

AtHoc IWSAlerts™

Network-Centric Emergency Mass Notification for Safety and Security

AtHoc IWSAlerts has been selected by some of the world's largest organizations, including the U.S. Department of Defense, protecting over 2 million Federal Government Personnel at thousands of locations.



“ The AtHoc-based system can automate personnel recall and continuity of operations and can manage personnel accountability in emergencies. Most recently it was used extensively to support the Coast Guard's response to the Deepwater Horizon oil spill. ”

– Ted Kim, USCG Lt. Commander

Challenge

During emergencies, it is critical to quickly and accurately notify all personnel of threats, provide instructions and be able to assess in real-time the status of all personnel. To effectively and instantly reach a mass audience as well as targeted individuals and groups, many government, commercial and military organizations now rely on one of their most pervasive assets – the IP network.

Solution Overview and Benefits

AtHoc IWSAlerts transforms the IP network into an enterprise-class mass notification system. By deploying AtHoc IWSAlerts, large private and public sector enterprises can rapidly and reliably alert thousands of employees in geographically dispersed buildings and facilities during an emergency.

AtHoc IWSAlerts provides:

- **Personnel protection:** Mass dissemination of alerts across multiple channels, to accelerate threat response
- **Personnel recall:** Rapid communication to personnel while off facility to report back to duty
- **Personnel accountability:** Real-time response tracking reports on the status and safety of all personnel
- **Critical communications:** Distribute important corporate information to employees, including IT mass alerting
- **Regulatory compliance:** Meets government and commercial emergency management, disaster recovery and continuity planning requirements, including fire and building safety (i.e. NFPA 72 2010 and DoD UFC 04-021-01)

AtHoc IWSAlerts – An Enterprise-Class Solution

AtHoc IWSAlerts has been designed as a highly secure, enterprise-class network-centric mass notification and emergency communication system. Its interoperability, scalability and security measures have led to its selection by highly demanding defense and commercial organizations including the U.S. Air Force, U.S. Army, U.S. Navy, U.S. Coast Guard, U.S. Department of Veterans Affairs, UCLA, Microsoft, Boeing and Raytheon.

AtHoc IWSAlerts can:

- **Transform your existing IP network** into an enterprise-class mass notification system for rapid communication, pervasive reach and cost effectiveness
- **Unify all communication channels and devices** via the AtHoc Unified Notification Server, into a single system to simplify activation, ensure message consistency and reduce alerting time
- **Manage the notification process across the enterprise** with pre-defined scenarios, operator access policies, multi-location support, alert activation flow, tracking and reporting
- **Monitor video feeds, physical security/life safety sensors** and external data sources to automatically trigger notification scenarios
- **Ensure accuracy of personnel contact information** by integrating with enterprise directories and supporting end user self-service updates
- **Improve building safety** by integrating with existing fire alarm and public address systems
- **Scale to support hundreds of thousands** of personnel worldwide

To learn more about AtHoc products and solutions, call 650.685.3000 or visit www.athoc.com



Features and Benefits

AtHoc IWSAlerts can manage the emergency notification process across your entire enterprise. Using a web-based console, operators from any location in the organization can activate alerts to virtually any device, track responses and view accountability reports. Automatic notifications can be triggered by physical sensors and data feeds. Notification processes can be defined to support both enterprise-wide and individual department needs.

Unified Notifications to All Devices

Through a single unified interface, AtHoc IWSAlerts allows you to quickly communicate a consistent message across multiple channels and delivery devices (customizable messaging per device) – all integrated using the IP network. The information is sent via multiple and redundant means, including:

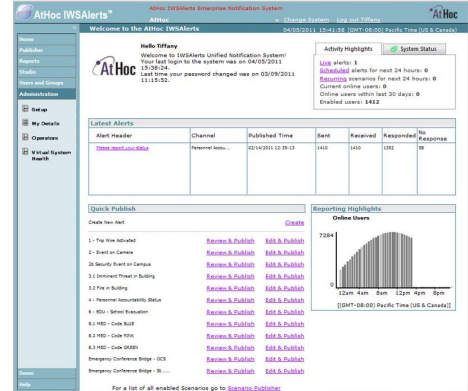
- **Networked Computers** – Delivery of audio-visual pop-up notifications to computer desktops connected to the IP network
- **Networked IP Phone Displays** – 2-way audio-visual (text, video, images) blast alerts to IP phone displays and speakers
- **Telephony** – Delivery of voice telephony alerts to any land, VoIP, mobile phone via on-site or hosted mass dialing services
- **Text-messaging** – Delivery of text-messages (SMS) to mobile phones, pagers, and BlackBerry devices
- **Email** – Secure digitally PKI signed email delivery with responses using the organizations’ email address (i.e. .mil, .gov)
- **Social Networks** – Send alerts through popular social networking channels, including Twitter and Facebook
- **Indoor and Outdoor Speakers** – Audio notifications to outdoor sirens and indoor public address systems
- **Cable TV and Display Boards** – Text, image or video alerts sent to digital displays
- **Radio Broadcasts** – Audio broadcasts to local radio stations
- **Land Mobile Radios** – Transmit alerts to security forces handheld LMR
- **Building Safety/Fire Protection** – Integrates with existing fire alarm systems
- **XML Feeds:** Output standard XML feeds (RSS, Atom and others) integrating with other systems and web sites

AtHoc Delivers – Secure Digitally PKI Signed Email Delivery with Responses

AtHoc IWSAlerts Integration with the SMTP delivery infrastructure enables emails to be sent directly using the organizations’ email address (.mil, .gov, for example) supporting customer GOV or DoD PKI digitally signed emails. End users can reply directly to email alerts by simply typing the number of the response option and hitting send. Having email alerts with digitally PKI signed signatures provides another level of confidence in meeting security and accountability requirements, following recent DoD and government directives. Enables the embedding of rich content including HTML, videos and links in email alerts that further enhances the already existing SMTP email alert functionality.

Response Tracking and Reporting for Personnel Accountability

During an emergency, all alert recipients receive multiple response options for reporting their status and acknowledgement on all personal communication channels (e.g., desktop, phone, SMS or email). The delivery, receipt and responses of the alerts are tracked in real-time, giving operators either a summary view or detailed delivery report for each alert recipient. Reports can be exported in PDF, CSV, Excel and more. This unique alert feedback loop provides critical accountability and visibility into the status of personnel across the enterprise.



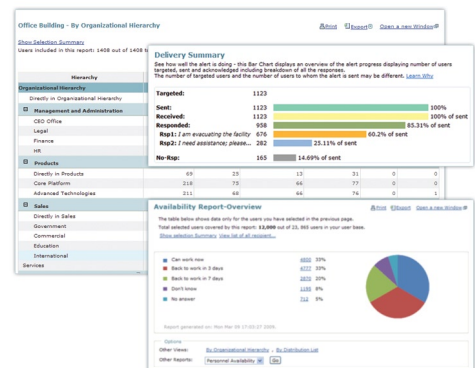
Web-based console for managing the entire notification process



Through a single web-based management console, launch and manage all communication channels simultaneously. Devices include computers, phones (cell, landline, VoIP), PDAs, pagers, BlackBerrys, computer kiosks, sirens, TV, Radio and PA systems

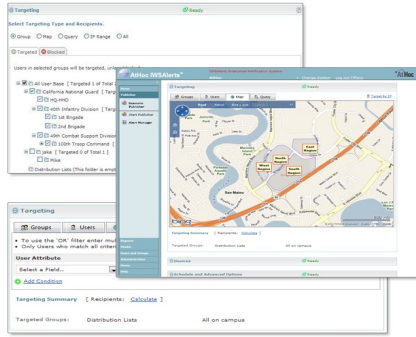


AtHoc IWSAlerts unifies all alerting channels, including triggering alerts to Giant Voice/PA systems and digital displays



Real-time response tracking provides accountability and visibility into the safety and status of all personnel

ATHOC IWSALERTS – NETWORK-CENTRIC EMERGENCY MASS NOTIFICATION FOR SAFETY AND SECURITY



Quickly target personnel by organizational hierarchy, geographical maps, named individuals, distribution lists or dynamic queries

Automated Emergency Scenarios and Processes

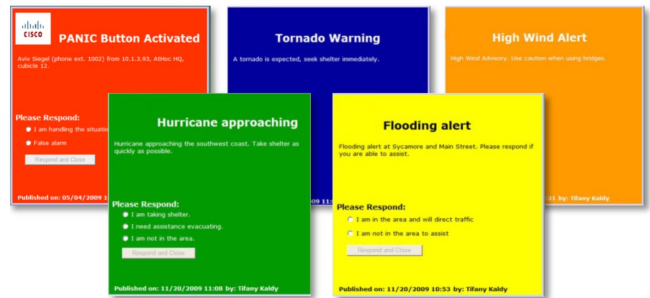
AtHoc IWSAlerts automates operating procedures for emergency situations by providing a library of over 100 out-of-the-box scenarios, including FPCON, INFOCON and warning conditions.

Scenarios include alert content, response options, targeted recipients and delivery devices. Operators can customize their own scenarios and processes or create new ones using simple web-based tools.

Within the publishing flow, AtHoc IWSAlerts allows for a single alert message to be sent to multiple recipients that share the same phone number (i.e. workgroup, department, call center) while automatically consolidating multiple alert messages into one notification that is then sent only once to the shared phone.

Personnel Can Be Targeted by Organization, Geography, or Individual Names

AtHoc IWSAlerts can target people based on organizational structure, distribution lists, physical location, individual name or dynamic database query. Personal and mass notification devices (such as sirens and display boards) can be targeted using visual geographic maps, enabling the selection of buildings, regions or zones to be notified. Dynamic targeting can be accomplished using a combination of attributes such as individual, role, location or IP address. During the publishing flow, an operator can block or remove individual recipients by name, from a targeted distribution list set for notifications.



A sample of the over 100 out-of-the-box alert scenarios



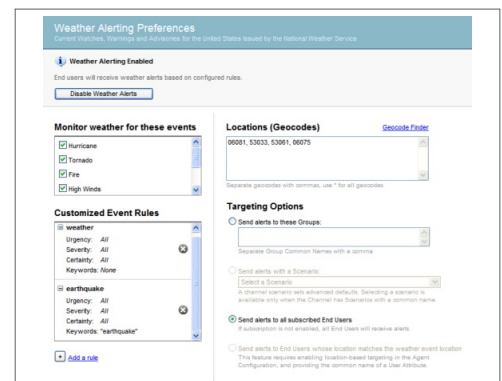
The panic services feature on a Cisco IP phone, and resulting popup alert sent to security personnel

Real-time Alerts to Security Personnel Using IP Phone Panic Button

Specific keys on IP phones can be configured as Panic or Duress Buttons. By clicking on such button, end-users can send real-time alerts to security officer or Emergency Operation Center (EOC) operators quickly and quietly. The Panic Alert received by the EOC operators identifies the effected individual as well as the location and type of emergency, allowing security operators to take immediate action.

Event Monitoring and System Interoperability

Emergency alerts are often triggered by physical sensors (e.g., fire alarms, video surveillance and chemical detectors) or external data sources (e.g., National Weather Service content feeds). AtHoc IWSAlerts can monitor these events, and using pre-configured business rules, it can automatically activate any emergency scenario. By utilizing Common Alerting Protocol (CAP), XML and web services, AtHoc IWSAlerts also enables communication with external systems, such as federal, state and local agencies for information sharing and interoperability.



Monitoring external sensors and event sources, including critical weather conditions using the AtHoc Weather Alerts Module

Up-to-date Contact Information and Self-service

Maintaining the accuracy of personnel contact information is crucial for the success of any large-scale emergency notification system. AtHoc IWSAlerts addresses this challenge via a three tiered approach:

- **Integration with Organizational Repositories** – AtHoc IWSAlerts concurrently integrates with multiple enterprise user directories to continuously synchronize personal and organizational information. Supported repositories include Active Directory, LDAPv3, MilIPDS, CivPDS and common HRMS applications.
- **Operator Management** – Local operators can either manually update contact information for their local personnel or import personnel rosters in common file formats such as CSV or XLS.
- **User Self-service** – Individual end users can access and modify their own personal information and device preferences through a web-based, self-service portal, as well as view their personal alert Inbox.

Self-service module allowing end users to update their own contact information, alerting preferences and status

Health Monitoring and Supervision

AtHoc IWSAlerts provides administrators complete visibility into the health of the system and end devices via visual indications, system and detailed event logs as well as sending proactive notifications of any important system and device status change that may affect the notification process. Visual indicators within the system give the operator immediate awareness as to the status of various capabilities and features (i.e. red, yellow, green). Supervision of the system is achieved across all system components, including network and integrated end devices, such as strobes, alarms, and displays.

Enterprise-wide Operations and Multi-tenancy

With its enterprise capabilities, AtHoc IWSAlerts can be deployed centrally using a “secure private cloud” architecture to support a multi-site implementation while catering to the alerting needs of each individual group. This means that organizational emergency directors can disseminate alerts to the entire user population with visibility across the entire enterprise, while providing each remote site its own “private” alerting system. AtHoc IWSAlerts also includes a permissions management system that controls operator access rights to scenarios, contact information and device types. Beyond increased data confidentiality and network security, this centralized (“private cloud”), enterprise-wide approach provides a common notification system across the enterprise. Additionally, private cloud deployments reduce infrastructure and maintenance costs and enables organizations to notify and collect responses from hundreds of thousands of personnel in minutes.



AtHoc IWSAlerts can be deployed to support a single site or deployed in a centralized data center, supporting a multi-site organization while catering to the needs of each location – capable of notifying hundreds of thousands of personnel in minutes. All alerting devices can be triggered either by a local site or centrally by headquarters

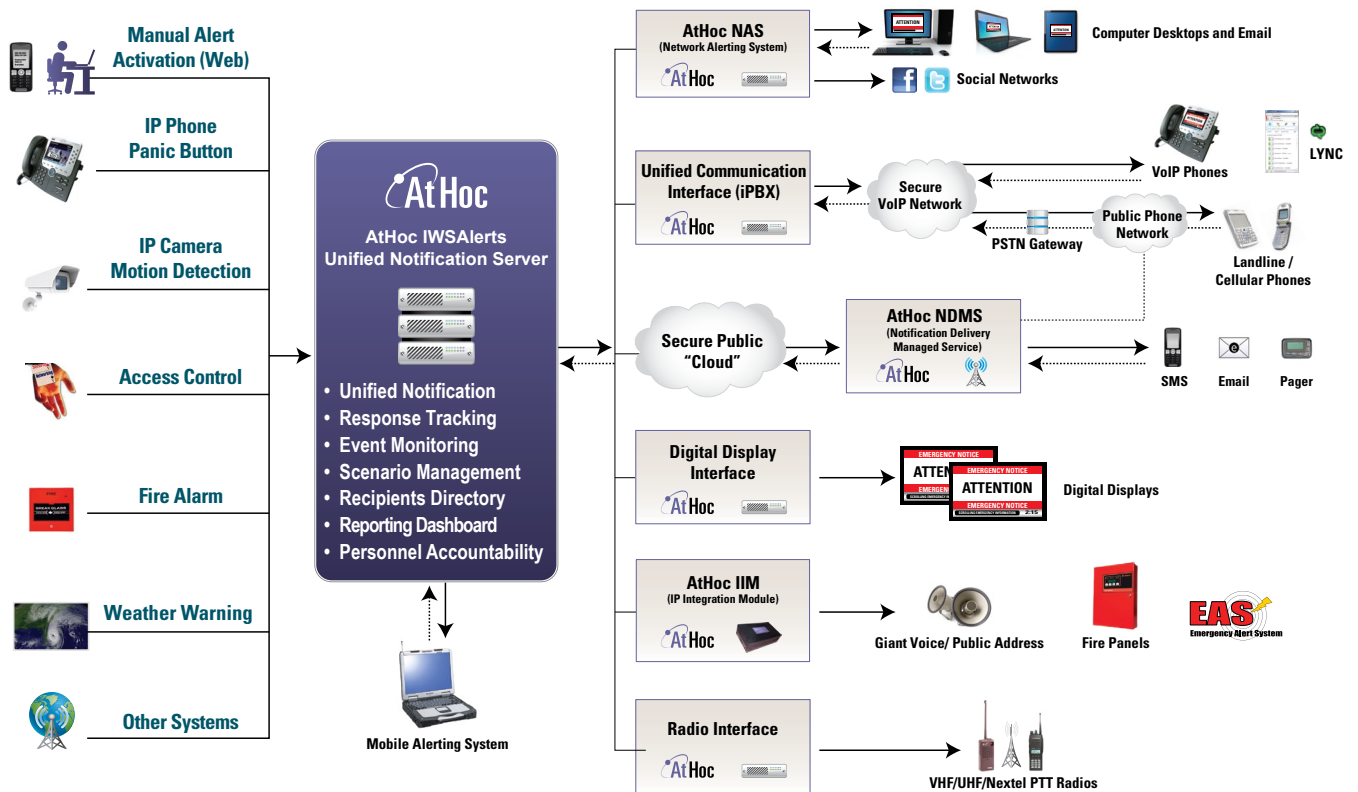
Enterprise-class Architecture

AtHoc IWSAlerts provides numerous enterprise capabilities, including:

- **Interoperability and Integration:** Uses standard and open protocols including CAP, XML and web services
- **High Availability:** Automatic and manual failover to an alternate site in case of critical failure of primary site
- **Security:** Provisions for secure communication, authentication and encryption using industry-standard PKIs
 - Digitally PKI signed email (SMTP) delivery and sending directly using the organization’s email address domain
- **Scalability:** A load-balanced server farm to support hundreds of thousands of end users
- **User Directory Integration:** Active Directory, LDAP and other common enterprise directories accessible via API
- **Deployment Flexibility:** Multiple delivery options including:
 - **On-premise:** Entire system deployed behind the firewall leverages secure integration with user directory and internal resources including network, Cisco Unified Communications Manager, Microsoft Lync, Public Address Systems, siren systems and physical security sensors
 - **On-premise with Telephony Alerting via IP-Based Unified Communications Technology:** Delivery of alerts as audio messages to any land, mobile or VoIP phone
 - **Hosted/Software-as-a-Service (SaaS):** Available as a service from a redundant and highly available remote hosting facilities, speeds deployment and eliminates the need for on-site hardware. AtHoc SaaS service is certified per NIST SP 800-53 Rev3 IA controls at FIPS-199 Moderate classification
 - **On-premise with Hosted Managed Notification Delivery Service:** Software installed locally with secure access to remote communication center for mass telephony dialing and text messaging without taxing local telephony resources
 - **On-premise with Hosted Failover:** Software installed locally with failover to host facility, assuring redundancy

AtHoc Mobile Alerting System

AtHoc Mobile Alerting System (MAS) includes an **PATENT PENDING** AtHoc IWSAlerts server instance that is packaged preloaded on a ruggedized or semi-ruggedized laptop computer. MAS can connect to a central alerting site via Virtual Private Network using wired or wireless transmission. It can also use the local AtHoc IWSAlerts server for direct access to the remote communication center, maintaining telephony alerting capabilities in the event of a catastrophic breakdown of local infrastructure. If an evacuation is necessary, AtHoc’s MAS is fully portable and can be carried easily by a single person. Data is synchronized from central site to local site to ensure the local site is always up to date. The system allows Internet connectivity through Local Area Network, WiFi, wireless broadband and satellite channels. MAS does not depend on the local infrastructure (e.g. PBX, IP network) to provide full alerting capabilities.



The above architecture diagram shows the role of AtHoc IWSAlerts in monitoring events from multiple sources (on left), delivering alerts to multiple devices and capturing responses from individuals (on right)

Compliance with Federal Requirements and Guidelines

National Fire Alarm and Signaling Code (NFPA 72)

The National Fire Alarm and Signaling Code (NFPA 72) updated its code in 2010 to include Distributed Recipient Mass Notification Systems (DRMNS). The NFPA code provides the blueprint for the implementation of ENS (or as the code labels it DRMNS) in facilities nationwide. AtHoc fully complies with NFPA 72 (2010) DRMNS requirements.

UFC Recommendations for Network-Centric Alerting Systems

The DoD's Unified Facilities Criteria (UFC) 4-021-01 titled "Design and O&M: Mass Notification Systems," provides planning and design of mass notification systems and applies to U.S. military departments and defense agencies. AtHoc IWSAlerts fully complies with the specifications for Network-Centric Alerting Systems (NCAS) incorporated in the UFC.

NIST SP 800-53 Rev3 IA Controls at FIPS-199 Moderate Classification

AtHoc IWSAlerts has been certified for its SaaS service per NIST SP 800-53 Rev3 IA controls at FIPS-199 Moderate classification. This process is equivalent to DIACAP (MAC level II) security certification processes done by our government customers. AtHoc is the only vendor to offer such certified SaaS service.

Security and Network Certifications

AtHoc IWSAlerts has numerous DoD security and network certifications and complies with key DoD security requirements, including:

- DIACAP – certified under DoD Information Assurance Certification and Accreditation Process, DISA 8500
- NIST SP 800-53 IA Control Set - certified under Rev 2 and Rev 3
- Army-wide Certificate of Networthiness (CoN)
- Navy/Marine Corps Intranet (NMCI) Certificate to Operate
- Defense Information Systems Agency (DISA) FSO Gold Standard and applicable STIGs
- DoD Common Access Card (CAC) requirements
- DoD Password Management Policy
- Secure PKI Digitally Signed On-Premise email delivery
- DoD Standard Ports and Protocols compliant

DoD Instructions and Requirements

- DoD Instruction 6055.17 "DoD Installation Emergency Management (IEM) Program": AtHoc IWSAlerts is fully compliant with the Mass Warning and Notification capability.
- Air Force Instruction (AFI) 10-2501 "Emergency Management Program Planning and Operations": AtHoc IWSAlerts meets the AFI's network-centric alerting requirements pertaining to installation warning systems.
- AFI 10-218 "Personnel Accountability in Conjunction with Natural Disasters or National Emergencies": AtHoc IWSAlerts

supports this AFI by proactively querying personnel for status and providing accountability reports to operators.

- Navy Anti-Terrorism Force Protection (ATFP): AtHoc IWSAlerts complies with the requirements of the ATFP program responsible for all Navy installations.

Deployable on All Major DoD Networks

AtHoc IWSAlerts has been deployed on the following networks:

- NIPRNET (Unclassified but Sensitive Internet Protocol Router Network)
- SIPRNET (Secret Internet Protocol Router Network)
- NMCI (Navy/Marine Corps Intranet)
- JWICS (Joint Worldwide Intelligence Communications System)
- ONE-NET for OCONUS Navy

Federal Continuity Directive 1 (FCD 1)

Federal Executive Branch National Continuity Program and Requirements Agencies should have procedures in place to contact employees in the event of an emergency. Agencies should establish alternative means for employees to contact the agency in the event an emergency causes a disruption to the regular means of communication with the agency.

OMB Memorandum M-05-16: Regulation on Maintaining

A national directive designating OMB with the authority to issue a regulation on certain telecommunications functions under Section 414 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of Public Law 108-447).

National Communication System (NCS) Directive 3-10

The National Security Presidential Directive 51/Homeland Security Presidential Directive 20 established a comprehensive program designed to ensure survival of our constitutional form of government and the continuation of the performance of National Essential Functions under all conditions.

Section 508 of the Rehabilitation Act

Section 508 requires federal departments and agencies to ensure that personnel with disabilities have fair access to and use of IT systems. AtHoc Desktop Notifier™ (the desktop component of AtHoc IWSAlerts) software passed the Department of Commerce test for Section 508 compliance.

HEA and Clery Act Compliance

Amendments to the Higher Education Act and Clery Act require universities to: Develop and implement communication systems for emergencies and develop procedures or notify their community about emergency situations.



AtHoc, Inc.
www.athoc.com

2215 Bridgepointe Parkway, Suite 150
San Mateo, CA 94404

Tel: +1.650.685.3000
Fax: +1.650.685.3010

