



Network-Centric Emergency  
Notification Systems

# AtHoc IWSAlerts™ – Editions Comparison Summary

## Features

Version 6.1.8 (build 42), Updated: 9/18/08

Express Standard Enterprise Enterprise  
NAS

	Express	Standard	Enterprise NAS	Enterprise
<b>Network Alerting System (NAS) – Desktop Notifications</b>				
1. Delivery of audio-visual and video notifications to network-connected desktops, including capturing responses	✓	✓	✓	✓
2. Client support for Windows XP/Vista and Mac OS X 10.4 (Tiger) and 10.5 (Leopard)	✓	✓	✓	✓
3. Delivery of alerts via email, BlackBerry messages and text-messaging (SMTP)	✓	✓	✓	✓
<b>Telephony Alerting System (TAS) – Phone Voice Messaging and Mobile Text Messaging</b>				
4. Delivery of notifications to recipients as voice messages to land or mobile phones, including capturing responses		✓		✓
5. Delivery of alerts via mobile text-messaging (SMS/SMPP)		✓		✓
6. Supports both hosted telephony service[1] and integration with existing local telephony alerting devices including VoIP[2], both using secure Web Services, XML and/or CAP		✓		✓
<b>Sirens, Giant Voice and Public Address Notifications Activation</b>				
7. Delivery of audio notifications to outdoor sirens ("Giant Voice") or indoor speakers/Public Address system [2]		✓		✓
8. Activate a pre-existing scenario (or "key") for targeted speaker/pole locations		✓		✓
9. Use text-to-speech to create on the fly an audio message consistent with other messaging capabilities		✓		✓
<b>Unified Notification – Personal and Non-personal Mass Notification Devices</b>				
10. Web-based unified console for single activation of alerts across multiple delivery devices		✓		✓
11. Device selection based on user preference, scenario definition or operator override selection		✓		✓
12. Delivery to personal devices: desktop notifications, phones, SMS/Text messaging, email, Fax, TTY/TTD; and to non-personal devices: Giant Voice/PA, Fire Alarms, Display Boards, Kiosks, Radio, LMR and TV[2]		✓		✓
<b>Notification Process Management – Scenarios, Geographical and Organizational Targeting</b>				
13. Targeting based on multi-level organizational hierarchy, geo-based mapping and distribution lists	✓	✓	✓	✓
14. Alerts may be defined on-the-fly, based on pre-defined scenarios or based on recurring schedule	✓	✓	✓	✓
15. Scenarios include: content, responses, recipients, delivery devices and permitted operators	✓	✓	✓	✓
<b>Response Tracking, Reporting and Archiving</b>				
16. Support for one or more response options presented to recipients for acknowledgement	✓	✓	✓	✓
17. Real-time aggregated alert delivery and response summary; graphical view (bar, graph or pie charts)	✓	✓	✓	✓
18. Detailed analysis for organizational hierarchy, groups and specific levels and members	✓	✓	✓	✓
<b>End User Information Management and Self-service</b>				
19. Recipients management including: viewing, creating, editing, lists creation, and import/export	✓	✓	✓	✓
20. Web-based Self-service portal to allow end users to update their own information, devices and view alerts	✓	✓	✓	✓
<b>Enterprise User Management and LDAP/AD Integration</b>				
21. Integrating with enterprise user repositories including Active Directory, LDAP and others[2]			✓	✓
22. Defining custom user attributes such as role or rank – allow grouping and targeting based on such attributes			✓	✓
23. Managing organizational structure/hierarchies, including targeting, reporting and grouping based on hierarchy			✓	✓
24. Concurrent integration with multiple sources of user data to create recipient records			✓	✓
<b>Enterprise Permissions Management for Operators</b>				
25. Permission policy tools for operators defining rights according to organizational unit, user groups or location (i.e. which operator can target certain users in certain locations or manage their user information)			✓	✓
26. Operators permission rights based on Scenarios (i.e. which operator can activate certain scenarios)			✓	✓
27. Role-based permissions for operators including: fully admin, alert activator, user data manager etc.			✓	✓
<b>Enterprise Multi-tenancy Management</b>				
28. Centralized deployment with multi-tenants capability (e.g. multiple departments or bases on a single system)			✓	✓
29. Logical segmentation between multiple organizations based on permissions and access rights			✓	✓
30. Allows "alert cascading" per defined setup of relations between departments and HQ			✓	✓
<b>Event Monitoring and System Interoperability</b>				
31. Monitor sources of information such as weather and sensors and automatically activate scenarios			✓	✓
32. Interoperability with other local or government agencies based on CAP/XML feeds			✓	✓
<b>Enterprise-class Network-centric Architecture</b>				
33. Support for number of operators	Up to 10	Up to 10	Unlimited	Unlimited
34. High Availability – automatic and manual failover to an alternate site in case of critical failure	✓	✓	✓	✓
<b>Compliance with DoD/Federal Regulations and Guidelines</b>				
35. Compliance with UFC 4-021-01, UFC 4-010-10, DITSCAP/DIACAP, Section 508 and JAWS	✓	✓	✓	✓
36. Deployed on all Major Department of Defense networks	✓	✓	✓	✓
37. CAP (Common Alerting Protocol) compliant – emergency management interoperability guidelines	✓	✓	✓	✓

[1] Internet-accessible Remote Communication Service Provider (RCS) using secure (SSL/HTTPS) communication (not requiring any local PBX interface).

[2] Please ask your AtHoc representative for currently supported list of devices.