MANTECH™
ALWAYS ADVANCING

Beyond the Send Button: Sentris® Protection for Microsoft Exchange & Outlook

Policy-driven enforcement for secure communications

Email is often the most vulnerable point for data spills in any organization. You need to know that your communications are secure without having to guess if a recipient is authorized or if an attachment is properly marked. **Sentris Protection for Exchange & Sentris Labeling for Outlook** provides that certainty through a unified, two-part system. By combining client-side labeling with automated enforcement at the server, Sentris ensures your emails, calendar events, and tasks are always classified correctly and delivered only to those authorized to see them.

Integrated Labeling and Protection

The Sentris Labeling Add-in integrates directly into your Microsoft Outlook ribbon, making the classification process a seamless part of your workflow.

Mandatory Marking on Send: To prevent unmarked data from leaving your outbox, Sentris requires a classification for every new email, reply, or forward. This protection extends beyond your inbox to include your Outlook Calendar events and Task assignments, ensuring a total security first approach.

Intelligent Attachment Roll-Up: You don't have to manually calculate the highest security level for your message. When you attach Sentris-marked files, the system automatically scans them and rolls up the email's overall classification to match the most sensitive attachment. It can even be configured to block unmarked attachments from being added in the first place.

Active Mailbox Filtering: Sentris works in the background to ensure even your view is protected. By applying a persistent filter, Sentris automatically hides items that exceed your current personal, facility, or network clearances. Your inbox always reflects exactly what you are authorized to see in your current context - nothing more, nothing less.

Automated Server-Side Enforcement

While client-side labeling occurs in Outlook, Sentris Protection for Exchange serves as the security checkpoint on the server, enforcing strict access controls before an email ever reaches a recipient.

Real-time Message Interception: Sentris intercepts every email as it flows through the Exchange Transport Service. It acts as a real-time validator, ensuring that policy is enforced at the server level, regardless of the user's device.

Recipient Validation: You no longer have to worry about accidentally cc-ing someone who isn't authorized for the content or attachments in your email. Sentris checks every intended recipient's clearances against the email's classification. If someone isn't authorized for the data, Sentris dynamically removes them from the delivery while allowing the message to proceed safely to those who are.

Sender Notifications: If a recipient is removed from your email, Sentris immediately notifies you. You'll receive an automated Validation Failure email detailing exactly who was denied access, along with a copy of your original message, so you can adjust your communication and stay on mission.

Digital Signatures & Encryption Enforcement: Sentris can be configured to require native Outlook digital signatures or message encryption to comply with your organization's security policies. If a message fails to meet these specific cryptographic standards, Sentris will reject it, ensuring only verified, trusted traffic is permitted.

Securing Your Enterprise Communications

By embedding directly into your email workflow, Sentris translates mandates like Zero Trust and CUI handling into clear, predictable operations. You and your team can focus entirely on the mission while your sensitive data remains protected from the moment you hit Send - ensuring every message, attachment, and calendar invite is verified before it ever leaves the organization.

LEARN MORE: MANTECH.com/products/sentris • Commercial.Services@MANTECH.com