

Sentris® Protection for CUI Environments

The Smarter Way to Manage CUI Policies and Markings

Protecting Controlled Unclassified Information (CUI) is critical to mission success, yet staying compliant while preventing data leaks remains a constant challenge for many organizations. Sentris simplifies this process by pairing user-friendly data labeling with a precise, multi-layered security framework. Built for Windows-based networks, it maximizes the power of your current Microsoft ecosystem while giving your organization the flexibility to scale and adapt your CUI enforcement as organizational and federal policies change.

Intelligent Governance

Integrating directly into your current network infrastructure, Sentris provides powerful, rule-based governance to enforce both CUI requirements and your own custom organization classification rules.

- **Enterprise-Wide Definition:** Define the precise types of sensitive information authorized to be processed across your Microsoft Windows networks.
- **Dynamic Authorization:** Authorize users, facilities, and networks for specific control markings based on your metadata definitions.
- **Intuitive Labeling Utilities:** Equip users with easy-to-use tools to consistently apply the correct CUI labels across Office files, emails, and various file formats.
- **Granular Access Control:** Lock down and control access to information based upon its associated security label.
- **Cross-Boundary Sharing:** Establish trusted connections with external organizations to securely share protected information across organizational boundaries.

Your Blueprint for CUI Compliance

Achieving compliance requires mapping federal mandates directly to your network operations. Designed to support the DoD Risk Management Framework (RMF) Baseline + Accessibility Overlay requirements, Sentris meets or exceeds the strict confidentiality mandates specified for CUI and classified networks (including NIST SP 800-171). No matter what category of regulated or proprietary data your organization processes, Sentris provides the capabilities needed to manage your CUI readiness strategy across three distinct operational phases:

- **Establish Your CUI Framework:** Define your specific CUI registry requirements and custom organizational categories using the Sentris Administration Tool. This creates a centralized, enterprise-wide policy baseline that governs how sensitive data is authorized to be processed across your network.
- **Enforce CUI Markings:** Eliminate guesswork from user workflows. Sentris guides the user via a wizard interface to automatically apply the required safeguarding labels, coversheets, and distribution statements to their Microsoft Office files.
- **Control CUI Dissemination:** Meet strict NIST and DFARS dissemination mandates by locking down data boundaries. Sentris evaluates user, facility, and network clearances in real time, enforcing rule-based parameters to ensure CUI is only exchanged with authorized personnel, whether collaborating internally or sharing across organizational boundaries.

Driving the Shift

Sentris simplifies complex data classification, making it easier to share information securely and allowing system security officers to enforce user and organizational access control. By ensuring consistent labeling of classified information and CUI, it accelerates replacing “need to know” with “responsibility to provide.”

