# Security and JCAT

JCAT is a Java based software platform. Using Java addresses many basic application security concerns protecting both the user's computer environment and JCAT itself. For more information on the security that the Java Software Environment offers see: http://java.sun.com/docs/books/tutorial/security/index.html. Network security is also a concern as JCAT also offers scalable remote user collaboration between instances of JCAT running on any operating system that supports the JRE version currently used by JCAT. These collaboration sessions are SSL encrypted and offer other security features as described below. The user may obtain version information for JCAT as well as the Java Runtime in use by the system by accessing the “About” dialog in the Help menu at the top of the application.

### Ports and the Security Dialog

JCAT allows the user to change the port numbers that JCAT will use for collaborating. By default the port is set to 1098, and collaboration is functional right out of the box. Note that a collaboration session will also use one port higher and one port lower then what is specified by the user. Thus if 1098 is specified then ports 1097, 1098 and 1099 will be used when collaboration is active. In order to change port settings, the administrator must use the Security Settings dialog accessible through the Tools menu. In order to access the security dialog for the first time, the default pass phrase (primate) may be used. Once the user has access to the dialog, the pass phrase may be changed. There is no limit on character length or number of words but the pass phrase is case-sensitive. Many computer systems are protected by hardware firewalls and/or routers and in such a case these devices must be configured to allow the ports selected for collaboration. Some computers also have firewalls and spyware protection software installed. These applications may require special configuration as well. Windows firewall which is packaged with Windows XP is an example of this type of software.

### Access Files

There are two files in the *<JCAT_HOME>/resources/config* directory: they are *access.jc* and *prime.jc*. Both of these encrypted files must be present for collaboration to work properly, if these files are damaged or deleted, the administrator should retain a backup copy of the default files shipped with the tool. Once the administrator replaces the missing or corrupted access files with backup files, the user may access the security dialog using the default pass phrase.

**Encryption and Authentication**

As of JCAT version 1.1, collaboration sessions are fully encrypted. Three files inside the config directory mentioned above are now required for collaboration to negotiate a secure connection. These files include a security certificate created and self signed by the JCAT team, a key-store file and a trust-store file. Collaboration uses 128bit RC4 SSL encryption with RSA cryptography and MD5 hashing to ensure data integrity.

There are also several options for enabling authentication by users to the collaboration session. Currently you can enable one of three types of authentication for users connecting to your hosted session: 1.) You may use session password authentication in which you specify a single password for your session that every user will use to authenticate. 2.) User list authentication allows you to configure a unique username and password for each user connecting. 3.) IP Address authentication allows you to configure a list of IP addresses which you will allow to connect to your session. This type requires you to know or get this information from clients before starting a session. When one of these types of authentication is enabled, users are required to enter proper information or are otherwise denied access to your collaboration session.