Secure Chat Solutions for Enterprise Networks, White Paper

Trusted IRC Server Manual # TS-1000-004

Revised September 2017

For this Trusted IRC Server document we present all aspects of the software in two sections and formats for the reader: 1) presented via technical breakdown with line by line capabilities in section ‘Server Capabilities’ and 2) again as a mission need/impact and the software capabilities addressing those solutions in section ‘Challenges and Solutions’.
Our Mission is to Support Your Mission

Trusted Solutions' is dedicated to providing continuous reach back and front line products and support for Command and Control customers in operational environments. In many instances chat is the most effective means to collaborate, continuing to operate when other essential lines of communications are down or degraded. Understanding this demand, its critical use in coordination, integration and execution, and its ability to save lives is why we are available around the clock to ensure your mission requirements are met.

Professional Support Services

- On-site setup, World Wide.
  - Regardless of location or situation we provide hands on-site installation, setup and operational testing
  - Our staff includes U.S. DoD security cleared personnel with access levels capable to visit most areas and sites
  - Currently using an IRC server software? We have upgrade and switchover procedures to mitigate downtime.
  - Proprietary customer specific scenario and solution models engineered to meet your needs
- 24x7 reach back support.
  - Emergencies on your part constitutes one on ours and we provide that level of support and commitment
  - Providing solid continuity through employee rotations
- Critical response, front line support team. We are there, anywhere.
  - On call for worldwide, front line support as your mission dictates
- Client and server level administrator training available on-site
  - For a single instance or on a recurring, rotational basis we can develop a training strategy and schedule to fit your needs
  - Sync us in with your administrator changeover or employee rotations and we can provide hands on group military/contractor training to get personnel up to speed on their newly inherited systems
- Chat Program Level Management (IRC / XMPP / etc.) and On-Site, short and long term, support available.
- Program Management expertise to control and guide IRC chat, XMPP chat and other collaborative tools for multiple commands, multiple domains and to provide a synced intra-command solution
- Physical 'on-site' and 'in seat' contractual support is also available for short term and long term needs
  - Product and Process Control: Dynamic, Adaptive and Accountable
  - Mission requirements are dynamic and what works today may be insufficient tomorrow
  - With Trusted Solutions you have control and instant support response. We are at the ready for new requirements, updates and new capabilities/features.
  - Software and Program Control and Oversight through us. As a customer you have a direct and immediate line of communication to us in implementing changes or to provide better/new 'Trusted Solutions’ to fit your operational needs
Trusted IRC Server

Trusted IRC Server is designed for United States Department of Defense and NATO Partners, replacing antiquated IRC servers and standardizing secure and reliable IRC communications across all mission networks.

Trusted IRC Server's core is the most advanced, secure and stable IRC server platform in the world. Changing the IRC paradigm, expanding IRC capabilities and security, Trusted Solutions has developed elite server side elements focused on diverse architectures with need for high security, high assurance systems that provide near real-time, multi-user collaboration for the peacetime and joint warfighter's mission. Trusted IRC Server features represent quantum leap approaches in Command and Control (C2), created specifically on demands from commanders and leadership, planners, in-fight users, information security personnel, system and network administrators.

Server Capabilities

Multi-SERVER, Multi-NETWORK and Cross-Domain

- Developed to work with any IRC client in government and tactical mission environments that require cross-network or cross-domain processing
- Links are created between two or more servers via dedicated server-to-server links, optionally encrypted and compressed, to create in-network redundancy and enable cross domain communications as needed
- Designed to work optimally with a client's enhanced SSL and Security capabilities to comply with security needs across a wide range of network setups using configurable port mapping and encryption options
- Allowing multiple communities the ability to chat across domains in full or restricted/limited access setups

- Global Redundancy and Reliability Ensuring Continuity of Operations
  - Engineered capabilities to 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 world
  - Behind the scenes Server Data and Chat Log replication between the Hub and Leaf servers enables side-by-side or geographically separated servers to mirror the latest Primary server-side configurations and mission chat log history preventing a single point of failure or chat data loss
- In concert with administrative DNS change this backup capability provides swift and seamless automatic failover; minimizing downtime, requiring no setting changes on end user clients, and allowing the warfighter to continue mission essential operations in the event of a network or primary server outage.
- One server, or a series of servers, can be configured as spares in the data replication scheme providing even further redundancy in the event of an outage.

- **Secure Direct Client to Client & HBSS Mirroring of File Sending Control**
  - Direct Client to Client (DCC), aka file sending or file sharing, allows clients to send files back and forth (peer to peer) without taxing server resources.
  - Administrators have full control of filetype sending - for instance allowing text files and document files - *.txt and *.doc - while preventing executable and installation packages - *.exe and *.msi, along with the option to disable file sending completely.
  - This allows mirroring a site's Host Based Security System (HBSS) File Sending Control policies, enabling a highly requested need without compromising network and baseline security.
  - Secure Direct Client to Client (SDCC) file sending, with compatible clients, adds to this feature by allowing transfers files across SSL/TLS, encrypting the file transfer with a private key after a public key handshake.

- **Full Mission and Whisper/Private Chat Logging**
  - A must have Information Assurance auditing feature for building chat timelines for mission after action reviews, investigations and other legal/official/historical purposes. Our tracking system logs provide a 100% account of every conversation passing through the single server or on a central server for linked configurations.
  - Logs are secured and controlled for access to need to know elements, recorded on a centralized syslog server in a controlled access area, are easily administered, and are keyword searchable for incident review and action.
  - All chat data saves are done per channel, per conversation, per day and stored in manageable per type and per year/month/day structures.
  - Logs contain, in addition to channel chat, all possible accountability information: IP addresses, AD name, real names, nicknames, server information, connects, exits with everything server time stamped and formatted for any document reader application.

- **Information Disclosure Incident Mitigation**
  - Trusted IRC has integrated very detailed and specific features to mitigate disclosure incidents and to rapidly track, isolate and remove any chat text as needed.
  - In Channel User Lists are tagged repeatedly, creating the ability to track each and every user in a channel by name and IP for each chat line typed.
  - This enables a usable and manageable ‘who was there’ and ‘how can I find them’ capability at the exact time of any incident or event.
  - Classification Banners | Server to Client Classification banners, the same as on most controlled desktop displays, sent to and displayed on compatible IRC Client.
  - In single or cross-domain setups the IRC Client displays an administrator configurable, unobtrusive classification banner for the server and in each channel/room Window clearly establishing the highest level chat allowed in that channel/server.
Chat History on Demand (aka back chat) | Sent to the Client

- This feature is essential for sites or platforms with network inconsistencies or frequent drops. Users do not miss critical chat.
- On initial connect, or reconnect when dropped, users can immediately request chat history in one channel or every channel and get back into their mission flow and into the fight.
- Instant 'one key' access to all chat history, user configurable, for your channel or room.
- Users that join a channel for the 1st time can request the last 5 minutes, 20 minutes, or as much as the last 12 hours of chat history, on demand and as needed, to get spun up for the work day.
- This feature not only gets users into the mission faster - it also mitigates extra channel chatter for 'repeat' or 'repost' requests in high traffic or high priority channels for initial connect and disconnected users.

SSL / TLS AES 256 bit Server to Server (Links) and Client to Server Encryption

- Strategic Enterprise environments are enabled with secure communications means through compatible clients, like Trusted IRC Client.
- Data passed through any of the server-to-server or server-to-client links cannot be modified by anyone and can only be viewed by authorized users in the IRC channel.
- Multi channel/port capable: this server platform is capable of running both secure, Standards-based secure transport protocols via Secure Sockets Layer (SSL), and non-secure IRC modes on any network ports. This is essential during client non-secure to secure transition phases and for legacy applications that cannot be adapted to secure architectures.
- IP filtering: on a secure server model where you must allow or waive an intranet application to have non-SSL access, you can limit access or allow access (whitelist or blacklist) an IP or group of IPs.

LDAP Username and Password Authentication - Server and Client

- The ability authenticate user access against Windows Active Directory LDAP servers or slapd *NIX servers.
- Domain level Username and Password authentication now provides a means for accountability and control.
- All details, such as the LDAP URI, the DN to search in, search terms, error and rejection messages, and more are configurable for logging, tracking and troubleshooting purposes.
- Can be used in conjunction with integrated security and engineered linking features to implement cross-domain solutions.

Server Wide Broadcasts

- Server outage notifications and any server wide notifications are now configurable as one time broadcasts or repeatable alerts to encompass all shifts.
 Administrators can inform every user of Critical Outages, Authorized System Interruptions, Server Classifications and other server wide alerts with ease and en masse.

All broadcasts are seen by all users (not just output to a minimized status window) and enable instant awareness to all chat participants.

No limit on the number of unique alerts or their frequency

- **Bandwidth Savings Using Compression/Decompression**
  - IRC's chat protocol speed has been increased using server side 'Zip Links', enabling in-line real-time compression and decompression with up to 75% less bandwidth used.
  - The most bandwidth savings are seen in cross domain and cross AOR servers. Server-to-Server links pass all chat traffic between federated servers and can use the compression protocol to extensively minimize traffic passed on the network.
  - Server-to-Client compression decreases traffic passed by up to 75%. This is greatly needed by high latent/low bandwidth users and may also prevent the up and down connectivity frustrations that remote sites and end units with network anomalies face.

- **Channel Operators | Channel/Room Control**
  - Operator (OPs) requests, previously a high demand tasking for server administrators, have now been made manageable and, if needed, are able to be delegated to other authorized sections and limited personnel, such as an after hours helpdesk, supporting 24/7 missions.
  - The OPs give a user, site or complete section 'Channel Operators' privileges for command and oversight of their rooms with the ability to set passwords, hide rooms, post/edit topics, and to kick/ban unauthorized chat participants or create invite-only channels.

- **Network Port Assignment Control | Default 6667 is No Longer a Security Issue**
  - Port Range 6665 thru 6669, with default Port 6667, is IRC's default range. This is also the port range that worms, viruses, Trojan horses and spyware may target for vulnerabilities. As a result HBSS and Antivirus programs actively block this port at the Operating System while Network Administrators routinely block this port on the enclave firewall.
  - In direct response to this Malware IRC security concern, Trusted IRC Server can allocate single port and port range connections so the client and server can move away from port range 6665 thru 6669, and to a 'Green Port' and range allowed by your Network Administrators and security guidelines.
  - This keeps your network and baseline standards in place without compromising them for chat.

- **Administrator Awareness and Control**
  - Behind the Scenes: Keep the Server Running
  - Trusted IRC Server has extensive behind the scenes awareness and controls enabling an IRC administrator to real-time auditing of all user and internal server events.
- Monitor Normal User Events: Connects, Disconnects, User Counts, User Stats, Nick Name Changes, Topic Changes, etc
- Keep track of Server Operation: Server Links, Servers Maps, Server connects or splits, Network drops, Services starts and stops, and more
- Watch Administrator Events: failed user connection attempts, failed Operator attempts, server changes, Service restarts, Config File changes and more
- With these tools an IRC administrator section or Help Desk can view and respond to server situations instantly

- Control and Maintenance
  - Trusted IRC Server has gone beyond other server model and has the ability to change server settings and refresh changes into a live, running server environment
  - Administrator can now process changes and server updates without the need for an Authorize Service Interruption (ASI) or mission impact to the user
  - The ability to change server banners, add broadcast messages, create Channel Operators, administer File Control, alter Connecting Ports, the Message of the Day and Deny and Allow lists and more without affecting mission operation.

- Upgradeable and Configurable
  - An ever vigilant environment's requirements must change and adapt, but any downtime to initiate changes may have a mission impact. Our server platform is configured for this contingency
  - We have built the server into a highly modular format conforming to any need to enable, disable, or modify any of the extended elements of the server allowing you to choose all, some or none of the options available
  - This also gives the ability to add, remove or update server level components by transparently 'refreshing' the server to encompass these changes without downtime, server rebuilding or user impact
  - Site specific modification or network wide requested changes and updates can be made and integrated into an existing, in use platform that does not affect the server’s core integrity and reliability or result in downtime

- 3rd party application support
  - Compatible with all IRC and IRC clients and products available to date. Support for scripting in products like mIRC, Pidgin, and Microsoft Chat
  - Multiple unique mission programs are designed to interact with IRC. Some of these can extract posted data to be used in external geographic plotting programs or in office applications that import/export chat data
  - Google Earth KML data extraction and similar planning tools and data programs have specifically been modeled into, and tested within, Trusted IRC Server’s application elements
  - We have adapted our server to interact effectively with these unique programs and can configure denial, access or interactivity based on local policies as directed
  - We provide contracted, continuing support for these evolving 3rd party programs and their integration into our server platform

- Information Assurance
Information Assurance Security Assessment via Retina Network Security Scanner version 5.16.2.2571 The Network Vulnerability Assessment and Remediation Management report from Retina version 5.16.2.2571, run in Fall 2015 on a Windows 2008 R2 Server, reports no known vulnerabilities created from Trusted IRC Server's installation or use.

Multiple Defense Information Systems Agency Security Technical Information Guide (DISA STIG) security requirements and recommendations detailed in this section and in the Challenges and Solutions section have been addressed by the following enhancements:

- Auditing - Server Chat: Full Server Chat Logging - logins, logouts, meeting attendances, mission topic changes, data access, physical access, etc. - with all possible accountability information: IP addresses, AD name, real names, nicknames, server information, connects, exits with everything server time stamped and formatted for any document reader application
- Auditing - System Events: all user, system and application events for IRC - including administrator changes, server restarts, administrator success/fail attempts, stats requests, etc. - saved independently from Server Chat in priority files based on general level or administrator level events
- Audit File Save Location: all audit log files can be recorded on a centralized syslog server in a controlled access area - user configurable as to data save locations
- File Transfers (DCC): control of filetype sending such as allowing text files and document files - *.txt and *.doc - while preventing executable and installation packages - *.exe and *.msi. Administrators have full file sending control along with the option to disable file sending completely
- Prevent IM Scripting Capabilities: this is done via the File Transfers control above
- Server to Server Security: IRC servers configured to use encryption to protect information from unauthorized users - SSL / TLS AES 256 bit Server to Server (Links) Encryption
- Client to Server Security: IRC clients configured to use encryption to protect information from unauthorized users. SSL/TLS connection - SSL / TLS AES 256 bit Client to Server Encryption
- Nickname and Username Control: Controlled by instituting Nickserv modules allowing nickname registration with a password
- Red Ports - Green Ports: Red Ports pose a high risk for routine use and Green Ports are allowed for use within the DoD. Trusted IRC Server can allocate single port and port range connections determined by your network administrators
- Access Control: Ensure unauthenticated users cannot join or participate - Section/site administrative control of channels giving the ability to post/edit topics, limiting users by bans / kicks / invites only, setting passwords, etc. as authorized. Server administrative control can be used to allow or ban users by nickname, IP address, or host mask
We have evolved the software to customer needs and security rules, not forcing the customer or security to adjust to the software. Our product's evolution is based on real mission use and end user inputs and will continue to adapt to mission and security needs via customer inputs.
Challenges and Solutions

Since its grassroots inception into DoD and NATO architectures IRC's mission requirements have increased drastically, demanding enterprise and command level reliability and security while continuing to provide for site, user and warfighter focused needs.

Through direct user and administrator involvement, via suggestions, inputs and field testing, Trusted IRC has evolved, answering the challenges faced by today's users and introducing features into our products not found in any other IRC platform in the world.

Below is a list of the major change requests (in blue), presented by their request's justifications in problem form or as a user need, the request's background details on mission focus & impact, and our engineered solutions (in red).

1. Multiple Servers with Multiple Clients in the Same AOR or Across the World

   With IRC's ever expanding mission needs and user base it is not feasible to only have a single server for user connection, either in terms of network usage or redundancy or server capabilities. Additionally multiple users with multiple different client software packages add the need and for a server's interoperable capabilities. In some cases a server may have thousands of users with multiple client types all reaching across the globe to a distant end server, creating thousands of connections with needs for thousands of firewall exemptions into one site or enclave. What is needed is a local compatible server connection point for users and the ability for that server to connect/federate/link to the distant channel hosting servers and communicate with other like users and communities across the globe, reducing bandwidth and creating failovers and redundancies on the network as needed.

   **Trusted Solution**

   Trusted IRC Server was developed to work with any IRC client in tactical mission environments that require cross-network or cross-domain processing. Links are created between two or more servers via dedicated server-to-server links, optionally (and optimally) encrypted and compressed, to create in-network redundancy and enable cross domain communications as needed. Trusted IRC Server is designed to work with a client's enhanced SSL and Security capabilities to comply with security needs across a wide range of network setups by using configurable port mapping and encryption options to meet local and network wide security policies. One firewall exemption need only be made – between linked servers. Creating a region specific server in this fashion can eliminate connectivity concerns across long-haul links that experience frequent disconnects. Multiple servers on a managed system gives administrators redundancy capabilities and users failover options on their network. Multiple communities can also connect in this method giving each community the
ability to either communicate with each other unrestricted, or by setting up channel blocks limiting certain communities to a defined set of channels and prevent cross domain classification conflicts.

2. A Reliable and Redundant IRC Network
The warfighter demands an IRC network that is up 100% of the time. Administrators need visibility into the server and options to meet this 100% - 24/7 - operational demand throughout a variety failure scenarios involving equipment failures, network outages, and more. Administrators need a high level of situational awareness on their servers to proactively monitor server events and respond instantly when anomalies are experienced. Administrators need Continuity of Operations abilities to mitigate failure impacts on the chat world.

**Trusted Solution**

Behind the scenes Server Data and Chat Log replication between the Hub and Leaf servers enables side-by-side or geographically separated servers to mirror the latest Primary server-side configurations and mission chat log history preventing a single point of failure or chat data loss. In concert with administrative DNS change this backup capability provides swift and seamless automatic failover; minimizing downtime, requiring no setting changes on end user clients, and allowing the warfighter to continue mission essential operations in the event of a network or primary server outage.

Administrative awareness and control are implemented for behind the scenes auditing and administration of all user and internal server events. This give administrators the ability to: monitor Normal User Events - Connects, Disconnects, User Counts, User Stats, Nick Name Changes, Topic Changes, etc, keep track of Server Operation: Server Links, Servers Maps, Server Connects or splits, Network drops, Services starts and stops, etc. watch Administrator Events - failed user connection attempts, failed Operator attempts, server changes, Service restarts, Config File changes, etc. and respond instantly to all server situations.

In an IRC environment Chat related issues are frequently network related. Administrators can proactively monitor their server, see failures the second they occur, locate failures on the network to IP address ranges and possible geographically locations, and isolate troubleshooting efforts for networks and system administrators to the affected points with this information.

3. File Transfer Ability Is Needed That Does Not Compromise System Security
The ability to transfers files between users is an important feature when transmitting key pieces of data that need to be held in their original format – such as xls, txt, doc, - or data that is too large to simply cut and put into chat channels. This Direct Client to Client (DCC), aka file sending or file sharing, allows clients to send files back and forth (peer to peer) without taxing server resources. Additionally, other key files may need to be transferred to users on ground or in flight for mission use. Information Assurance will only allow this capability to be used if it conforms with security policies. A software package is needed that can perform all of these steps and still comply with Information Assurance policies.
**Trusted Solution**
As a response, Trusted IRC Server has developed file-transfers configuration modules that can be administrator modified to allow text files and document files - *.txt and *.doc - while preventing executable and installation packages - *.exe and *.msi, along with the option to disable file sending completely. This integrated ability give the IRC server Host Based Security System (HBSS) file mirroring and Secure Direct Client to Client (SDCC) file sending with compatible clients.

HBSS File Sending Control allows administrators to mirror a site's file type policies (similar to the restrict/allow file options that are set in e-mail), enabling a highly requested need without compromising network and baseline security. This feature is server administrator configurable and gives each server administrator the flexibility to change and conform their server to directed security needs.

4. **Provide a Definable, Secure, Retrievable and Usable Mission System of Record for All Needs**
Authorized users, which may involve Leadership, Information Assurance Officers or Investigators, need the ability to access and retrieve chat logs to build chat timelines for mission after action reviews, investigations and other legal/official/historical purposes. These logs must be secured for need-to-know elements only. The logs must be usable and manageable so that, once authorized for release, information can be collected sorted and organized with efficiently and effectively.

**Trusted Solution**
Trusted IRC Server’s Tracking System Logs provide a precise account of every action and conversation passing through the single server, or central server for linked configurations. The logs, their format and their details have been modified at mission users request to meet mission user needs.

All chat data saves are done per channel, per conversation, per day and stored in manageable and usable per type and per year/month/day structures. The logs contain, in addition to chat, all possible accountability information: IP addresses, AD name, real names, nicknames, server information, connects, exits with everything server time stamped to build an accurate and complete timeline and picture of chat events.

Logs are secured and controlled for access to need to know elements, recorded on a centralized syslog server in a controlled access area, are easily administered, and are keyword searchable for incident review and action.

Every effort has been made to provide a definable, secure, retrievable and usable system for all mission related purposes.

5. **Information Assurance: Stop Information Disclosure Incidents and Track Down Users**
Information disclosure incidents continue to occur where users chat sensitive information above the allowed classification levels on servers/channels. Information Assurance and Security Officers want to mitigate and potentially STOP information
disclosure incidents from occurring. If an incident does occur then the user or users and all potential recipients need to be identified (tracked down) so that containment, data sanitation and other resolution steps can occur.

**Trusted Solution**
To mitigate and potentially stop incidents from occurring Trusted IRC Server has developed Server Side classification banners, the same as on most controlled desktop displays, sent to and displayed on compatible IRC Clients. In single or cross-domain setups the IRC Client will display an unobtrusive classification banner for the server and in each channel/room Window clearly establishing the highest level chat allowed in that channel/server. This lack of a ‘reminder’ feature has been identified as the reason most incidents occur and its inception is projected to mitigate and hopefully stop these incidents.

For After Incident Actions Trusted IRC Server has included very detailed and specific features to actively inform and rapidly track, isolate and remove any chat text as needed. In Channel User List event details are logged repeatedly on the server, creating the auditing ability to track each and every user in a channel by name and IP for each chat line typed enabling a usable and manageable ‘who was there’ and ‘how can I find them’ capability at the exact time of any incident or event.

**6. In-Client Chat History for Immediate Mission Awareness**
Users on low bandwidth platforms or at remote sites frequently experience network related disconnects to the IRC server. This causes data and chat loss with seconds or minutes of mission related information. Other users involved in network wide outages lose chat capabilities as well. These users need a capability to continue their mission in the event of a sporadic failure.

Additionally, users that start their work shift generally a) start up their IRC client and b) join a channel. With 24/7 operations the chances that they join a channel with a mission-in-progress is high. The mission channels are 24/7 and participants may not be due to shift rotations, etc.

Users involved in these disconnect or initial connect scenarios typically have to whisper other users for updates (what did I miss? what happened?) causing delays or reposts in the channel itself for a current mission status taking up time and creating extra non-mission channel chatter. For many of these sites or platforms with network inconsistencies or drops their missions become frustrating and virtually unusable for information flow during disconnects. Users need a viable way to create a usable system and get up to speed and into their mission flow instantly in this, and any like situation.

**Trusted Solution**
Trusted IRC Server, expanding on the Full Mission Chat Logging feature, has created a user definable and on-demand retrievable chat history feature which can pull a channel’s chat history from the server to the user instantly. Via a typed command or by tying the function to your defined hotkey you can initiate a simple ‘one key’ access to all chat history for that channel enabling immediate situational awareness. You can further narrow your request to get the last 5 minutes, 20 minutes, or as much as...
the last 12 hours of chat history, on demand, to get spun up for the work day or back into a disconnected mission flow.

The sites or platforms that once had frustrating and virtually unusable chat capabilities on 'bad network days' now have a workable and reliable solution. This feature allows a dropped user the ability, once reconnected, to instantly retrieve all critical chat conversations missed during disconnects - seconds or minutes, it doesn't matter. This feature is now a staple for users and has changed the mission paradigm for these IRC platforms.

7. Administrator Ability for Server Wide Notices or Alerts
Information dissemination on important information, such as outages or alerts, does not always make it to the end mission players for IRC. With thousands of interconnected users and channels an IRC Notice/Alert System needs to be in place to disseminate information such as planned or known outages (server or network), issues, alerts and notices to each and every user in a chat network for immediate situational awareness.

**Trusted Solution**
Trusted IRC Server has administrative control over outage notifications and any server wide notifications. These are configurable as one time broadcasts or repeatable alerts to encompass all shifts. Administrators can inform every user of Critical Outages, Authorized System Interruptions and other server wide alerts, to include server Classification Messages with ease and en masse. All broadcasts are seen by all users (not just output to a minimized status window) and enable instant awareness to all chat participants without interfering with chat. This feature has been built to engage on all IRC clients – even those that allow hiding of alerts messages by default. There is no limit on the number of unique alerts or their frequency.

8. Low Bandwidth Users – Ground Forces and Airborne Platforms
Forces actively engaged in joint operations and deployed in a wide range of areas must rely increasingly on low bandwidth beyond line-of-sight wireless communication systems and network-enabled capabilities to support their mission. This convergence of requirements and constraints – for on ground, in-flight users and airborne platform intelligence users - has placed an increased emphasis on the use of chat systems and their operational utility. A priority IRC server must be in place that is configurable to address connectivity for these users.

**Trusted Solution**
Low bandwidth users often experience slow connects, multiple disconnects and sporadic network connectivity during their in-flight or in-flight use. Network inconsistencies are not always avoidable and at time must be met head-on with solutions that can offset and work around these issues. The 'In-Client Chat History' feature was developed specifically for these user types as one solution. Additionally Trusted IRC Server has created advanced operational configuration items to reduced Client bandwidth and maintain user keep-alive functions.
For the Server-to-Server communications, chat protocol speed has been increased using server side 'Zip Links', enabling in-line real-time compression and decompression with up to 75% less bandwidth used. Bandwidth savings are seen in cross domain and cross AOR servers. Server-to-Server links pass all chat traffic between federated servers and can use the compression protocol to extensively minimize traffic passed on the network to prevent the up and down connectivity frustrations that high latent/low bandwidth users at remote sites and end units with network anomalies face.

9. Channel Owners Need Full and Continuous Administrative Control of Their Channels
Mission Channels come in all flavors. Some are 'open' or public, while others are invite only and restricted to specific users or sites. Channel Owners, such as the controlling unit or site, need the ability to oversee and administer their own channels to ensure their mission goals are met. At the same time they should not have too much control to crossover or administer other mission channels outside of their mission scope. IRC Server administrators have overall 'one time' control when creating a channel but with thousands of channels the requests to kick, ban or administer each user while still administering the server can be too demanding.

**Trusted Solution**
Channel Owners now can have full command of their channels with the ability to set passwords, hide rooms, set topics, and to kick/ban unauthorized chat participants. These controllers are known as OPs. OP requests have previously been a very high demand tasking and configurable as only a temporary solution for IRC server administrators. These same administrators are still in charge of the overall Owner process but can create one-time, persistent changes for user OPs. Additionally, this administrator function can have applied security rules set so that setting OPs can be delegated to other limited authorized personnel, such as an afterhours helpdesk and non-server administrators, with minimal effort and no compromise in the server security. This allows the ability for Tiered Support; key for administrators and Help Desks or support sections focusing on multiple systems.

Entire sections and sites can now be allowed full control of their mission channels giving them the ability to post/edit topics, limiting users, setting passwords, etc. as authorized by the server admins and site policy.

10. Network Port Assignment Control | Default 6667 is No Longer a Security Issue
Many network devices, software firewalls and antivirus programs block certain ports by default due to security concerns. Network and System administrators typically must open these ports for programs to function. Network guidance along a wide variety of government and military networks have policies to block default chat protocol port ranges – such as IRC's 6665 thru 6669 range – at the enclave level in an effort to stop worms, viruses, Trojan horses and spyware and increase network security. A solution needs to be implemented where chat can function and security is maintained.

**Trusted Solution**
Trusted IRC Server can allocate single port and port range connections so the clients and servers can move away from ports 6665 thru 6669 to a port and range determined by your command and network administrators. For example, client-to-server connections can be refused on the default port 6667 while being allowed on a port listed in the DISA Category Assurance List.

A best practice network goal would be to standardize the IRC servers (software and setup) on your network and then move all IRC chat into a new 'Green Port' or 'Conditional Port' range dictated by policy.

11. Upgradeable and Adaptable to System and Security Requirements
System Administrators need a standardized IRC server model that meets current system and security requirements and is upgradeable and adaptable to future needs. Additionally chat users need a product that can have capabilities added or changed, targeted for site or network specific use, without creating an entire new software package or requirement.

**Trusted Solution**
Trusted IRC Server has been developed to address security concerns across a wide range of network infrastructures. Challenges for IRC in an operational environment differ across operations. We understand that there is not a one-fits-all solution and that software flexibility is required.

For current needs, Trusted IRC Server has tested compatibility with all IRC protocols and IRC clients. We have adapted our server to interact effectively with multiple 3rd party software platforms identified for mission use. Google Earth KML data extraction and similar planning tools and data programs have specifically been modeled into and tested within Trusted IRC Server's application elements. Administrators can configure denial, access or interactivity based on local policies as directed. We provide contracted, continuing support for these evolving 3rd party programs and their integration into our server platform.

For future needs, Trusted Solutions created the server as a highly modular format, allowing it to conform to any need of enabling, disabling, or modifying any of the extended elements. This allows you to choose all, some or none of the options available. This modular format also gives the ability to add, remove or update server level components by transparently 'refreshing' the server to encompass these changes without downtime, server rebuilding or user impact.

This refreshing ability means that site specific modifications or network wide requested changes and updates can be made and integrated into an existing, in use platform that does not affect the server's core integrity and reliability or result in downtime.

12. Information Assurance
Information Assurance (IA) managers require a usable, manageable and adaptable software platform that conforms to corporate level and local security guidance in a variety of operational environments.
**Trusted Solution**
Multiple IA requests have been received, and solutions developed to increase security, provide user auditing and to diminish chat incidents.

From core level Server-to-Server and Server-to-Client encryption components, advanced level Auditing, Tracking methods and Access Controls, Trusted IRC Server has responded by integrating multiple security measures and changes based on these IA manager requests, DISA guidance and user needs.

We have changed the program to work with the security rules, not the security rules to work with the program. This keeps your network and baseline standards in place without compromising them for chat.

**13. Product Support and Administrator Training**
A 24/7 mission requires 24/7 support – period. Non-standard and ad-hoc servers have been are set up on various networks, sites and other platforms around the world. Configuration Managers, Managers and Administrators need a standardized approved software program that has oversight, training and continuous support capable of meeting current demands and in keeping continuity through employee rotations.

**Trusted Solution**
Trusted Solutions' U.S. DoD security cleared personnel can provide hands on-site installation, setup and operational testing. We provide 24x7 reach back telephone and e-mail support. We also provide worldwide, critical response, front line support for immediate setups and emergency level issues as the mission dictates.

We provide solid continuity with Server and Client level administrator on-site training. Sync us in with your location’s administrator changeover or employee rotations and we can provide hands on training to get personnel up to speed on their newly inherited systems.

Additional Chat Program Level Management, Consultation and ‘on-site’ and ‘in seat’, short and long term, support available. We have IRC Program Management expertise to consult and control IRC chat for multiple commands.

With Trusted Solutions you have control and instant support response. If you have a new requirement, need updates and new features or new products immediately, we are at the ready. As a customer you have software and program control through us with a direct and immediate line of communication in implementing changes or to provide better/new 'Trusted Solutions' to fit your operational needs.
Trusted Solutions is a United States software development and support firm located in Nashville, Tennessee. Our team of professionals has extensive and varied backgrounds in civilian, military and government environments. Our wide knowledge base of organizational programs, policies and procedures coupled with highly dedicated and motivated individuals brings a diverse intensity into the projects we undertake.

Our specific experience as Enterprise Chat Engineers on a variety of networks gives us the ability to stay on target and sync with the warfighter's mission, providing all-encompassing and sharply focused products to accomplish critical objectives that enable our customer to save lives.

Trusted Solutions’ software is designed for use by the United States Department of Defense, associated agencies and NATO Partners. Our mission is to support your mission and our software focus is to provide up-to-date usable, reliable, robust and secure products to the warfighter as part of that effort.

Our Scalable Software allows for today’s mission needs and is adaptable to integrate future requirements. Our Energized Development Team can design and create new IRC products and solutions to accomplish the mission. And our Dedicated Support Team, with U.S security cleared employees, can meet organizational IRC needs, on or off site, with 24/7 reach back support and critical on-site support and assistance anywhere in the world.

Trusted Solutions’ contracts and customers include the U.S. Air Force, U.S. Marines, U.S. Air National Guard, Northrop Grumman, Lockheed Martin, Boeing, MIT Lincoln Laboratory and Sterling Computers (NETCENTS-2) under program vehicles such as the Missile Defense Agency (MDA), Command and Control, Battle Management, and Communications (C2BMC) and server software and support for multiple pre-deployment training sites.