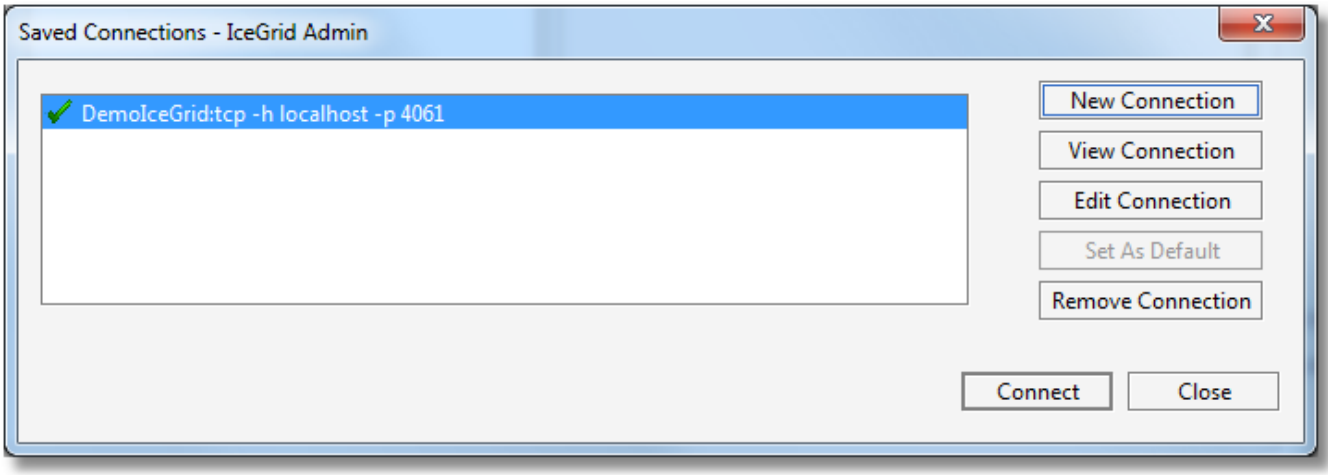
Connection to an IceGrid Registry

In order to administer or monitor an IceGrid deployment, you need to connect to the IceGrid registry of this deployment. If your IceGrid registry is replicated, you can connect to any replica for monitoring purposes; if you intend to change definitions, for example describe a new server, you need to connect to the master IceGrid registry. This page describes how to connect to an IceGrid registry.

On this page:

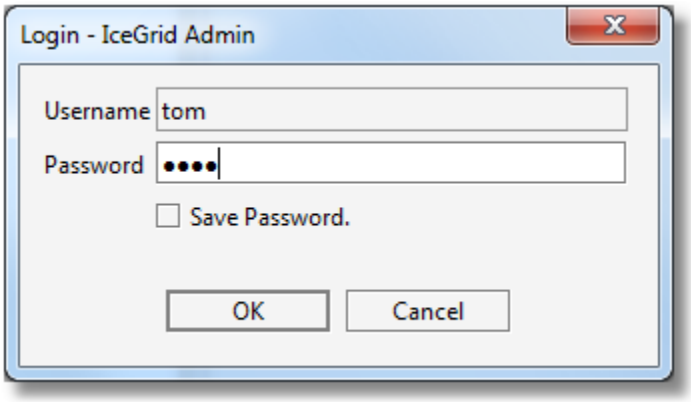
Connecting using a Saved Connection

Use `File > Login...` or press the  button to open the `Saved Connections` dialog:



Then double-click on the IceGrid registry you want to connect to, or select the IceGrid registry and click on the `Connect` button.

If the connection contains saved credentials, IceGrid Admin will immediately attempt to connect to the selected IceGrid registry with these credentials. Otherwise, it will open a new dialog to request the missing password (two passwords in some cases), such as:



Creating a new Connection

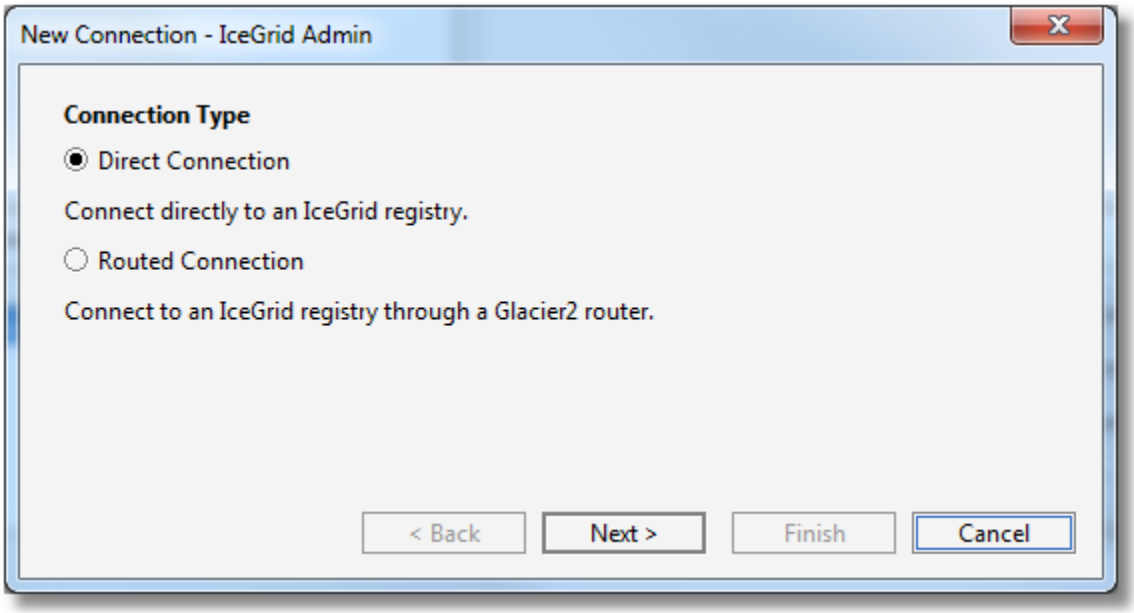
In the `Saved Connections` dialog, click on `New Connection` to open the New Connection wizard.

Below are 3 typical connections to illustrate the wizard steps:

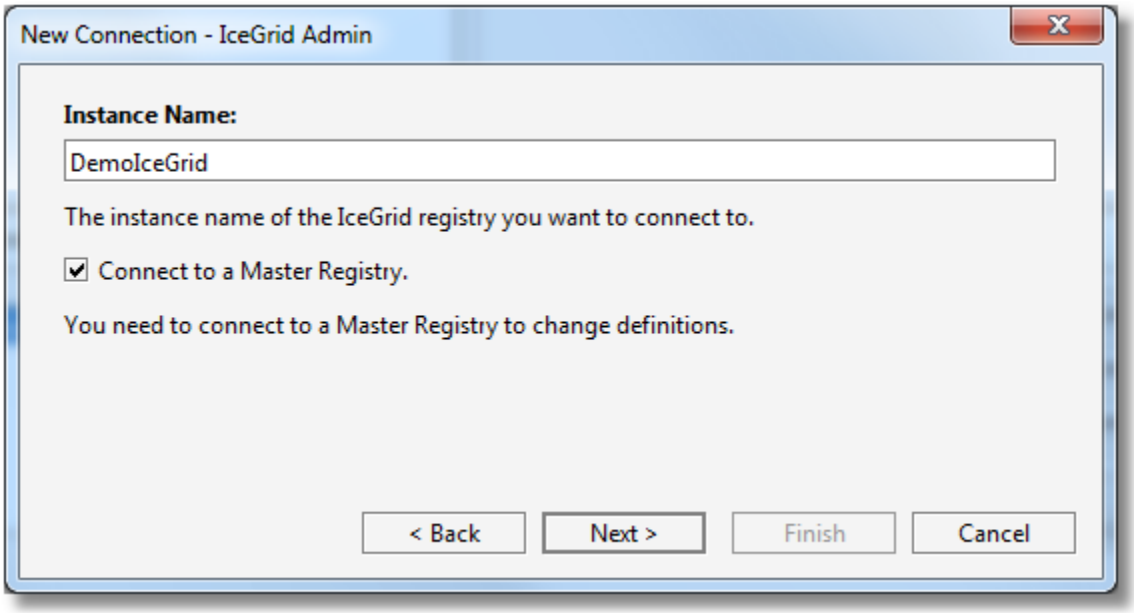
TCP Connection to a local IceGrid registry

We create a TCP connection to the IceGrid registry running on localhost:

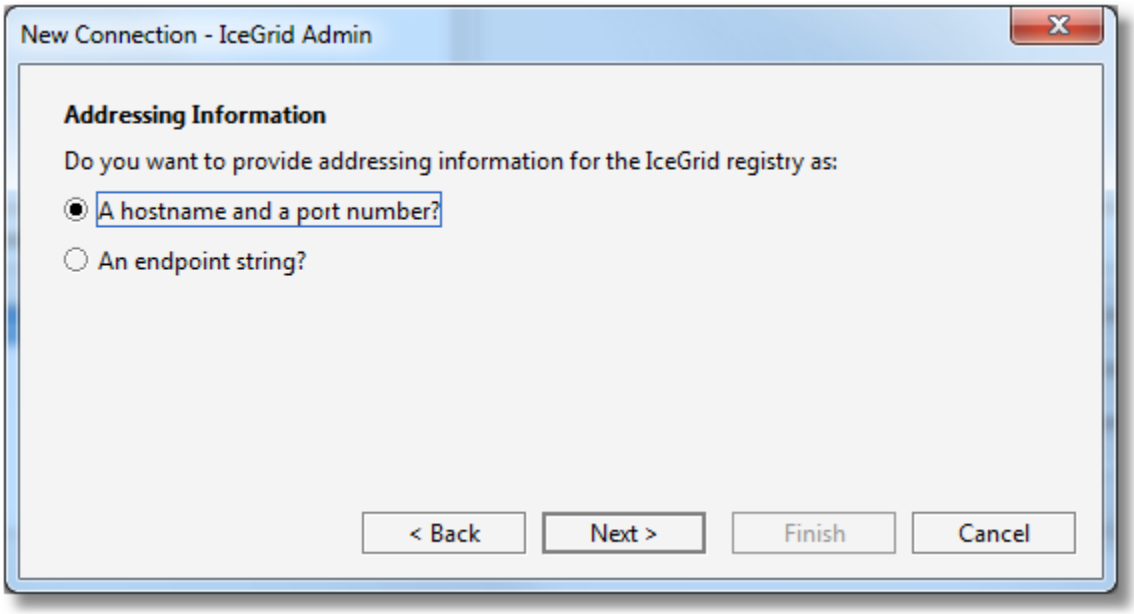
Step 1: we select Direct Connection



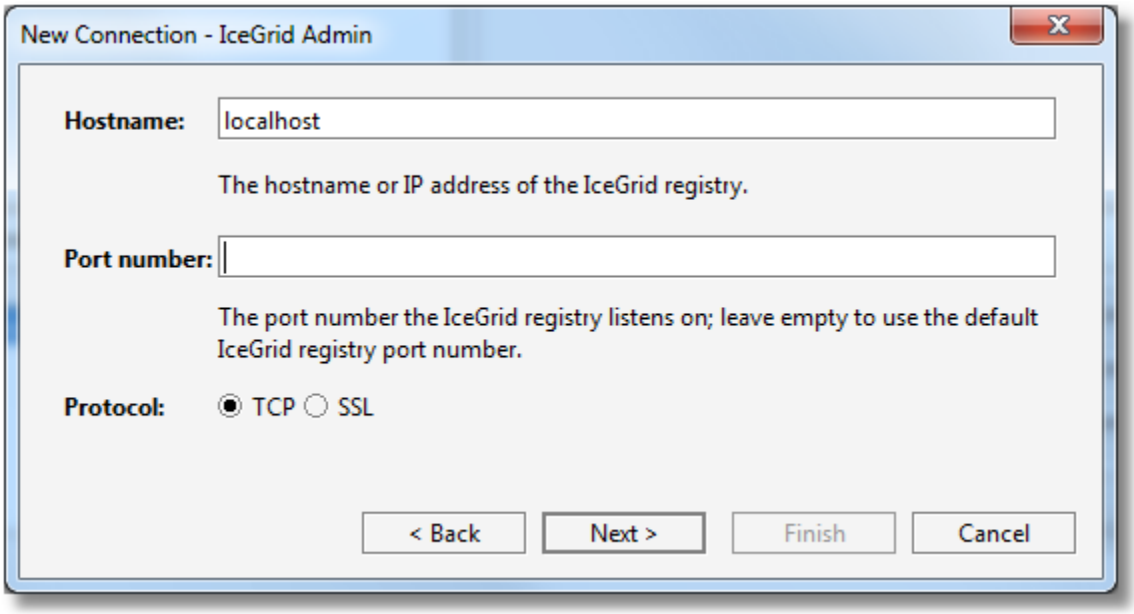
Step 2: we enter the name of your IceGrid instance. This corresponds to the `IceGrid.InstanceName` property in the target IceGrid registry configuration.



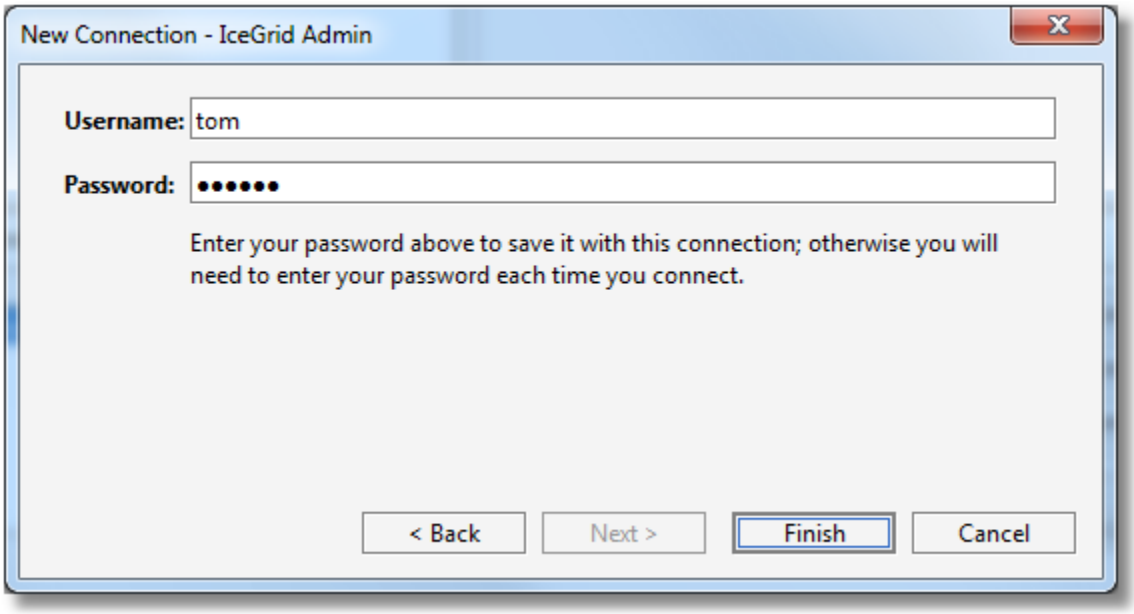
Step 3: we enter the addressing information as a hostname and port number



Step 4: we enter `localhost` for the Hostname, leave port number blank and keep TCP as the protocol



Step 5: we enter a username and password for this connection



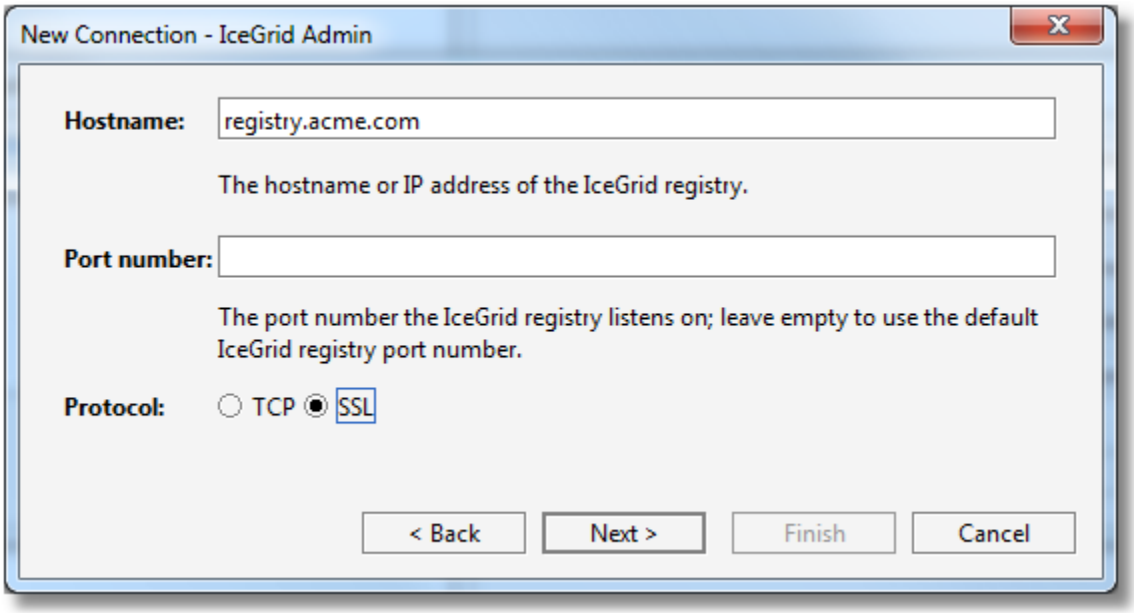
Step 6: we click on the `Finish` button to save the connection; IceGrid Admin then attempts to connect to the IceGrid registry

SSL Connection to local IceGrid using X.509 Credentials

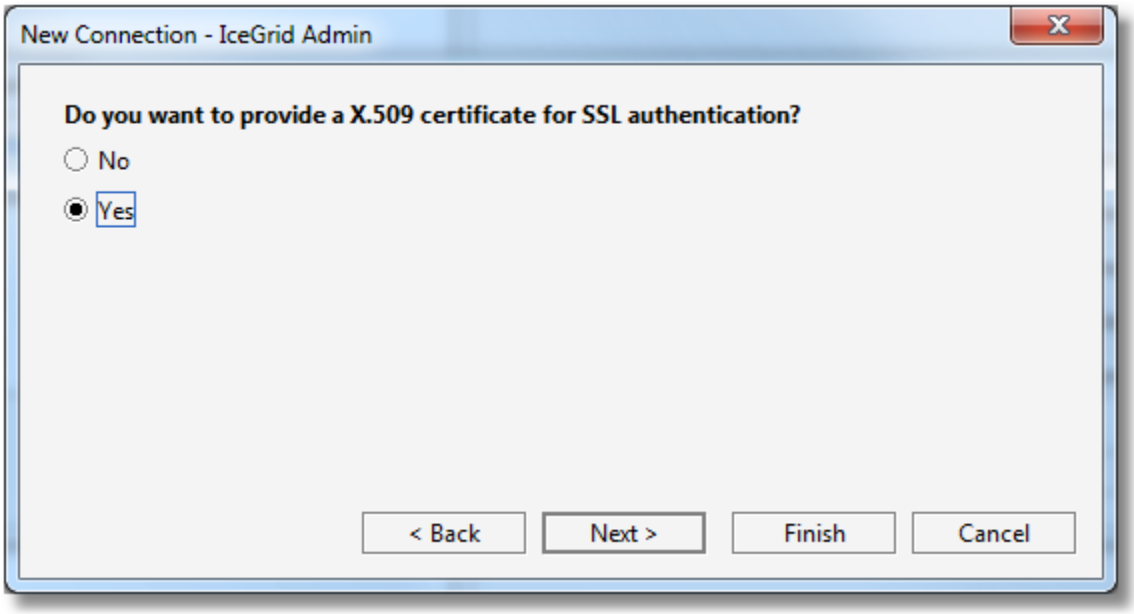
We create a SSL connection to a directly-reachable IceGrid registry, and authenticate with this IceGrid registry using our X.509 key (also used for SSL authentication). The target IceGrid registry must be configured to accept SSL connections and authentication using SSL credentials; see `IceGrid.Registry.AdminSSLPermissionsVerifier`.

Steps 1 to 3 are identical to the simple TCP connection described above.

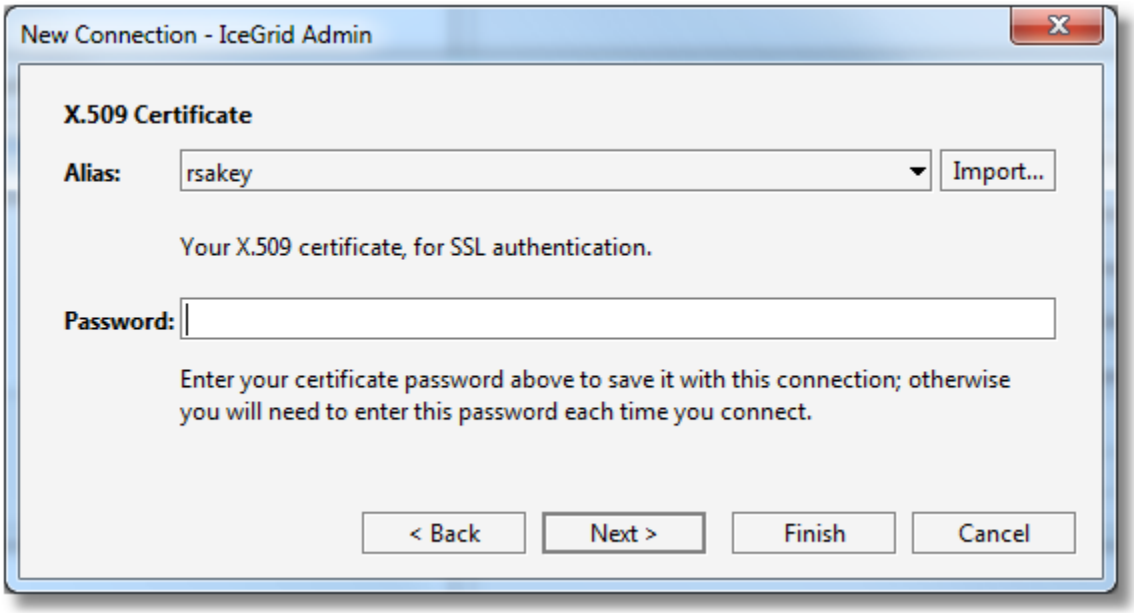
Step 4: we enter the hostname of the IceGrid registry, we leave the port number empty to use the default IceGrid port number (4061 for TCP and 4062 for SSL), and we select SSL for Protocol



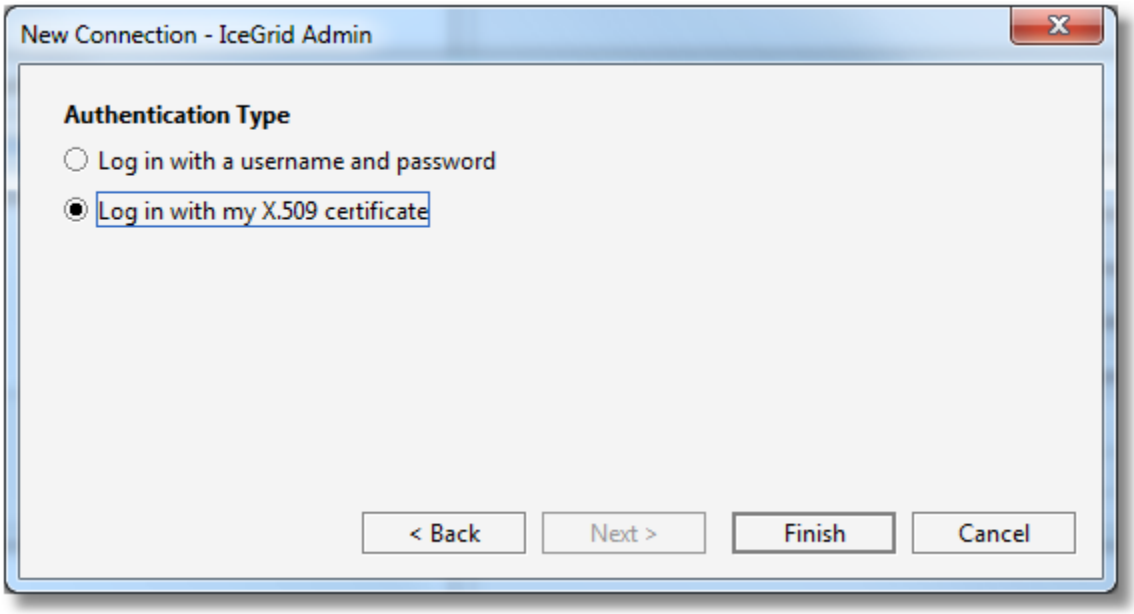
Step 5: yes, we want to provide a X.509 certificate for SSL authentication



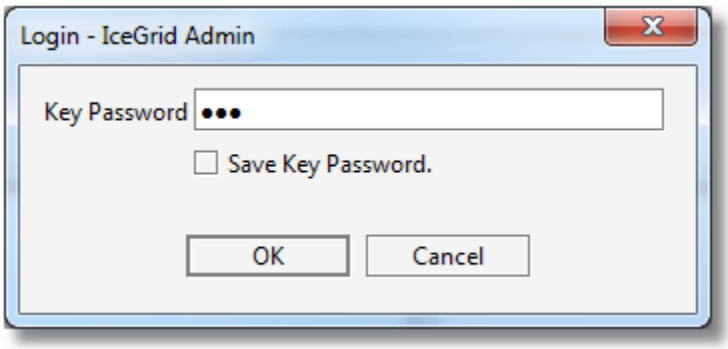
Step 6: we select the X.509 key used for SSL authentication from the Alias drop-down list; list this corresponds to the My Certificates set in the Certificate Manager described in the next section. Click on the `Import...` button to open the Certificate Manager dialog.



Step 7: we choose to use this X.509 certificate (carried through the SSL connection) to authenticate ourselves with the IceGrid registry.



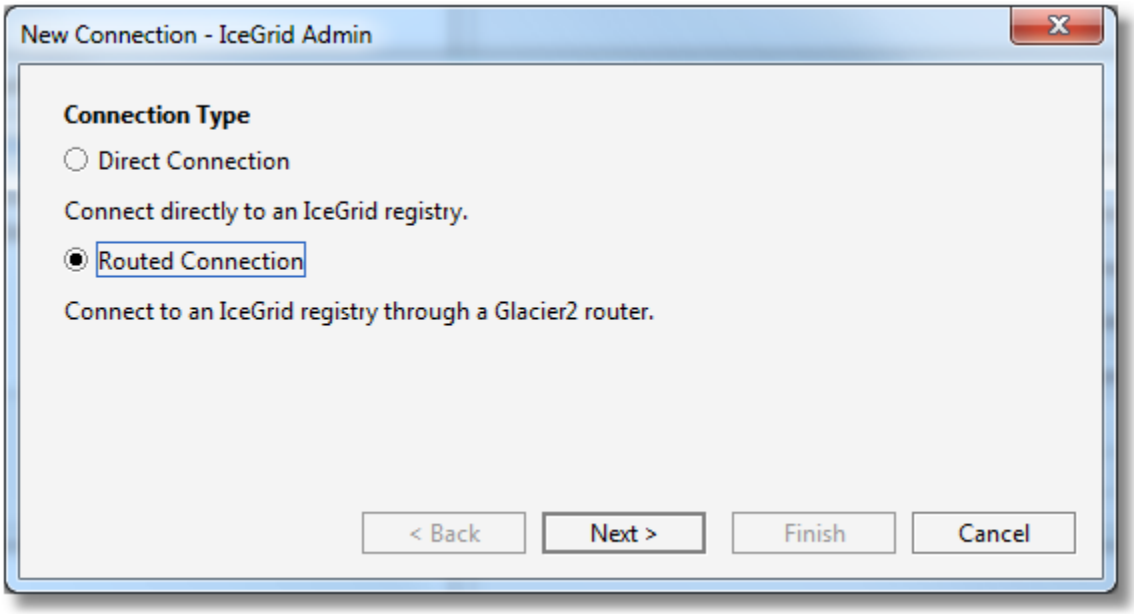
Step 8: we click on the `Finish` button to save the connection and connect to the IceGrid registry. Unless we entered (and therefore saved) the X.509 key password with the connection, we are prompted for this password:



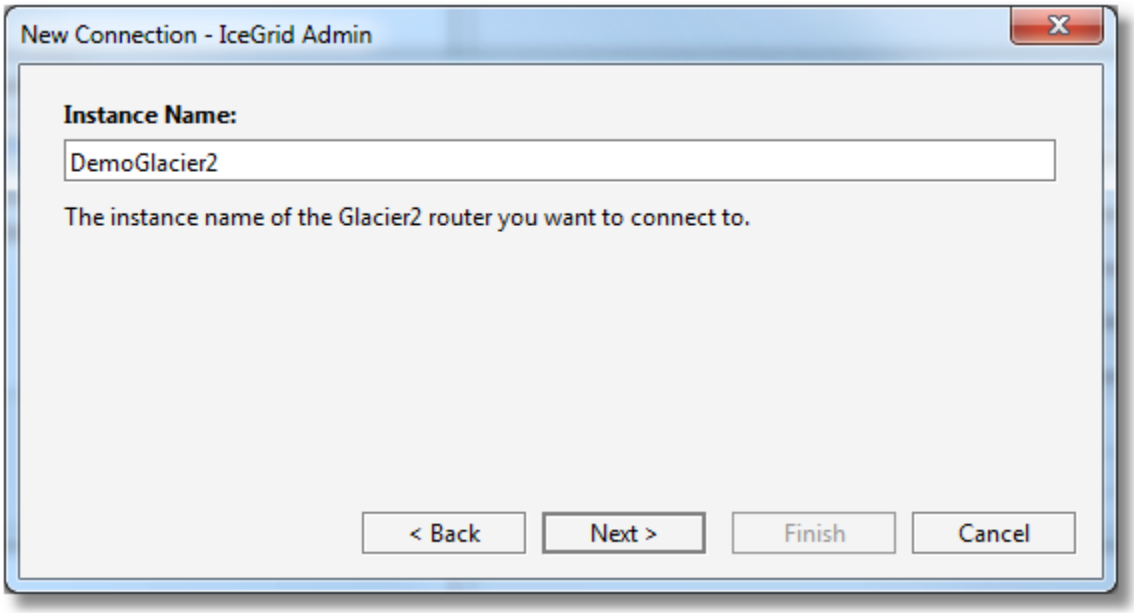
SSL Connection through Glacier2 router

We connect to an IceGrid registry "behind" a Glacier2 router. In this case, we need to connect to the Glacier2 router and authenticate ourselves with this Glacier2 router. We do not provide any information about the IceGrid registry itself: we will connect to the IceGrid registry identified by the target Glacier2 router configuration. See Glacier2 Integration with IceGrid.

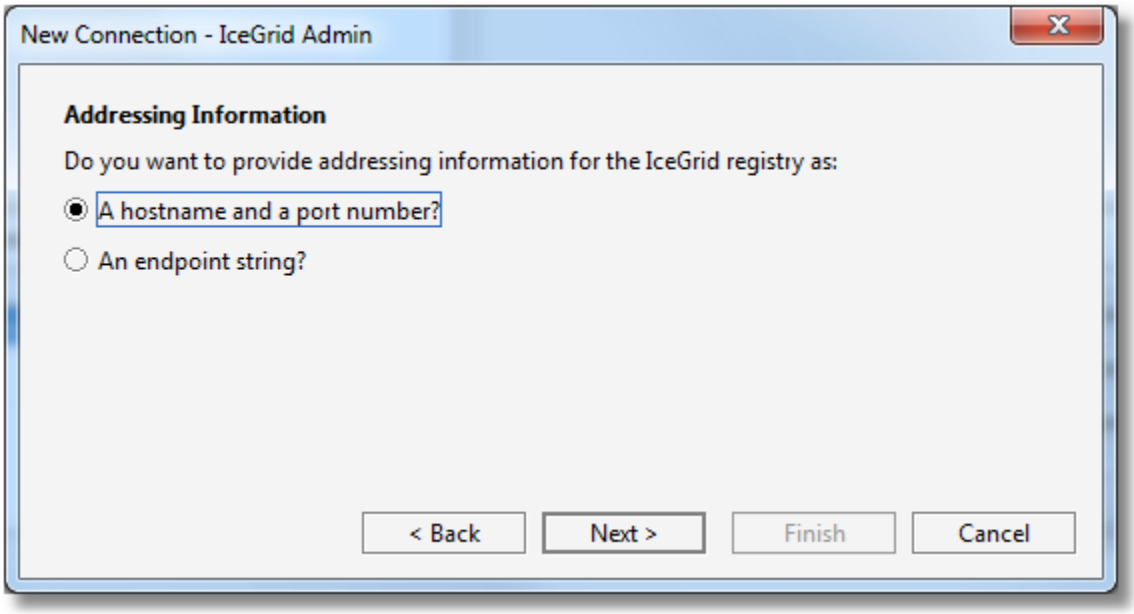
Step 1: we select Routed Connection



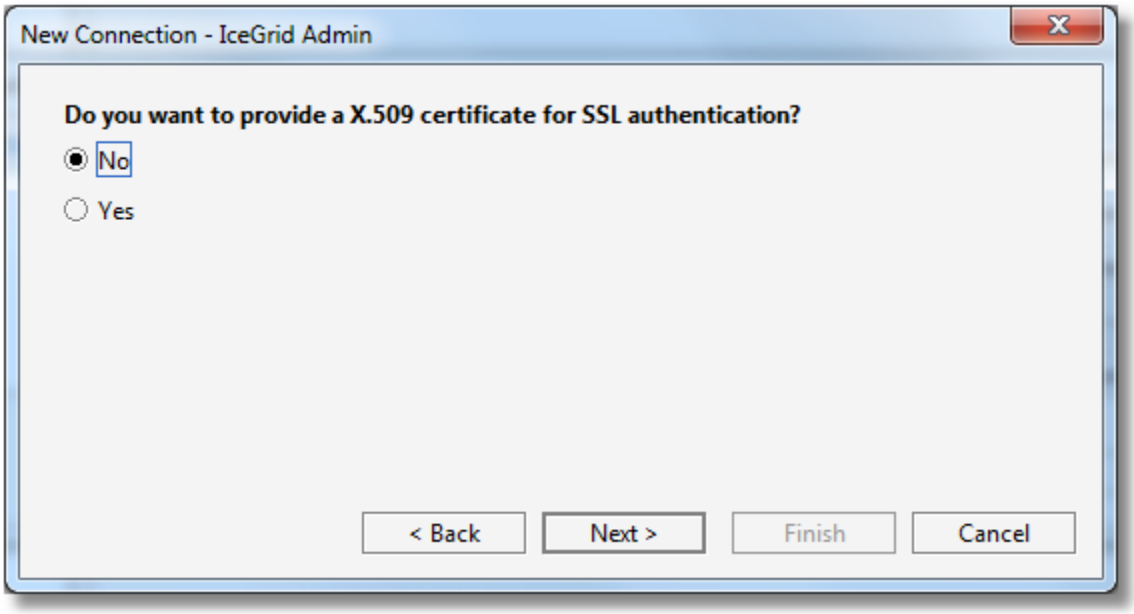
Step 2: we enter the instance name of our Glacier2 router. This corresponds to the `Glacier2.InstanceName` property in the target Glacier2 router configuration.



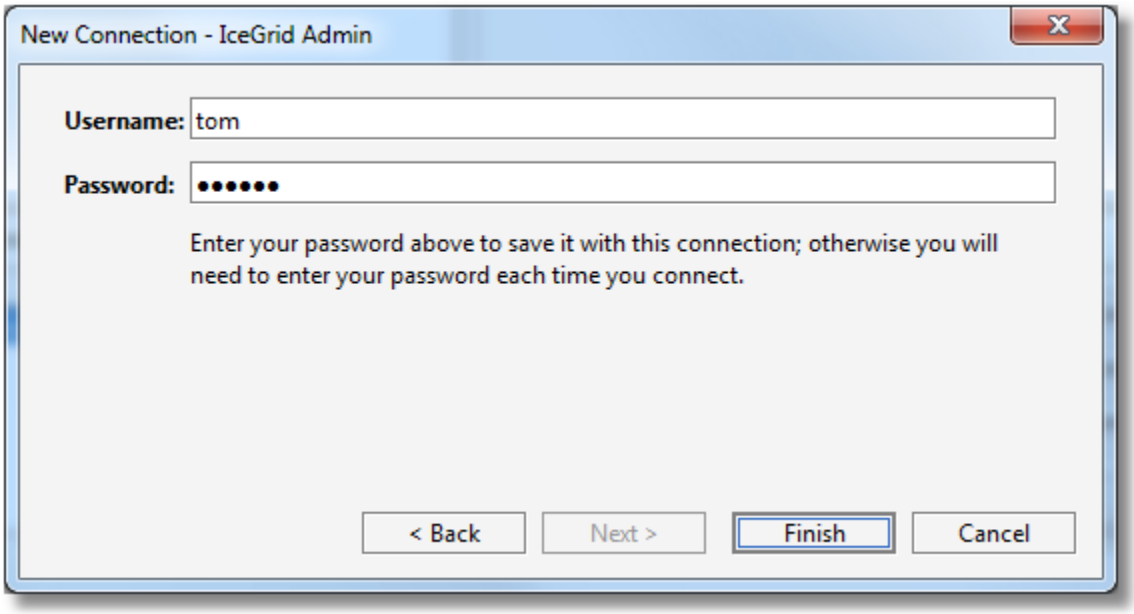
Step 3: we enter the addressing information for the target Glacier2 router as a hostname and port number



Step 4: we choose not to authenticate ourselves for SSL, so we do not provide a X.509 certificate.



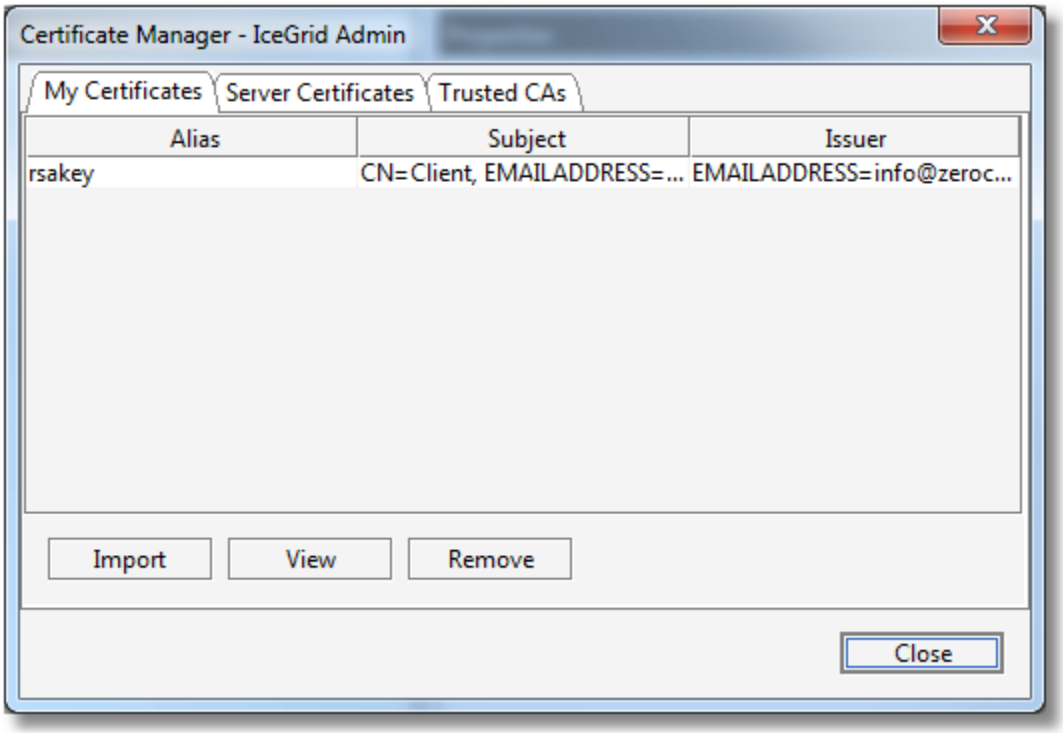
Step 5: we provide a username and password for the connection to the Glacier2 router



Step 6: we click on the `Finish` to save the connection; IceGrid Admin then attempts to connect to the IceGrid registry through the Glacier2 router.

SSL Connections and Certificates

IceGrid Admin maintains a persistent store of X.509 certificates for SSL connections with IceGrid registries. You can import, view and remove these certificates with the Certificate Manager. Use `File > Certificate Manager...` or click on the `Import...` button in the Connection wizard to open the Certificate Manager:



The Certificate Manager maintains 3 sets of certificates:

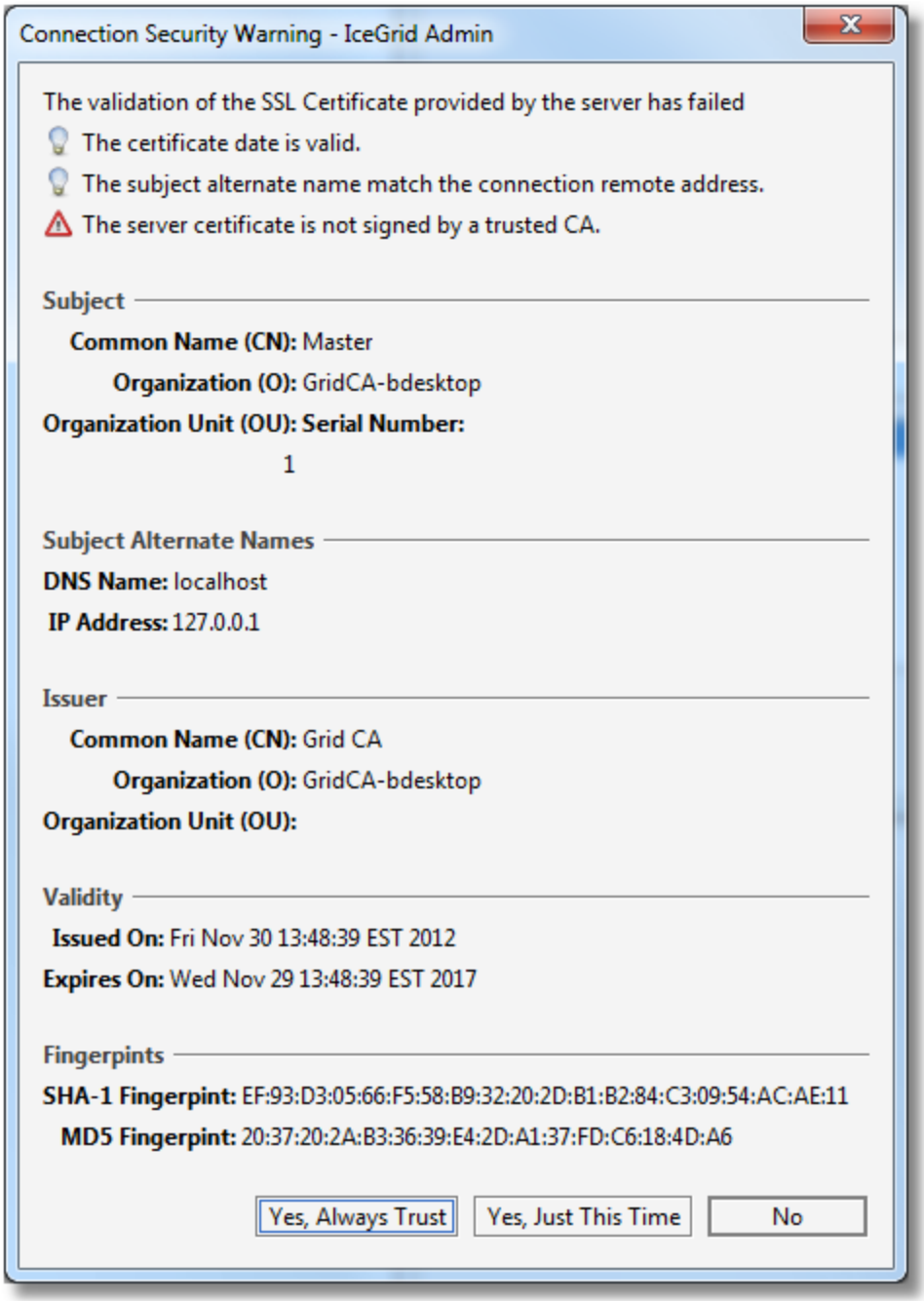
- **My Certificates**
  These certificates are used to authenticate IceGrid Admin when establishing a SSL connection with an IceGrid registry or Glacier2 router (this first authentication is at the SSL level); once the SSL connection is established, this certificate can also be used to authenticate with the target IceGrid registry or Glacier router (at the application level).

- **Server Certificates**
  The certificates of IceGrid registries and Glacier2 routers that IceGrid Admin trusts when establishing a SSL connection. All certificates signed by a Trusted CA (see below) are automatically trusted and usually do not need to be imported in this set.

- **Trusted CAs**
  The certificates of Certificate Authorities.

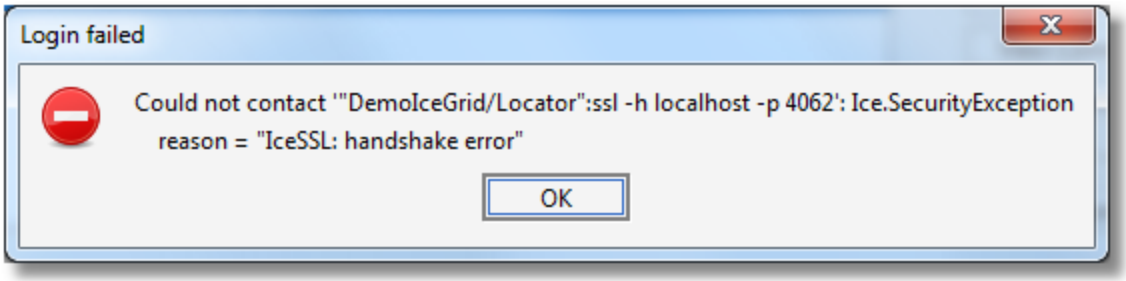
You do not need to import server certificates or CA certificates prior to establishing a SSL connection with an IceGrid registry or Glacier2 router. IceGrid Admin performs the following checks when establishing a SSL connection:

- If the X.509 certificate presented by the IceGrid registry or Glacier2 router matches a Server Certificate, proceed
- Otherwise, if this certificate is signed by a trusted CA, is valid (*now* is within the certificates validity period) and its alternate name is a match for the SSL connection remote address, proceed
- Otherwise, display a Connection Security Warning dialog similar to the dialog below to let you decide whether or not to proceed with this certificate:



If you select `Yes, Always Trust`, the certificate is added in the persistent Server Certificates set.

A "client" X.509 certificate (saved in My Certificates) is only necessary when the target IceGrid registry or Glacier2 router requires one. This depends on the setting of the `IceSSL.VerifyPeer` property in those servers: when `IceSSL.VerifyPeer` is 2, IceGrid Admin must provide a valid certificate. If you forget to provide a certificate, or provide an invalid certificate, the connection establishment will fail with an IceSSL error comparable to the following:



Editing a Saved Connection

In the `Saved Connections` dialog, click on `Edit Connection` to edit a connection. This opens the Connection wizard for your saved connection. With this wizard, IceGrid Admin does not attempt to connect to the target IceGrid registry when you click on the `Finish` button.

Closing a Connection

Use `File > Logout` or press the  button to disconnect from an IceGrid registry. This clears all information in the Live Deployment pane.