SENTINEL

By Trusted Solutions

Secure Chat for Military Tactical Edge and C2 Environments

OVERVIEW

The SENTINEL Secure Chat products are the culmination of Trusted Solutions' twenty years of experience in the development, deployment, and sustainment of secure chat networks for active C2, Intelligence and tactical edge mission environments.

Trusted Solutions is a US only, Veteran Owned Company, focused on providing secure, reliable, and valuable chat solutions to US DoD Agencies and their mission Partner Nations.

This document seeks to provide the reader with an overview of capabilities and benefits provided by the SENTINEL Secure Chat solution. If you have any questions, please contact us at:

Trusted Solutions, LLC
205 Powell Pl Ste 100
Brentwood, TN 37027
+1 (615) 975-5625

12/15/2021

CONTINUITY & TRANSITION

The SENTINEL Secure Chat System allows organizations to transition from legacy chat clients to SENTINEL seamlessly, with minimum required training and significant improvements in security, functionality, and overall user experience.

- **SENTINEL Chat Server.**

The SENTINEL Server is the next evolution of the Trusted IRC Server, that has over a decade in operational use with the U.S. Department of Defense. SENTINEL Server updates include decreased bandwidth, additional security and functionality that can only be realized with the SENTINEL Server and SENTINEL Client working together.

- **SENTINEL Chat Client.**

The SENTINEL Chat Client provides a modern, user-friendly interface that was created with the user/operator in mind. The SENTINEL Chat Client maintains all of the currently available functionality of legacy clients but reduces many of their laborious, multi-pull down menus and scripting requirements into single-button select features. The intuitive interface allows new users to begin using SENTINEL with minimum time required for training.

- **Continuity in Transition.**

SENTINEL was designed to allow ease of transition for those units migrating from legacy chat servers and clients. Older chat clients will continue to work with the SENTINEL Server, maintaining their same available functions, and the SENTINEL Chat Client can work with other IRC Servers. The true benefits and maximum capabilities are derived from the SENTINEL Chat Server and SENTINEL Chat Client operating collectively.

SECURITY & CONTROL

The SENTINEL Client and Server combined solution is designed to control and secure message and file transmission and storage in C2 and tactical edge environments.

- **End to End Encryption (E2EE)**

SENTINEL Chat Client provides encryption for sending of files and messages. This feature can be switched off if the client is utilized to communicate with non-secure chat Servers.

- **User Verification via PKI Token**

SENTINEL collects PKI via CAC enabled devices on devices. This information is gathered and applied to user WHOIS data when this information is available.

- **Alternate User Verification and ID Collection**

Additionally, for situations where remote operators are not able to be verified via PKI tokens, the user's specific computer or appliance data (IP, Mac, Device Names, etc.) is also collected to extended user WHOIS information and sent to the server for logging and user verification processes.

- **Secure, Encrypted and Controlled Client-to-Server-to-Client Based File Sending**

The SENTINEL Chat Client has true secure file sending with multiple administrative controls and non-repudiation features. Files can send files securely and be stored for recipients on the SENTINEL Chat Server. Recipients are alerted to files sent and Senders are provided a receipt of file acceptance. Files are deleted from the file server at an Administrator specified time interval.

- **Legacy Secure DCC File Sending**

Direct Client to Client (DCC) file sending is supported, with compatible clients, and as allowed by a chat network's policy.

- **Secure Message and File Transfer Archiving to Provide Full Non-Repudiation of Users**

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity. This function provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. All exchanges of messages or data within the chat network are administratively logged for After Action Review (AAR) and/or Investigations.

- **Access Port Control**

SENTINEL Chat Server can allocate any single port and port range connection so the client and server can move away from standard chat port ranges from 6665 thru 6669, and to a 'Green Port' and port ranges designate by Administrators and/or based on individual unit security guidelines.

- **Chat Administrator Tools**

Back-end Administrator tools help ensure server security and uptime via real-time monitoring of critical network performance and security data, including server connections, user connects / disconnects, nickname changes, list of unverified users, bot detections, overall user count, overall messages sent/received for day, month, year, logging, and file expiration configurations.

DoD COMPLIANCE & STANDARDS

- Air Force Certificate to Field (CTF) / Authority to Operate (ATO) **(IN PROCESS)**
- US Company Developed, Produced, and Assured
- For US DoD and Partner Distribution Only *(no public release versions)*
- Regular Code Security Reviews, Scans, Patches and Updates (Sustainment)

INTEROPERABILITY FEATURES

- **Legacy Client & Server Support**

The SENTINEL Server is compatible with all known existing US and Partner Nation mission utilized chat client applications, including, but not limited to, mIRC, Pidgin, hexChat, TransVerse and MAKO.

The SENTINEL Client is compatible with all known operating chat servers in the US DoD community including, but not limited to, Bahamut, OpenFire, and MAKO servers.

- **Rapid Expansion of IRC domains and networks**

SENTINEL Secure Chat based networks and components are highly modular and can rapidly add entire domains and networks for tactical edge and fixed support C2 environments. This dominant feature of SENTINEL allows network administrators to quickly create or remove whole secure chat domains for Task Force, Partner Nation, or emergency C2 groupings.

- **Cross Protocol Communications**

The SENTINEL Gateway feature bridges IRC and XMPP users together in a single, collaborative mission chat environment via an integrated protocol gateway feature. This integrated solution allows for combined, cross-community and cross network chat, in controlled and secured chat channels, compartmentalized by classification needs and fully controlled and configured by system Administrators.

RELIABILITY FEATURES

- **Low Bandwidth Requirement Met**

In expeditionary, aviation, underwater, and other tactical edge or edge C2 enclave environments, SENTINEL ensures reliability of chat networks by optimizing our development to operate in Bandwidth restrictive environments to minimize or eliminate network drop offs and/or disconnects.

- **Data Compression & Sending Optimization**

SENTINEL Server-to-Client compression decreases data traffic passed by 90% or more. This is required by high latency/low bandwidth users and minimizes and/or prevents disconnection frustrations suffered by tactical edge sites and users.

The highest bandwidth savings, reaching into 95% ranges, are seen on platforms that surface or join the network for a limited time and collect a bulk of data.

- **Network Design, Fail-Over & Redundancy Planning**

SENTINEL is engineered to seamlessly merge two or more geographically separated/online and available server access points or dedicated server/fully mirrored backups, mitigating local site failure impacts on the rest of the chat network.

- **Developed, Tested, and Proven in Active Mission Environments**

The SENTINEL Secure Chat solution's development is based on Trusted Solutions' decade of continuous improvements to meet forward operating combat and C2 mission requirements. Keeping development focused on mission-oriented capability, while making sure ongoing maintenance and improvements are kept current, is what Trusted Solutions does best.

MISSION USER DRIVEN DEVELOPMENTS

SENTINEL Secure Chat solutions are based on active mission user requirements. Many of SENTINEL Secure Chat Server and Client Solution features are direct requests from Mission Level Supported customers. Some other critical mission directed developments include:

- Back-Chat Recall / What'd I Miss (WIM)
- Security / Classification Banners
- No Registration Required for Client Software
- Gateway Cross Protocol Communications
- Keyword InfoGuard Information Assurance Protocol
- Secure, Encrypted and Controlled Client-to-Server-to-Client Based File Sending
- Data Compression & Sending Optimizations
- Alternate User Verification and ID Collection
- Mission Time-Stamp customizations

SENTINEL SECURE CHAT CAPABILITIES	Mission Requirement Set By:	Requirement Met
NETWORK CONFIGURATION		
Secure Cross-Network Configurations	**AFCENT / MDA**	✔
Fail-Over & Redundancy	**AFCENT**	✔
Mirrored Site Redundancy	**AFCENT**	✔
AES-256 with 2048-bit RSA sent and stored	**US Army / AFCENT**	✔
Unlimited Users for Server	**AFCENT**	✔
SERVER CAPABILITIES		
IRC Protocol v3 Communication	**AFCENT / US Army**	✔
XMPP Chat Communication	**DISA / AFCENT**	✔
Cross XMPP to IRC Communication	**DISA / AFCENT**	✔
Chat Logging across XMPP and IRC	**AFCENT**	✔
Secure Server Based File Sending	**AFCENT / MDA /**	✔
Support for Legacy DCC file sending	**AFCENT**	
Chat Administrator Server Tools	**AFCENT**	✔
Compatible with Legacy Chat Clients in Use	**AFCENT / US Army**	✔
CLIENT CAPABILITY		
Encrypted Sending	**AFCENT / US DoD**	✔
Data Compression @ 80 -90%	**AFCENT / AWACS**	✔
LDAP Authentication	**AFCENT**	✔
PKI Token Reading, when available	**AFCENT**	✔
User Verification if PKI not available	**AFCENT**	✔
Security / Classification Banners	**AFCENT**	✔
No Registration Required for Client Software	**AFCENT**	-
Mission Time Stamp Customization	**AFCENT**	✔
Back-Chat Recall / What'd I Miss (WIM)	**US NAVY**	✔
User Interface and User Experience Updates	-	✔
Other DoD RELATED REQUIRMENTS		
CTF for USAF (AFCENT)	**AFCENT**	X
ATO for USAF (AFCENT)	**AFCENT**	x
Mission Level Development & Tech Support	**AFCENT**	✔
United States (US) Produced and Supported	**US DoD**	✔
DoD & Nation Partners ONLY Distribution	-	✔
Developed from Mission User Feedback	-	✔

✔ = Capable X = Not Met - = N/A