# How to Create Policy

**Environment :** Xcitium Dome Secure Web Gateway

**Summary :** After enrolling networks as explained in how-to-add-new-location, the default global policy will be applied automatically to end users in your networks. Dome SWG allows you to create new policies then deploy them to your networks as required. In addition, you can also create and deploy polices that are tailored for specific users, groups and departments

**Video Tutorial: Click to open the Video Tutorial**

**Prerequisites**

- It is assumed that you have already C1 account

- It is assumed that you have already Dome SWG instance in your C1 portal

- It is assumed that you have already add your location (please read how-to-add-new-location )

**Configuration Steps:**

***Step 1 : Connecting Dome SWG Portal***

i. Login to C1 portal from https://one..Xcitium com

ii. Go to **Application** --> **cDome Standard**

iii. Cdome Standard (SWG) portal will be opened on another tab

**Step 2: Creating New Policy**

After enrolling networks as explained in how-to-add-new-location, the default global policy will be applied automatically to end users in your networks. Dome SWG allows you to create new policies then deploy them to your networks as required. In addition, you can also create and deploy polices that are tailored for specific users, groups and departments

i. Go to **Configuration -- > Policy**

ii. Click on "**New Policy**" button

iii. Enter Policy Name and Remark (optional)

- **Policy Order :** Select where the rule has to be placed. The drop-down will display the number of rules that are currently available. If you select '1', then the policy will be placed at the top of the list.
- **Name:**Enter a name for the policy.
- **Remark :** Enter appropriate comments for the policy.

iv. Click '**Next**' to proceed 'Select Object'

v. In the '**Select Objects**' section, you can specify the object(s) for which you want to apply the policy

- **Select Location** – By default 'Any' will be selected. Click on the field and select the trusted network from the list. The networks that are added in Locations will be displayed from the drop-down including 'Roaming Users' to apply the policy to roaming devices. To add new location please see how-to-add-new-location
- **Select User** – By default 'Any' will be selected. Click on the field and select the user(s) from the list. The users that are added in User Management will be displayed from the drop-down.

- **Select Group** – By default 'Any' will be selected. Click on the field and select the group(s) from the list. The groups that are added in User Management will be displayed from the drop-down.
- **Select Department** – By default 'Any' will be selected. Click on the field and select the department(s) from the list. The departments that are added in User Management will be displayed from the drop-down.

vi. Click '**Next**' to process further

vii. In **Apply Policy** section , you can specify the security and web content profiles that you want to add to the policy.

- **Advanced Threat Protection Profile** – The default profile will be selected. The drop-down will display the ATP exception profiles that are available in Security Policy section. Select the appropriate ATP profile from the list.
- **Containment** – Select whether you want to run unknown files in the sandbox. Refer to the section 'Configuring Containerization Settings' for more details. By default, Containment is enabled.
- **URL Filtering Profile** – The default profile will be selected. The drop-down will display the URL filtering profiles that are available in URL Filtering section. Select the appropriate URL filtering profile from the list.
- **SSL Inspection Settings** - Allows you to configure how Dome Standard should act if SSL certificates for the visited websites are untrusted or revoked. Please note this is a global setting, meaning any modification done will apply for all the policies. Clicking the 'Show Details' link will open the 'SSL Inspection' page. Refer to the section 'Configuring SSL Inspection Settings' for more details.
- **File Type Control Policy** – Displays file download restriction rules that were created in 'Configuration' > 'WebContent Policy' > 'File Type Control'. See File Type Control Rules for more about this area. Select the appropriate file control rule you wish to apply.

viii. Click **Create** button to apply your policy.