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
- Creating a new Connection

 - TCP Connection to a local IceGrid registry
 SSL Connection to local IceGrid using X.509 Credentials
 - SSL Connection through Glacier2 router
- SSL Connections and Certificates
- Editing a Saved Connection
- Closing a Connection

Connecting using a Saved Connection

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

Saved Connections - IceGrid Admin	×
DemoIceGrid:tcp -h localhost -p 4061	New Connection
	View Connection
	Edit Connection
	Set As Default
	Remove Connection
Connect Close	

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:

Login - IceGr	id Admin
Username	tom
Password	••••
	Save Password.
	OK Cancel

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

New Connection - IceGrid Admin	×
Connection Type	
Direct Connection	
Connect directly to an IceGrid regist	y.
O Routed Connection	
Connect to an IceGrid registry throug	gh a Glacier2 router.
< B	ack Next > Finish Cancel

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

New Connection - IceGrid Admin
Instance Name:
DemoIceGrid
The instance name of the IceGrid registry you want to connect to.
Connect to a Master Registry.
You need to connect to a Master Registry to change definitions.
< Back Next > Finish Cancel

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

New Connection - IceGrid Admin		×
Addressing Information		
Do you want to provide addressing i	information for the IceGrid registry as:	
A hostname and a port number?		
O An endpoint string?		
< B	ack Next > Finish Cancel	

Step 4: we enter <code>localhost</code> for the Hostname, leave port number blank and keep TCP as the protocol

New Connection	- IceGrid Admin
Hostname:	localhost
Port number	The hostname or IP address of the IceGrid registry. The port number the IceGrid registry listens on; leave empty to use the default IceGrid registry port number.
Protocol:	● TCP ○ SSL < Back Next > Finish Cancel

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

New Connectio	n - IceGrid Admin	×	
Username:	tom		
Password:	•••••		
	Enter your password above to save it with this connection; otherwise you will need to enter your password each time you connect.		
	< Back Next > Finish Canc	el	

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 lceGrid registry, and authenticate with this lceGrid registry using our X.509 key (also used for SSL authentication). The target lceGrid 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

New Connection -	IceGrid Admin	
Hostname:	registry.acme.com	
Port number:	The hostname or IP address of the IceGrid registry. The port number the IceGrid registry listens on; leave empty to use the default IceGrid registry port number.	
Protocol:		
	< Back Next > Finish Cancel	

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

New Connection - IceGrid Admin	×		
Do you want to provide a X 509 certificate for SSL authentication?			
⊖ No			
Yes			
< Back Next > Finish Ca	ancel		

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.

New Connect	tion - IceGrid Admin			
X.509 Ce	rtificate			
Alias:	rsakey 👻 Import			
	Your X.509 certificate, for SSL authentication.			
Password	d:			
	Enter your certificate password above to save it with this connection; otherwise you will need to enter this password each time you connect.			
	< Back Next > Finish Cancel			

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

New Connection - IceGrid Admin		x
Authentication Type		
 Log in with a username and pass 	ssword	
Log in with my X.509 certificate		
	Park Nath	
< B	Back IVext > Finish Cancel	

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:

ogin - IceGrid Admin	
Key Password	
Save Key Password.	
OK Cancel	

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

New Connection - IceGrid Admin	×	
Connection Type		
 Direct Connection 		
Connect directly to an IceGrid regist	ıy.	
Routed Connection		
Connect to an IceGrid registry throu	gh a Glacier2 router.	
< B	Back Next > Finish Cancel	

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

lew Connection - IceGrid A	dmin	×
Instance Name:		
DemoGlacier2		
The instance name of th	e Glacier2 router you want to connect to.	
	< Back Next > Fin	ish Cancel

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

New Connection - IceGrid Admin	x
Addressing Information	
Do you want to provide addressing information for the IceGrid registry as:	
A hostname and a port number?	
O An endpoint string?	
< Back Next > Finish Cancel	

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

New Connection - IceGrid Admin	x
Do you want to provide a X-509 certificate for SSL authentication?	
 No 	
⊖ Yes	
< Back Next > Finish	Cancel

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

New Connection	n - IceGrid Admin	Ŋ
Username:	tom	
Password:	•••••	
	Enter your password above to save it with this connection; otherwise you will need to enter your password each time you connect.	
		1
	< Back Next > Finish Cancel	
		J

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:

Certificate Manager - IceGrid A	dmin	—X —
My Certificates Server Certif	icates (Trusted CAs)	
Alias	Subject	Issuer
rsakey	CN=Client, EMAILADDRESS=	EMAILADDRESS=info@zeroc
Import View	Remove	
		Close

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:

Connection Security Warning - IceGrid Admin
The validation of the SSL Certificate provided by the server has failed
The certificate date is valid.
The subject alternate name match the connection remote address.
▲ The server certificate is not signed by a trusted CA.
Subject
Common Name (CN): Master
Organization (O): GridCA-bdesktop
Organization Unit (OU): Serial Number:
1
Subject Alternate Namer
DNS Namer localhort
IP Address: 127.0.0.1
IF Address. 127.0.0.1
Issuer
Common Name (CN): Grid CA
Organization (O): GridCA-bdesktop
Organization Unit (OU):
Validity
Issued On: Fri Nov 30 13:48:39 EST 2012
Expires On: Wed Nov 29 13:48:39 EST 2017
Fingerpints
SHA-1 Fingerpint: EF:93:D3:05:66:F5:58:B9:32:20:2D:B1:B2:84:C3:09:54:AC:AE:11
MD5 Fingerpint: 20:37:20:2A:B3:36:39:E4:2D:A1:37:FD:C6:18:4D:A6
Yes, Always Trust Yes, Just This Time No

If you select ${\tt Yes}$, ${\tt Always}$ ${\tt Trust},$ 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 lceGrid registry or Glacier2 router requires one. This depends on the setting of the lceSsL.VerifyPeer property in those servers: when lceSsL.VerifyPeer is 2, lceGrid 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 lceSsL error comparable to the following:

Login fail	led
	Could not contact "DemoIceGrid/Locator":ssl -h localhost -p 4062': Ice.SecurityException reason = "IceSSL: handshake error"
	ОК

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.