Security and Audit (SA)

- Tracks and traces data changes including pre-authorization of actions to ensure proper permissions
- Provides tighter control over the manufacturing process
- Produces secure storage and record control for electronic records per 21 CFR Part 11
- Provides a full audit trail history of production data collected
- Configurable—no programming
- Enables a single network of security measures
- Uses encryption and check sum data protection routines to secure information
- Reduces errors, omissions and deviations
- Interfaces with existing user directory domains
- Group based permissions to simplify management

**Introduction**

Security and Audit (SA) provides controls for individual or multiple Syncade™ Smart Operations Management applications. In FDA-regulated industries, SA ensures that your Syncade Suite system is 21 CFR Part 11-compliant. In all industries, it provides complete security services, such as user authentication, electronic signature and transaction activity control that must be logged to an audit trail.

**Benefits**

**Robust Password Policy.** SA features a Password Policy control function that allows the system administrator to set rules for user passwords, such as maximum number of failed login attempts a user is allowed before being rejected from the system. In addition, the Password Policy editor can force alpha/numeric and mixed-case controls for user passwords to make system tampering even more difficult. Other Password Policy controls include the number of days a password is valid before it expires and the minimum length of a password. Users can be imported and authentication can be performed through Microsoft Active Directory or equivalent systems. This integration allows for a single network of application identification and authentication.
Regulatory Compliance. For the FDA-regulated industries, SA enables and facilitates 21CFR Part 11 compliance for electronic records and signatures. Off-the-shelf functionality controls all transactions that insert, update, or delete documents, records, or data. Each event is logged to the transaction database for auditing purposes. This easy-to-set-up user control capability is a tremendous benefit during plant inspections by regulatory agencies.

Audit Trail. The audit trail function provides a complete, unchangeable view of transaction activity. SA collects, reports, and maintains all required data for complete traceability, as well as operator and personnel application data. The system administrator can be electronically notified of activity.

Ease of Permission Configuration. All industries benefit from the security that SA provides. User authentication ensures your system is accessed only to those with proper permissions. SA also provides various levels of permission through a simple configuration engine. Check boxes allow quick and easy setup of groups permissions. Your Syncade Suite system can be as flexible as you desire ranging from using current logons to perform actions (no e-signature) or requiring e-signatures for every action.

Product Description
Entities are the basic building blocks of the SA application. Entities are objects or processes that are defined for each of the Syncade applications, and these entities are how SA controls the way users interact with the applications. Every entity has a unique name identifying a particular object or process within a Syncade application. SA allows organizations to define permissions for each entity. These permissions allow users to add, delete, modify, read, print, or use the object or process defined by the SA entity. When a user attempts to perform an action, SA is notified and determines if the user is authorized to perform that action. Once the user has been authorized, the data within the database is updated accordingly. The activity is also recorded in the audit trail, which cannot be altered. Any attempted tampering with the audit trail database will trigger a notification to a designated administrator.

Organizations using SA are able to define their own security needs throughout the Syncade applications. SA supports various authentication methods including two-token authentication (a user name and password), one token (just password), or no authentication (the current user will be logged as performing that action). This flexibility allows the user organization to tailor application security for their specific requirements.

SA can be integrated with third party user systems, can be used as the sole user authentication application, or a combination of both. Keep internal employees in your current system while providing customers, vendors, etc limited access to only what they require through SA. DeltaV domains in SA are also supported.

SA, when used with the other Syncade applications, is the engine for controlling and securing electronic data collection for manufacturing operations.

Other Syncade Smart Operations Management Applications
- Equipment Tracking (ET)
- Electronic Batch Record (EBR)
- Materials Management (MM)
- Batch Production Records (BPR)
- Training & Development (TD)
- Recipe Authoring (RA)
- Document Control & Archiving (DCA)
- Weigh & Dispense (WD)
- Manufacturing Information Portal (MIP)

General System Requirements
A server class PC with Internet Explorer is needed to support the Syncade solution. Microsoft SQL Server is the underlying database. Please consult the factory for further details regarding hardware requirements and software versions.
All Syncade applications use SA for security authentications and audit trails.

Security and Audit policies are easy to set up.
Security and Audit policies are easy to set up.

To locate a sales office near you, visit our website at:  www.EmersonProcess.com/Syncade
...or call us at:  Asia Pacific: 65.777.8211
Europe, Middle East: 41.41.768.6111
North America, Latin America: +1 800.833.8314 or
+1 512.832.3774
...or email us at:  Syncade@Emerson.com