

GSISsh-Term

[GSISsh-Term](#) is a Java based terminal client application for accessing the Grid.

Users have to place the required grid certificates appropriately in their machine before they can access grid. Please follow the following steps:

Prerequisites:

Jdk version 1.5 or Above.If you don't have you can go to "<http://www.oracle.com/technetwork/java/javase/downloads/index.html>" and download the latest version and install.

After the installation of jdk click the below link and download the GSISsh-Term tool.It will start downloading the tool and install in your system.

Download GSISsh-Term: <http://portal.garudaindia.in/gsisshterm/jws.jnlp>

Step 1:

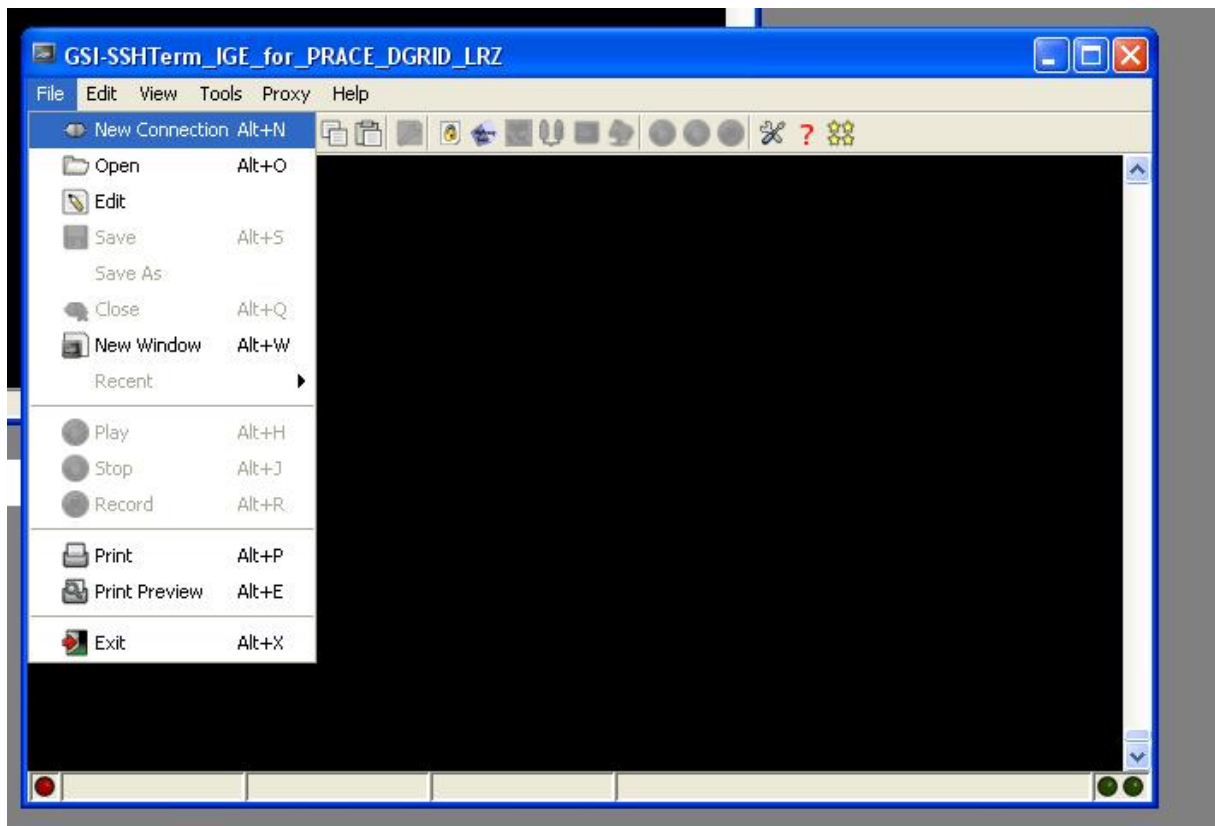
Once the installation of completed ,Go to Start ->All Programs -> GSI-SSHTerm.You will get the following window.Accept the policy and click on run.



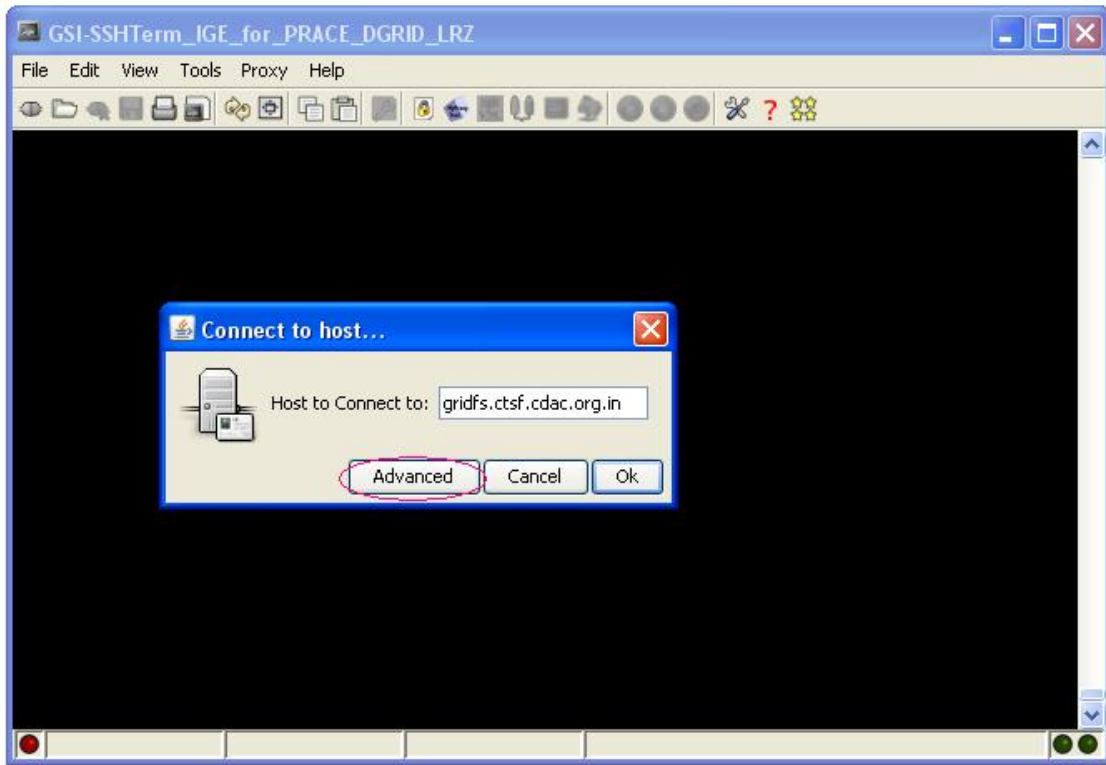
Step 2:
Accept the policy and click on run again.



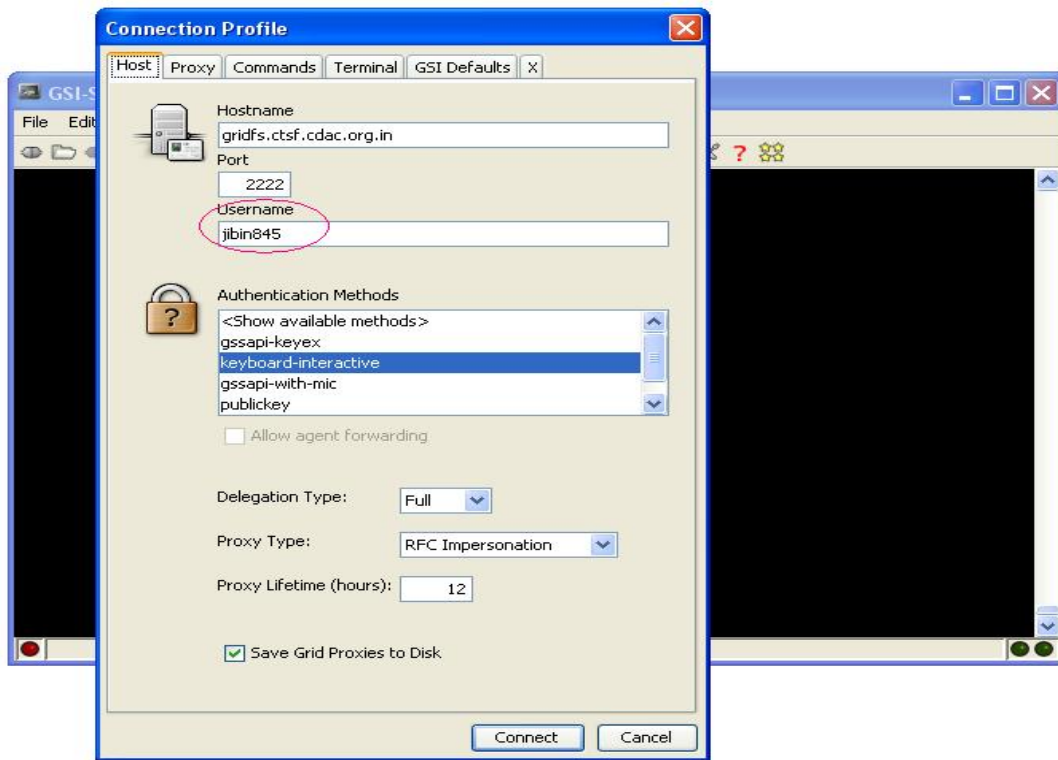
Step 3:
Now go to File and Click on New Connection.



Step 4: In Host to Connect to window enter "**gridfs.ctsf.cdac.org.in**" and Click on Advanced Button.

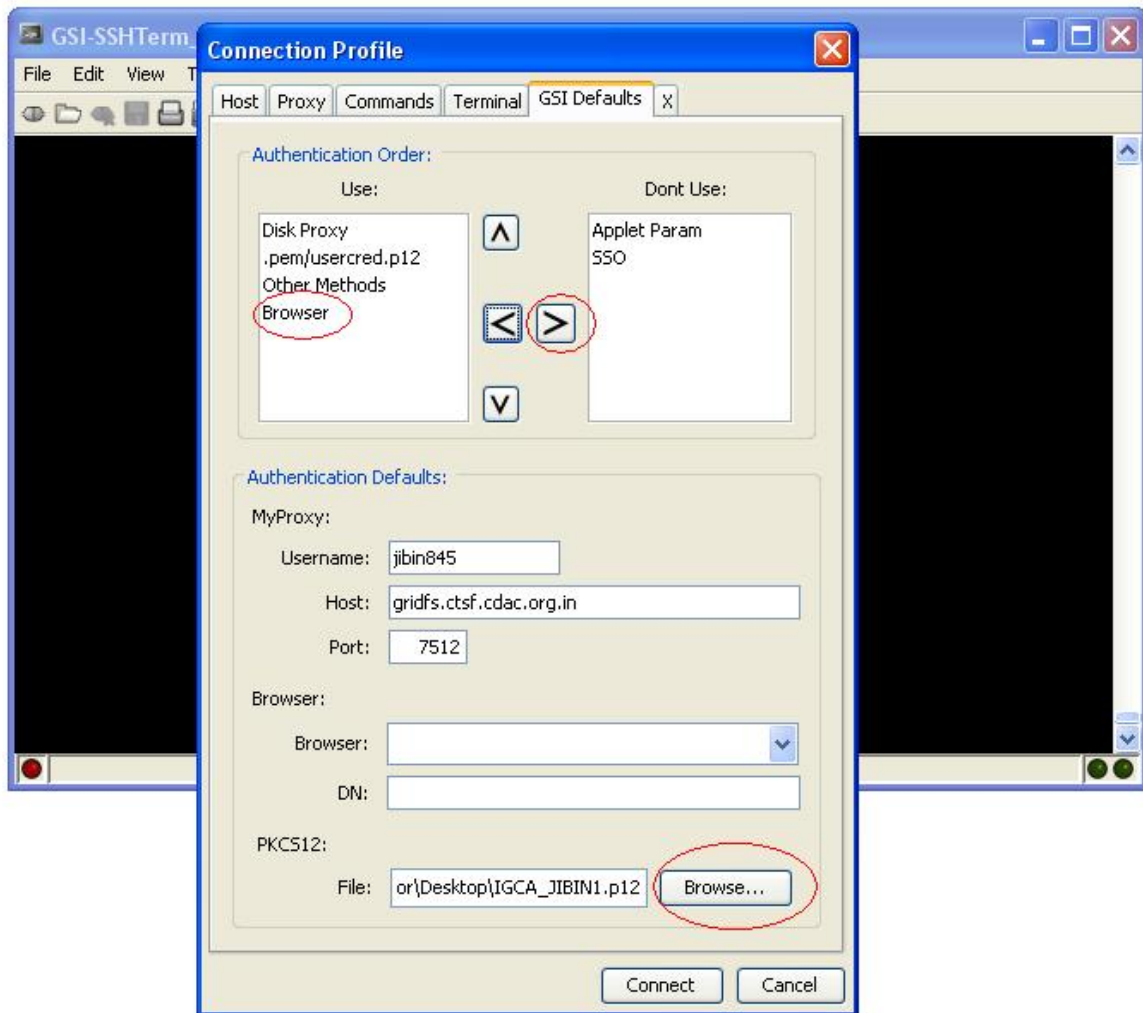


Step 5: In Host tab Enter your Garuda user name and leave other settings as it is. (See the below picture)



Step 6:

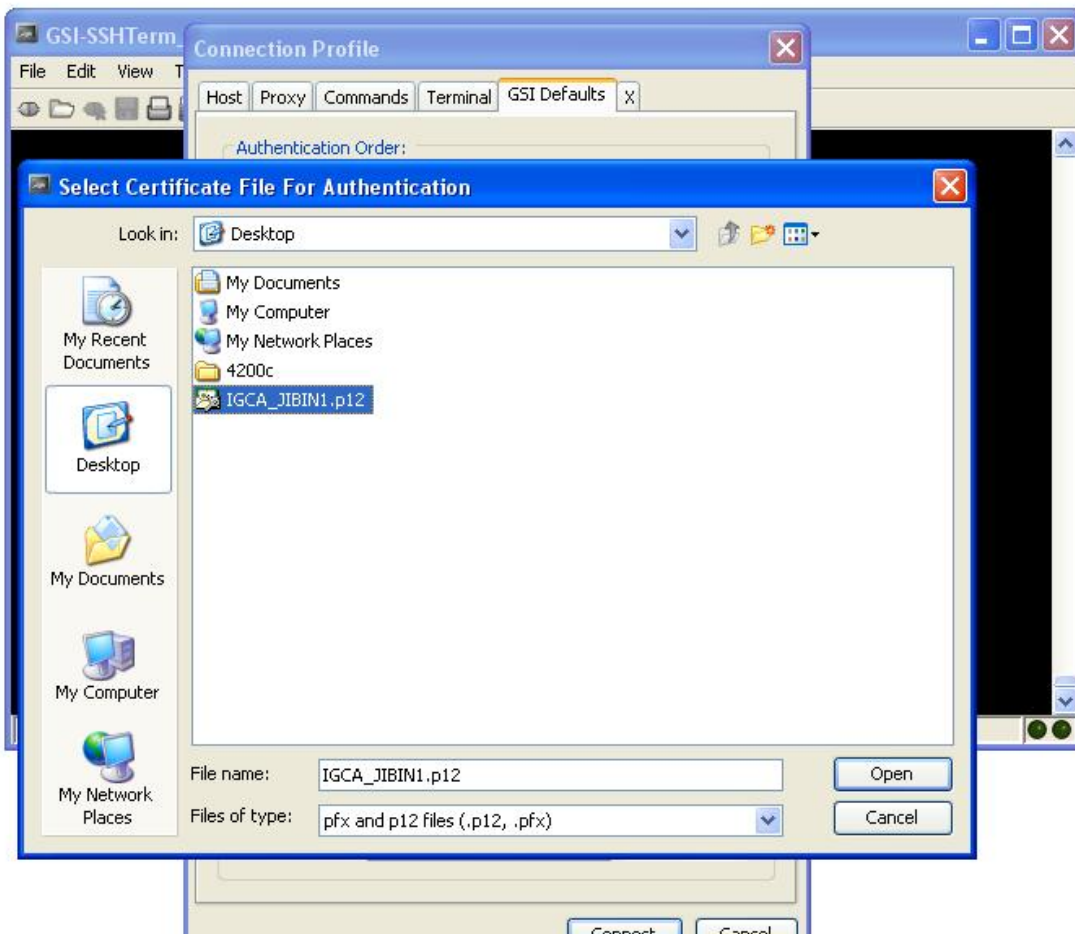
Go to GSI Defaults tab and select Browser from Authentication Order "Use" pane and place in "Dont Use" pane. Also in PKCS12 section click on Browse to Locate your IGCA certificate.



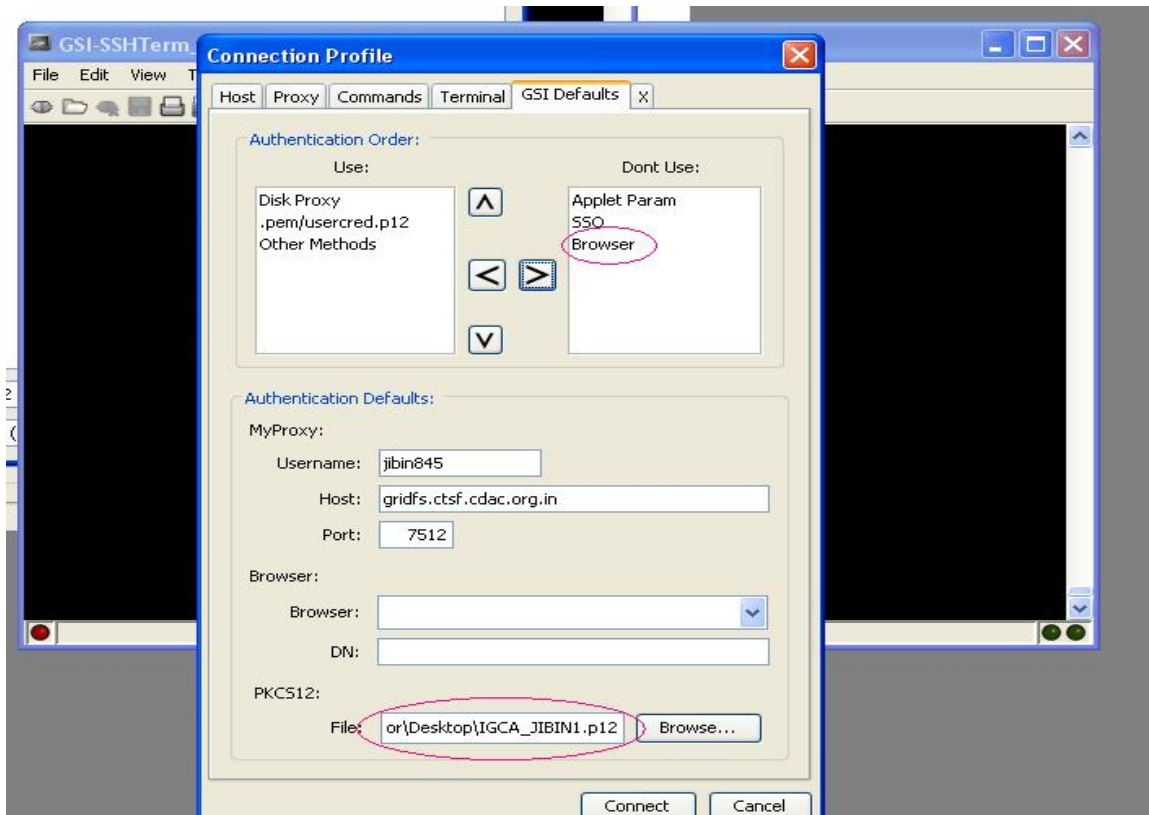
Step 7:

Go to the location where you have kept your IGCA certificate and click on it to Open.

Note: Follow the below guide to export your IGCA cert (.p12 or .PFX) from the browser, <http://ca.garudaindia.in/index.php/information/faq/export-the-certificates-obtain-pfxps12-file/>

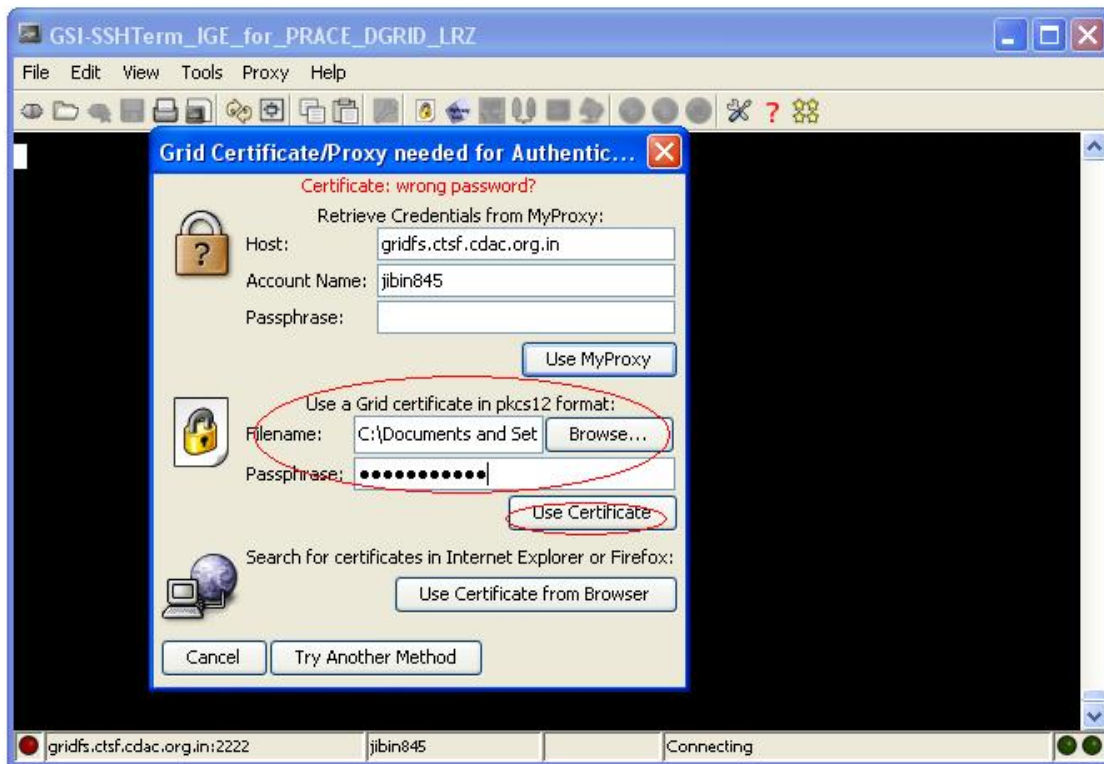


Step 8:
After the above two steps the window will look like the below picture. And click on "Connect".

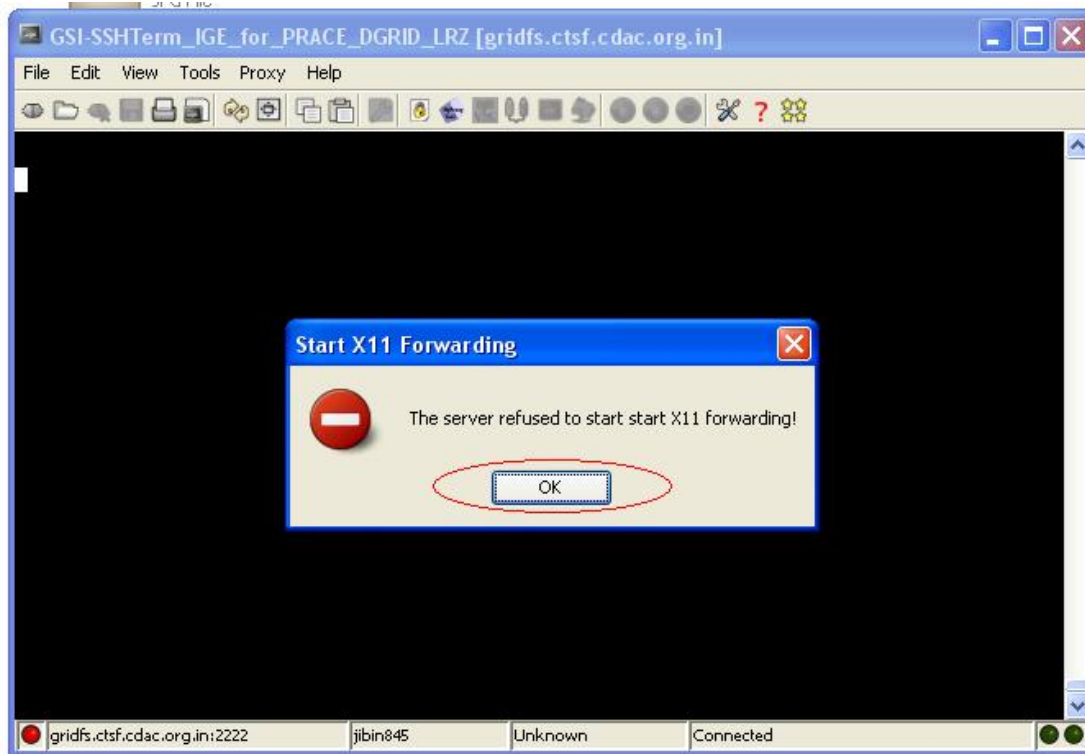


Step 9:

In the next window Enter your passphrase(password used while exporting the IGCA certificate from the browser) and Click on "Use Certificate".

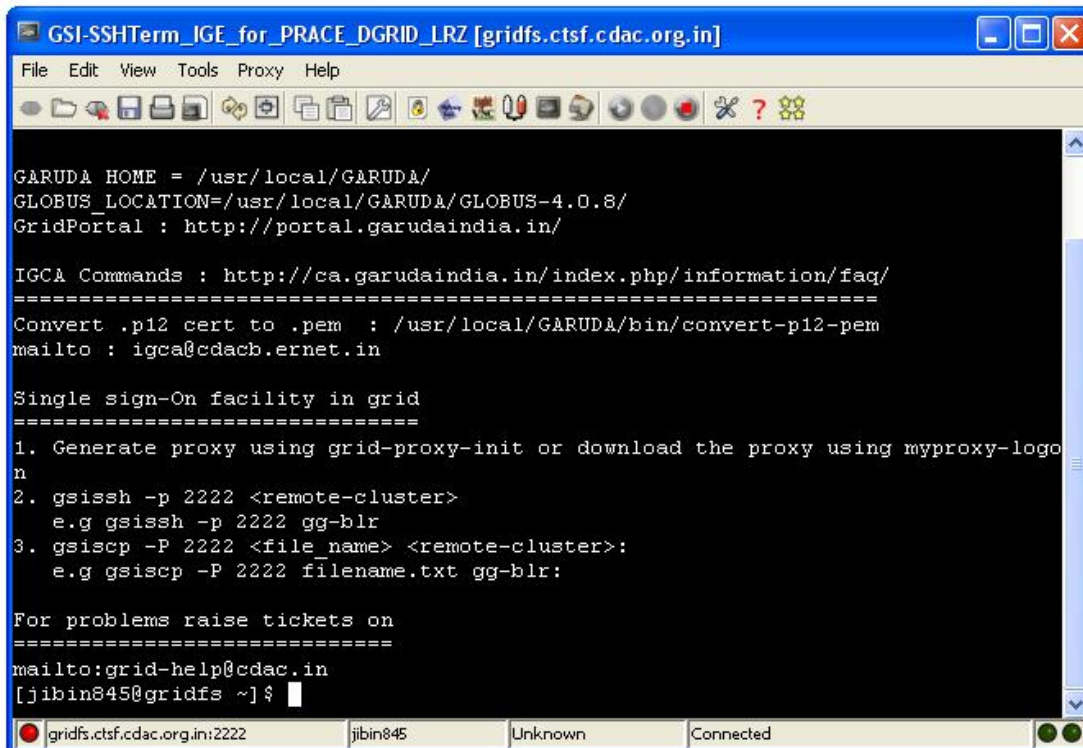


Step 10:
You will get a message like below ,Click on OK.



Step 11:

Now you are connected to Garuda Head machine and It look like the below picture.



NOTE:

While performing Step 9 if it not getting connected or if you see the following/similar error message window.



In this case, you need to install two additional jar files named `local_policy.jar` and `US_export_policy.jar`, from Sun (watch out: files with identical names but different content are already present on your local computer!). A copy of these files, providing a subset of the supported functionalities (only supporting up to 512 bit security, but not 1024 bit encryption), is already included in your local JDK and JRE. However, the complete version is not provided directly due to import control restrictions. To use a PKCS12 file, the complete version is necessary. Please kindly download the following two files and replace your local copies of these files with the new ones provided by the following links:

- ⤴ http://www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-java-plat-419418.html#jce_policy-1.5.0-oth-JPR (for JDK/JRE 1.5)

- ⤴ <http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html>(for JDK/JRE 1.6).
- ⤴ <http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>(for JDK/JRE 1.7)

Extract the two jar files and copy them to

- ⤴ `{JRE_installed_directory}/lib/security` if JRE is installed
- ⤴ `{JDK_installed_directory}/jre/lib/security` if JDK is installed