



OpenText™ AXS-One Supervision Archive

The OpenText AXS-One Archive lowers organizational costs and risk by providing the ability to confidently and systematically respond to a broad range of compliance requirements, investigations and litigation. Financial institutions are continually challenged with the requirements of new regulations, as well as corporate mandates to protect data privacy. The OpenText AXS-One Archive addresses these challenges through the Supervision module.

Meet SEC/FINRA Supervision Demands

The OpenText AXS-One Archive makes it easy for you to meet SEC/FINRA and other compliance demands through Supervision, allowing policy-based review post distribution of email, instant messages and attachments in support of your organization's policy requirements. Content from every archived email, IM and attachment is scanned for specific keywords you identify. When suspicious content is found, archive workflows automatically route the message to the appropriate supervisor's queue for review. Supervisors then review and approve messages in bulk or individually, reject any or all items or escalate for further review. Review criteria, processes and roles are highly configurable based on policies defined by the organization.

Reporting and Auditing

Online reports can be generated in real time, enabling reviewers and supervisors to monitor the process, enabling organizations to stay on top of their compliance and risk exposure. The workflows of the AXS-One Archive maintain a complete audit history for every message. This translates into an electronic process chain of custody for every email, instant message and attachment.

BENEFITS

- *Enforce corporate policies for regulatory compliance and corporate governance*
- *Reduce the time and cost associated with legal discovery requests*
- *Effectively manage data as part of an overall information governance strategy*
- *Reduce the cost of the IT storage infrastructure*

OpenText AXS-One Supervision Archive provides secure preservation of messages and enables an auditable chain of custody for every message and attachment, helping to enforce governance and legal discovery policies.

Benefits of Supervision

- **Reduce messaging risks**
Automated content scanning helps deter employees from engaging in correspondence that violates corporate policies and regulations.
- **Support for regulatory audits**
Highly configurable review criteria, processes and roles enable supervisors to review/approve/reject messages in bulk or individually, or escalate for further review.
- **Scalability**
Configurable for small departments through global enterprises, supporting multiple email infrastructures.
- **Content filtering and surveillance**
Process automation capabilities detect undesirable and confidential content using keyword and phrase triggers for audit, risk management and remedy.
- **Secure preservation of messages with full audit trail**
Records are secured and preserved in their original format and all user activity is logged.

Key Capabilities of the OpenText AXS-One Archive

- **Policy-Driven**
The OpenText AXS-One Archive is purpose-built to enforce policy-driven archiving in support of information governance, regulatory compliance and eDiscovery processes. Policies are also available to address key storage issues, such as server backups, restores, quota management and capacity planning.
- **Retention Management**
The retention and destruction of all archived records is based on configurable policies. A complete chain of custody is created and maintained, which can be used to prove the exact process and physical location of files throughout their lifecycle.
- **Regulatory Compliance**
Capture all or selected messages (inbound, outbound and internally delivered) for specific users before they are delivered to a recipient's mailbox. Irrefutable data is captured and stored within the archive, maintaining an auditable chain of custody for every message and attachment, helping to enforce governance and legal discovery policies.
- **Secure Activity Logs**
The security of data is a key concern for IT and business users. Simple changes to log rotation activities can push logs to the archive for secure and managed retention. Using standard technologies to convert the logs into structured files, the content can be indexed and used by compliance and security teams to detect unauthorized access and hacking events, leading to improved security for the organization.