Deploying and Configuring Secure Global Desktop Portlet

This user guide provides a brief introduction about the Secure Global Desktop (SGD) portlet and explains how you can install and configure SGD portlet in Portal Server 7.2.

Secure Global Desktop Portlet

The SGD portlet adheres to the JSR 168 standard for writing portlets and aims to securely access and transfer information between SGD and Portal Server using SRA. The SGD portlet uses Single Sign-On mechanism and enables to launch Webtop sessions from within a portlet.

The SGD portlet can be configured by setting the following preferences.

▼ To Deploy and Configure SGD Portlet Using portal Server Console

Before You Begin

- Install Sun Java System Portal Server version 7.1 or above.
- Install SGD Server version 4.2.x or 4.3.x.
- Deploy SGD portlet.
- Login to Portal Server console and create a channel for SGD portlet.
- Edit the portlet properties and set the preferences as mentioned below.

1. **Login to Portal Server console.**
2. **Click Portals tab.**
   The Portals page appears.
3. **In the Portals pane, click portal1.**
   The Desktop Tasks and Attributes page appears.
4. **Select Enterprise Sample Org from the Select DN drop down list.**
5. **Under Tasks, click Deploy Portlet.**
   The Deploy Portlet wizard appears.
6. **In the Select Portal and DN page, select the Portal as portal 1 and DN as Enterprise Sample [Org] and click Next.**
   The Enter the Portlet WAR and Portlet Deployment Information page appears.
7. **Click Browse to choose the WAR file, Roles File, and Users file and click Next.**
   The Verify Information page appears.
8. **Verify the information that you choose and click Next.**
   The Results page appears.
9. **Click Finish to deploy the portlet.**
10. **Click Manage Containers & Channels in the Desktop Tasks and Attributes page.**
    The Manage Containers and Channels for the Portal that you have selected (portal 1) appears.
11. **In the left pane, click WorkContainer from the list of available containers.**
    The WorkContainer specific tasks and properties appear in the right pane.
12. **Under Tasks, click New Channel or Container.**
    The New Channel or Container wizard appears.
13. **In the Specify Portal and DN for Channel or Container page, select Portal as portal 1, DN as Enterprise Sampe [Org], and Type as Channel and click Next.**
    The Specify Channel Type page appears.

14 **Choose the Channel Type as Portlet Channel (JSR 168 or JSR 286) and click Next.**

The Specify Provider/Portlet/Producer Name page appears.

15 **Select a Portlet from the list and click Next.**

The Specify Channel Name page appears.

16 **Specify a name for the channel that you create. For example, sgdportletchannel and click Next.**

The Review page appears.

17 **Review the information that you have provided for Channel type, Name, and Provider. Click Finish.**

The Results page appears. A message appears that a new channel has been created.

18 **Click Close.**

The new channel is created and listed under the WorkContainer in the left pane of the Manage Containers and Channels for portal 1 page. The right pane displays the Tasks, Portlet Preferences, and Properties for the new channel.

19 **Set the `location` property of the SGD portlet as URL for SGD for Web Services. Usually, this URL is an HTTP or HTTPS that refers the SGD Web Server. The default URL is `http://localhost:80/axis/services/rpc/`.**

For example, if you want to configure for `access.indigo-insurance.com`, using HTTPS on port 8080, the format is `https://access.indigo-insurance.com:8080/axis/services/rpc/`.

Note – This URL is used by the web services client of the portlet. So, you can use the DNS name and port that are appropriate for resolution and connection from the host running the portal application.

---

20 **Set the `sgdaccess`, which is the access key to enable shared login between the portal application and SGD server.**

Set the `sgdaccess` value provided in the *tomcat-base*`/webapps/sgd/WEB-INF/classes/com/tarantella/tta/webservices/client/views/Resources.properties` file on your SGD server. The `sgdaccess` value format looks something similar to this `c2dkX3RydXN0ZWRfdXNlcjpJcSxnVDBHI2I0LVlxYUZAeFRkSA==`.

Note – The `sgdaccess` preference is optional. If you do not set this preference, set incorrectly, or if the third party authentication is disabled in Secure Global Desktop server, you will be provided with the standard SGD login, form where you can choose to save the SGD credentials for automatic login later.

---

21 **Set the Tarantella Client location, using the `tcc-location` preference. The base URL for the client can be set as optional, using the `tcc-location` preference. You can use either an absolute or relative URL. When you use a relative URL, you can download the client from the portlet application. When you set the `tcc-location` preference to `/tcc`, the portlet will proxy requests to the SGD Web Server.**

Note – This preference is for advanced use. Usually, the Tarantella Client is downloaded directly from the SGD Web Server by the web browser.

---

22 **Set the `tcc-sra-proxy-route` preference (network connection rule), to enable the SGD client route its AIP traffic through the SOCKS proxy using the local Netlet. This setting is only used, if the portlet detects that it is running through an SRA. If running in OpenPortal server mode, this setting is not used.**

For example, if the Netlet was listening on port 5555, the `tcc-sra-proxy-route` attribute will be `CTSOCKS:localhost:5555` or if SOCKS proxy is not used, then it is `CTTTAP:localhost:5555`.

▼ To Create and Configure a Static Netlet Rule

Follow the steps to create and configure a static Netlet rule.

1. **Login to Portal Server console and navigate to Secure Remote Access -> Netlet.**
2. **Select the appropriate DN, to specify the organization where you have deployed the SGD portlet and need to add the Netlet rule.**
3. **Create a new Netlet rule. To do this, navigate to Advanced -> Rules. Click create a new rule.**
4. **Enter a Rule name. Type the Local port value as 5555. This is the port on which Netlet listens on the client browser. Type the SOCK proxy server Fully Qualified Domain Name as Destination Host and SOCK proxy server port as Destination Port.**
5. **Save the Rule.**

820-4274

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A.