

for Microsoft® Office Communications Server

Security and Compliance for Microsoft Office Communications Server

Actiance Vantage™ for Microsoft OCS addresses the security, management, and compliance of Unified Communications (UC), including user policy management, message hygiene, malware prevention, and archiving for compliance. Enterprise communications environments are typically highly heterogeneous, consisting of the UC platform requiring corporate UC platform security as well as federated connections with external parties and networks – alongside native public instant messaging networks that do not connect with the corporate messaging platform.

UC Management Challenges

Businesses increasingly require role-based access control; manage at global, group and user levels; differentiate between group and federation policies; monitor Active Directory, IP-, and Domain-based policies; and control VoIP, Video, IM and group chat, and Live Meeting usage. Vantage enables role-based access control, policy management, VoIP, Video, IM and group chat, Live Meeting, disclaimers to end users, ethical walls, reporting, workflow and audit reports.

Data Leakage and Inbound Security Threat Challenges

Within collaborative environments such as Microsoft OCS, users continue to utilize publicly available real-time communications tools, such as Yahoo!, AIM, GoogleTalk, Windows Live, 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 OCS Deployments

Vantage™ provides granular security, compliance, and policy controls for Microsoft OCS, 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, FERC), Vantage™ delivers additional benefits to native OCS implementations, in architectures where it is deployed either with or without Microsoft Forefront.

AT A GLANCE

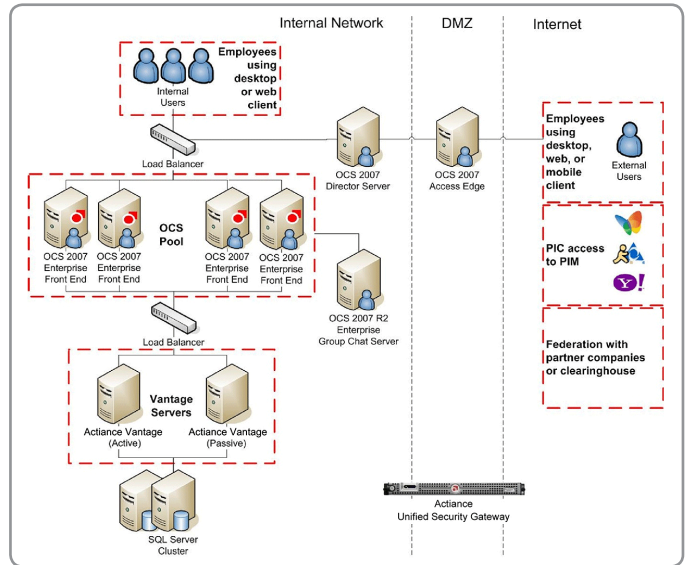
Vantage™ ensures security, management, and compliance for Real-time and Unified Communications – from presence and instant messaging to conferencing and voice.

KEY FEATURES

- Support for OCS R2 and Live Communications Server (LCS) as well as public IM networks
- 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
- Auditing of OCS events for audio, video, and Live Meeting events including allow/block users, ethical walls, start and end times, and participant join and leave times
- Configurable “Poison Room” policies for ethical wall enforcement in OCS 2010 Live Meeting sessions
- Call Admission Control (CAC) features include resource allocation for audio, video, and collaboration sessions
- Integrated with Active Directory to define permissions at the company, group, and user levels to enforce ethical boundaries and acceptable use policies
- Prevents data leakage through content filtering and regular expression
- Full support for Multiple Points of Presence for OCS and LCS
- 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 UC events
- Auditing and easy retrieval of tamper-proof stored information based on granular searches of keywords, users, and time frames to meet e-Discovery requirements
- Leverage existing SQL databases for real-time storage
- Reporting for ROI, cross-charge, and usage analysis

for Microsoft® Office Communications Server

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 e-Discovery 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 OVER NATIVE OCS AND OCS WITH FOREFRONT

Function	Microsoft OCS	OCS plus Forefront	Additional Benefit Provided by Vantage
Central policy and logging for IM, Group Chat, VoIP, Video, and Live Meeting Activity	No central policy; partial data captured in disjointed data stores	No central policy; partial data captured in disjointed data stores	UC policy is defined centrally and applied across all 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	None	None	Support for all native, major public IM clients including GoogleTalk, Windows Live, AIM, and Yahoo!
Authentication & Authorization Services	Allow/block access at company, group, and user levels	Some additional policy configuration available	Policies at company, group, and user levels; Group-level ethical boundaries; IP address-based access controls; Access controls and monitoring options
File transfer management	Granular file transfer settings at company level only	Simple content inspection does not support regular expressions or match types	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	None	AV scanning of file transfers on OCS front end.	Support for Symantec, McAfee, TrendMicro, CA, ClamAV, Sophos, and Kaspersky. Zero-day worm blocking. Files are not scanned on OCS front end so no additional load.
SpIM blocking	Enhanced presence can filter on presence information	None	Content-based protection using white/black lists and custom rules
URL blocking	URL rewrite to remove hyperlink and/or add warning message	None	Domain-configurable and direction-configurable URL policies.
Federation management	Allow/block at company level and user level only	Allow/block at company level and user level only	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 presented only to external users in federated/PIC scenarios	Disclaimers presented only to external users in federated/PIC scenarios	Disclaimers sent inline and audited; disclaimer display controls at the IM network and group levels
Tamper detection	None	None	Guaranteed message order preservation; anti-tamper mechanism validates conversation integrity
File transfer capture	Captures names of transferred files only, not actual files	Captures names of transferred files only, not actual files	Files archived in database and shown in context in conversation review – single database deployment and reporting
e-Discovery retrieval	Requires a 3-database deployment, no built-in export of transcript data	None	Reports on IM usage, security violations, compliance violations, transcript reviews. Scheduling and auto-delivering available.

A-DS-010-VANTAGE-OCS-0111