the role and add the **Service Item Manager** capabilities.