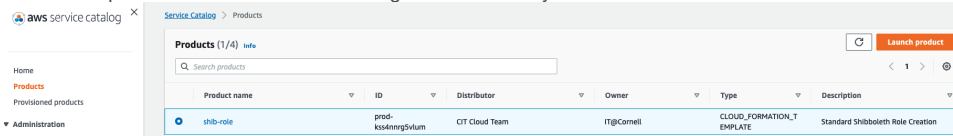


Creating Shibboleth IAM Roles with Service Catalog

The Service Catalog product is called 'shib-role' and is deployed to all AWS accounts to simplify the shibboleth IAM role creation process.

1. Launch the product from the Service Catalog Console within your AWS Account



2. Enter a Provisioned Product Name; this can be something that makes sense to you (ie. shib-developers)

Launch: shib-role [Info](#)

Standard Shibboleth Role Creation

Provisioned product name

Provisioned product name

Enter a unique name or select Generate name to provide a name automatically.

The name must start with a letter (A-Z, a-z) or number (0-9). Other valid characters include: hyphen (-), underscore (_), and period (.).

☐ Generate name

3. Choose a product version
4. Enter the product parameters

Product versions (1/1)

	Version	Created time	ID	Guidance	Description
<input checked="" type="radio"/>	v1.4.1	Tue, Apr 5, 2022, 6:07:50 PM EDT	pa-7c5rxe7ncsf74	DEFAULT	Updated parameter field constraints

Parameters

ADGroupName

Required! Enter an existing AD group name that contains members for this shibboleth role access

ProductContact

Required! Enter netID for Product Completion Notification. This product requires additional action to be performed by the CIT Cloud Team, this value is who will be contacted when tasks are complete.

Must not be blank and be standard netID formatting

RoleName

Required! Enter desired role name (this should NOT include the shib- prefix)

Parameter Input Limitations

Parameters


ADGroupName

Required! Enter an existing AD group name that contains members for this shibboleth role access

 Must not be blank and cannot contain the following characters # , + " \ < > ;

ProductContact

Required! Enter netID for Product Completion Notification. This product requires additional action to be performed by the CIT Cloud Team, this value is who will be contacted when tasks are complete.

 Must not be blank and be standard netID formatting

RoleName

Required! Enter desired role name (this should NOT include the shib- prefix)

 Must not be blank and contain only alphanumeric characters and underscores ' _ '

- a. ADGroupName = An AD group to be nested for granting access to this shibboleth role. This group should contain the member(s) who will need access to AWS.
 - i. What can I enter in this field?
 1. **Must not be blank and cannot contain the following characters # , + " \ < > ;**
 - ii. What if I do not have an Active Directory group to provide?
 1. Please review the following for creating Active Directory groups - <https://it.cornell.edu/cornellad-cuvpn-group/create-group-cornellad>
 - b. ProductContact = This should be the netID of the individual filling out this form and who the Cloud Team will contact once manual actions are completed on our end.
 - i. What can I enter in this field?
 1. **Must not be blank and be standard netID formatting**
 - c. RoleName = The name of the IAM role, excluding the 'shib-' prefix, ie. 'developers'
 - i. What can I enter in this field?
 1. **Must not be blank and contain only alphanumeric characters and underscores ' _ '**
5. Select 'Launch Product'
 - a. A notification and TDX ticket is sent to the CIT Cloud Team Support queue for the remaining steps.
 6. Create / Attach an IAM Policy to this newly created role.