

Phone: +1-770-738-2101 Option 5

E-mail: icehelpdesk@theice.com

ICE CHAT FREQUENTLY ASKED TECHNICAL QUESTIONS

FREQUENTLY ASKED QUESTIONS

PASSWORDS

- ✦ **Are passwords assigned to users? Can they change them?**
 - Yes, random passwords are assigned to users and they can change them.
- How are passwords stored remotely (i.e., in encrypted form on a protected resource)?**
 - Passwords are SHA hashed (similar to encryption) and stored in a secure directory.
- ✦ **How are passwords stored remotely (i.e., in encrypted form on a protected resource)?**
 - Passwords are SHA hashed (similar to encryption) and stored in a secure directory.
- ✦ **Are there any minimum password requirements?**
 1. Passwords must be between 7 to 14 characters in length.
 2. Passwords must include at least 3 of the following types:
 - lowercase,
 - uppercase,
 - numbers,
 - special characters

Special characters allowed are:
` ~ ! @ # \$ % ^ & * () - _ = + [{] } \ | ; : ' " , < . > / ? ÿ ½

LOGGING IN AND AUTHORIZATION

- ✦ **Do accounts lock out after a certain number of failed attempts?**
 - Yes. Accounts are locked after ten (10) consecutive failed attempts.
- ✦ **Are there measures to ensure that a user can only log in from a particular IP address or range of addresses (i.e., Joe can only log in from a particular machine(s))?**
 - Yes, this can be configured.
- ✦ **Are authorization credentials cached (i.e., stored in cookies)? If so, how long are they valid for?**
 - Yes, they are cached for the life of the session and expire upon logout.

ENCRYPTION AND INFORMATION INTEGRITY

- ✦ **Is traffic sent to/from client machines encrypted? If so, what encryption scheme/algorithms are used?**
 - 128-bit or stronger encryption is used to authenticate and encrypt all communication between client applications and our servers. Encryption prevents potential malicious third parties from intercepting sensitive data and credentials in transmission. The controls inherent to SSL and TCP provide additional integrity to ensure content is not tampered with by a third-party during transmission.

TRADE EXECUTION

- ✦ **Can ICE Chat be utilized to execute trades?**
 - In the default configuration, ICE Chat cannot be used to execute trades.
 - Some versions of ICE Chat can be used to block in ICE cleared trades.
 - Some versions of ICE Chat can be used to connect to ICE and execute trades on the ICE trading platform. Users with this version will need a WebICE ID that is specifically permissioned and approved by your ICE Admin for access.

CONNECTIONS/INTERNET

- ✦ **Does ICE Chat utilize the Internet?**
 - Yes
- ✦ **What does the communication dialogue look like? Are connections initiated inbound or outbound or both? On which ports?**
 - ICE Chat always initiates and creates a HTTPS session on port 443 to the system with x.509 certificate.

Are documents of destination IP servers and ports to which clients will connect (if servers are hosted remotely) available?

- Clients connect to the following addresses:
yj.theice.com (63.247.112.159) via port 443
yjstreaming.theice.com (63.247.112.158) via port 443

DATA STORAGE

- ✦ **Is there any data stored remotely that may give away proprietary information or techniques? If so, what kind of data is stored remotely? How is that data secured?**
 - Only bid and offer indications are stored in the operational database. No other proprietary information or techniques are stored remotely. The system provides authentication and authorization. The database is secured from remote access except from designated administration IPs.

SERVERS AND AVAILABILITY

- ✦ **Can ICE CHAT be run from a terminal server or Citrix server?**
 - Yes.
- ✦ **Does ICE CHAT function with a proxy server?**
 - Yes.
- ✦ **Does ICE CHAT have a high availability component?**
 - Yes. The hardware is hosted at ICE's primary datacenter which has an excellent network infrastructure and SLA backed peering relationships with other backbone providers. The hardware is clustered, allowing the system to continue operation even after the failure of multiple nodes. Additionally, we maintain a full disaster recover site from a physically separate location.

COMPLIANCE MONITORING

- ✦ **What mechanism does ICE Chat have for compliance monitoring?**
 - All indicative information (bid/offer indications, messages) is logged and accessible through ICE CHAT(for short term log retrieval) or the ICE Chat client area (for retrieval of all logs). Administrators can also be granted access to monitor logs in real time. Optionally, logs may be sent to 3rd party content archiving systems, generally on an inter-day basis on the client's request.

UPGRADING

- ✦ **How is ICE CHAT upgraded? Is re-installation required?**
 - ICE CHAT is automatically upgraded over the internet. No user intervention is required.
 -

WINDOWS REGISTRY

- ✦ **Does ICE CHAT modify the Windows Registry?**
 - No, ICE CHAT makes no changes to the registry and does not alter or create any new files in the Windows System directory.

SUPPORT

- ✦ **Is Support provided?**
 - Yes, phone, IM and electronic support are provided during standard New York, Singapore and London trading hours.

SECURITY AND STABILITY OVERVIEW

PHYSICAL

- Servers are hosted at ICE's primary datacenter. ICE uses Windows and UNIX systems. All systems follow build standards to ensure standardization and security. The Information Security group monitors, assigns, and tracks patch status to respond to vendor operating system or application alerts.

SYSTEM:

- Operational system on RedHat Enterprise Linux and Solaris.
- System employs clustering architecture to ensure high availability and seamless failover in the event of a hardware failure
- Data is replicated on multiple servers and archived nightly to multiple physical locations

NETWORK:

- ICE uses a 3-tier network architecture with two layers of firewalls between customers and ICE databases. Customer connections are routed to application servers via high-performance load balancers. Application servers handle encryption, user-authentication, and market routing and pass data through the second firewall tier to data servers and databases. Intrusion Detection Systems at production and office facilities monitor network traffic against industry-standard and ICE customized network activity signatures.
- External screening routers employ access control lists to terminate virus, worm, and common hacking attempts before they reach external ICE firewalls. Firewalls further parse traffic to ensure only specifically permitted sources can reach specific destinations and services. VPN or private line connections terminate outside external firewalls, but independently from Internet connection points.

APPLICATION:

- Access to the application controlled by password authentication over secure TCP/HTTPS (128 bit encrypted)
- Authorization done by server based on request and authentication credentials
- System requirements: Windows 2000 or greater and .NET Framework 3.5 (provided with installer)

Testing and Audit

- ICE conducts regular internal penetration testing and auditing to determine compliance with written policies and measure vulnerability. In addition, a third-party external penetration test is performed annually. The results of this test are used internally to verify internal audit processes and controls. An exhaustive SAS70 Type II audit is performed annually to produce independent verification and testing of ICE controls for external parties and auditors that rely on ICE. This scope of this report is evaluated each year and tailored in response to customer feedback and business developments. The report covers a 6-month test period.

MORE INFORMATION OR QUESTIONS

For additional information or questions regarding ICE Chat's compliance offerings, contact us at +1 770-738-2101 Option 5 or via email at icehelpdesk@theice.com.