INEO
Controlling Access

SecureEscorts Data Sheet

SecureEscorts from INEO solves complex Carrier Network Operation Centers (CNOC) issues by assigning security privileges by user in a central location and tracking activity in easy-to-access reports. It is an industry leading Access Control solution designed for CNOC's.

SecureEscorts provides authorized device access management to devices that use the following interface methods:
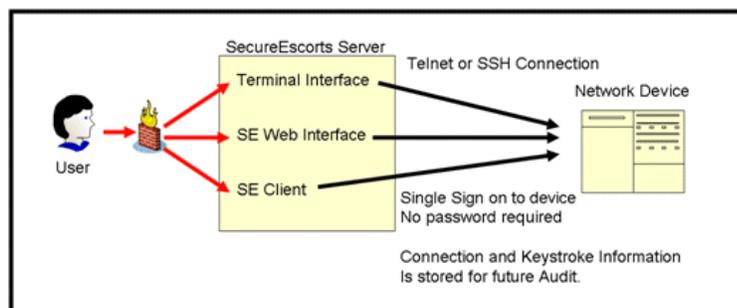
» TCP/IP Accessible Intermediary devices that convert protocols, such as terminal servers and protocol converters.
» GUI interfaces, or vendor Element Management System (EMS) application or Operational Support System (OSS).

It provides the capability to manage Escorted Access (Single Sign-On with session capture) to all Telnet, SSH, and mediated synchronous, asynchronous, and serial interface devices.

SecureEscorts provides a rules-based authorization engine that allows the customer's administrator(s) to define the profiles for both users and devices at a granular level. An administrator can manage these profiles to establish access rights for each user on a per device basis allowing for fine-grain access control. The administrator can also define and configure controls on user groups and device groups to establish time constraints, auditing controls, password constraints, filtering controls, and access rights.

INEO USA

92 Cornerstone Dr
Suite 145
Cary NC   27519
Ph: 919-467-2199
info@ineousa.com

Once the administrator has created profiles, users cannot bypass SecureEscorts to access a targeted device directly. SecureEscorts is the only source that knows the device's account and password information, forcing the user to be authenticated via SecureEscorts before being granted access privileges to any device. After authenticating the user, it then grants access to a limited set of devices to which the user has been authorized.

SecureEscorts provides summary reports on user sessions as well as detailed keystroke capture auditing files. In combination, these reports and files provide the most granular level of record maintenance for user-to-device sessions and the activity that occurred within each session. The auditing capabilities within SecureEscorts can be turned on or turned off on a per device or per user basis. When pre-engineering the system, the customer can define the amount of storage space required for on-board record storage. These records can be stored within SecureEscorts for a defined number of days and also be exported to external storage mediums for archiving and future retrieval.

Additional Benefits of SecureEscorts

» Designed to be platform- and vendor agnostic with regard to the end device or the EMS platform. SecureEscorts can secure access to devices as long as those devices are direct IP accessible using telnet or SSH interfaces; synchronous, asynchronous, or serial interface accessible through a mediation device; or accessible through most standards-based (windows, HTTP/S) GUI interfaces.

» Provides a security policy engine that is rules enforceable and controllable. These rules are based on user and device profiles, which can be easily established within the system by the customer's administrator(s). The policy engine allows for fine-grain authorization control and administrative management on a per user and per device basis.

» Allows administrators to effect mass changes – including suspension of users as in the case of groups of contractors.

» Allows the customer's administrator(s) to establish a hierarchical structure of users, user groups, devices, and device groups to which permissions can be applied at a granular level.

» Quick and easy set up with data available for use immediately after install.

For additional information please contact info@ineousa.com