

Vantage™ for IBM Sametime



Security and Compliance for IBM Sametime

Actiance Vantage™ for IBM Sametime addresses the security, management, and compliance of Unified Communications (UC), including user policy management, message hygiene, malware prevention, and archiving for eDiscovery. Enterprise communications environments are heterogeneous, consisting of the “enterprise” UC platform and typically several public instant messaging (IM) networks – requiring corporate UC platform security, federated connections with external parties and networks – alongside those publicly available networks that do not connect with the corporate messaging platform.

UC Management Challenges

Businesses increasingly require role-based access control; management at global, group, and user levels; differentiation between group and federation policies; monitoring of LDAP-, IP-, and Domain-based policies; and control of IM, group chat, and Sametime Meeting usage. Vantage enables role-based access control, policy management, IM, group chat, Sametime Meeting, disclaimers to end users, ethical walls, reporting, workflow, and audit reports.

Data Leakage and Inbound Security Threat Challenges

Within collaborative environments such as Sametime, users continue to utilize publicly available real-time communications tools, such as Yahoo!, AIM, Google Talk, and Skype, which results in a heterogeneous environment requiring a security and compliance solution that addresses the whole real-time communications spectrum. However, doing so presents some challenges.

- Malware has begun to appear in real-time communications channels. Increasingly, more damaging attacks are spreading to real-time communications in order to bypass existing security measures. Spam is also moving beyond the email inbox into the IM stream, further increasing the risk of inadvertent malware infection.
- Valuable proprietary information is often transferred outside the corporate network using unmonitored IM and UC channels.

Compliance, Liability, and Risk Challenges

In the USA alone, there are more than 10,000 laws relating to electronic and real-time communications. There are clear penalties for non-compliance with these regulations. Aside from fines, damaged reputations, and potential loss of intellectual property, the effort involved in recovering from these setbacks can be detrimental to ongoing business.

Actiance Vantage™ Enhances Sametime Deployments

Vantage™ provides granular security, compliance, and policy controls for Sametime, alongside publicly available IM networks, Web conferencing, and industry-focused IM communities such as Thomson Reuters Messenger, Bloomberg, and YellowJacket. Designed to meet an organization’s security, management, and compliance requirements for real-time communications, in addition to supporting all the key government and industry regulations (e.g., FISMA, FINRA, SEC, FRCP, Sarbanes-Oxley, MiFID, and FERCA), Vantage™ delivers additional benefits to native Sametime implementations.

AT A GLANCE

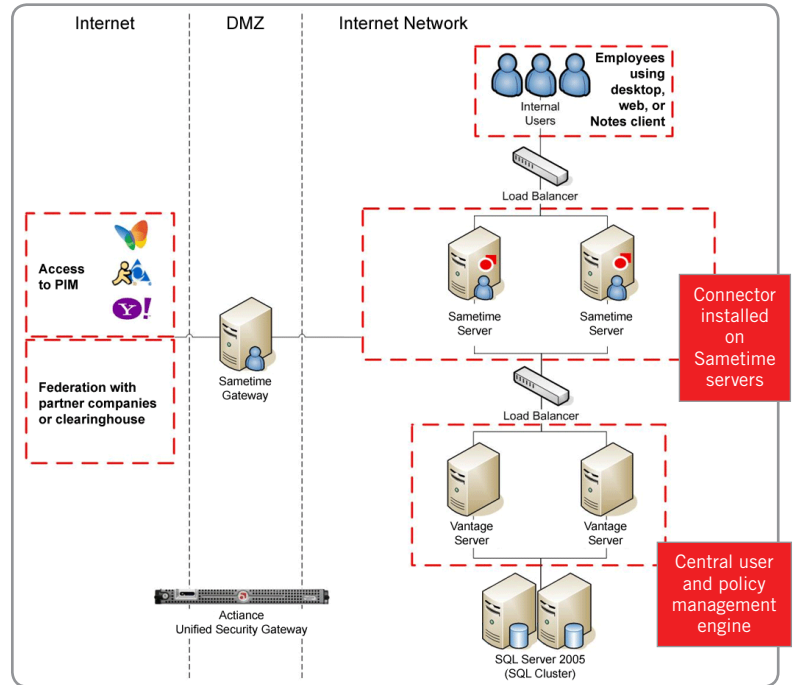
Vantage™ ensures security, management, and compliance for real-time and unified communications – from presence and instant messaging to group chat and conferencing.

KEY FEATURES

- Support for IBM Sametime as well as public IM networks for flexible deployment
- Provides policy setting, real-time monitoring, compliance, capture of file uploads, application of DLP/content filtering rules and enforcement of ethical walls for group chat
- Ethical wall enforcement
- Auditing of Sametime events for Sametime Meeting events, including allow/block users, ethical walls, start and end times, and participant join and leave times
- Integrated with Lightweight Directory Access Protocol (LDAP) to define permissions at the company, group, and user levels to enforce ethical boundaries and acceptable use policies
- Prevents data leakage over Sametime and public IM platforms through content filtering and regular expression
- Full support for multiple Points of Presence
- Supports Blackberry PIN and SMS Messaging
- Virus scanning of file transfers
- Secure, intuitive Web-based administration and reporting, including detailed usage reporting by log in, number of messages, time interval, and unified communications events
- Auditing and easy retrieval of tamper-proof stored information based on granular searches of keywords, users, and time frames to meet eDiscovery requirements
- Enterprise Reporting for ROI, Departmental Cross Charge, and usage analysis

Vantage™ for IBM Sametime

Actiance Vantage™ accurately and completely logs all real-time communications, including file transfers and blocked messages, to ensure compliance with corporate governance, data protection, and eDiscovery regulations. The transferred files are stored with the relevant messages, simplifying the review process and ensuring that all communications are seen in the context of a complete conversation and with message order preserved.



Additional Benefits For Sametime

Function	Additional Benefit Provided by Vantage
Central policy and logging for IM, Group Chat, and Sametime Meeting Activity	UC policy is defined centrally and applied across communication modalities; captured data is stored in a single location to provide a comprehensive view of system usage and a single integration point for data archival systems
Public IM client support	Support for all native, major public IM clients including Google Talk, AIM, and Yahoo!
Authentication & Authorization Services	Policies at company, group, and user levels; Group-level ethical boundaries; IP address-based access controls; Access controls and monitoring options
File transfer management	Policies at company, group, and user levels; Allow/block at all levels; Specify rules for file name/size/type; Can detect and block words, phrases, and full regular expressions and flag/block and/or alert based on content
Anti-virus and malware control, including bots	Support for Symantec, McAfee, TrendMicro, CA, ClamAV, Sophos, and Kaspersky. Zero-day worm blocking. Files are not scanned on Sametime front end so no additional load.
SpIM blocking	Content-based protection using white/black lists and custom rules
URL blocking	Domain-configurable and direction-configurable URL policies.
Federation management	Allow/block permissions at company, group and user levels; Ability to specify explicit partner, domain-based rules at company, group, and user levels
Legal disclaimer notification	Disclaimers sent inline and audited; disclaimer display controls at the IM network and group levels
Tamper detection	Guaranteed message order preservation; anti-tamper mechanism validates conversation integrity
File transfer capture	Files archived in database and shown in context in conversation review – single database deployment and reporting
eDiscovery retrieval	Reports on IM usage, security violations, compliance violations, transcript reviews. Scheduling and auto-delivering available.