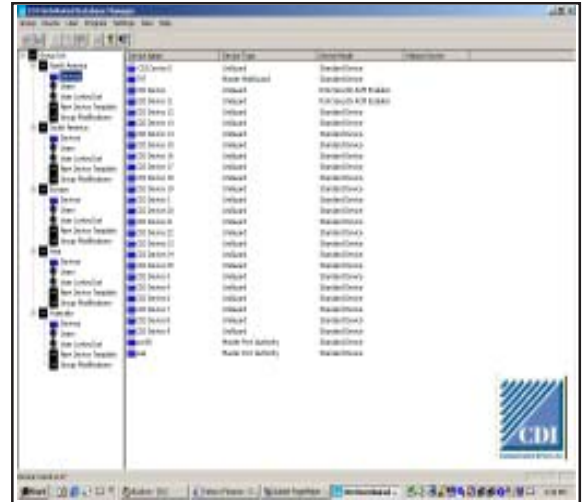




Distributed Database Manager DDM

- ✓ Central key management
- ✓ Windows XP/2003
- ✓ Performs updates automatically
- ✓ Updates are AES Encrypted
- ✓ Multiuser network capable
- ✓ Presents real time status info on network connected devices.
- ✓ Point and click technician device access
- ✓ Retrieves audit trail and reports



The problem

Managing a system of widely dispersed security devices can prove a daunting challenge. Making sure the user database and operating parameters of each unit is up to date can be an overwhelming job without a central management system. Managing each remote unit one at a time can be time consuming and problematic.

The Solution

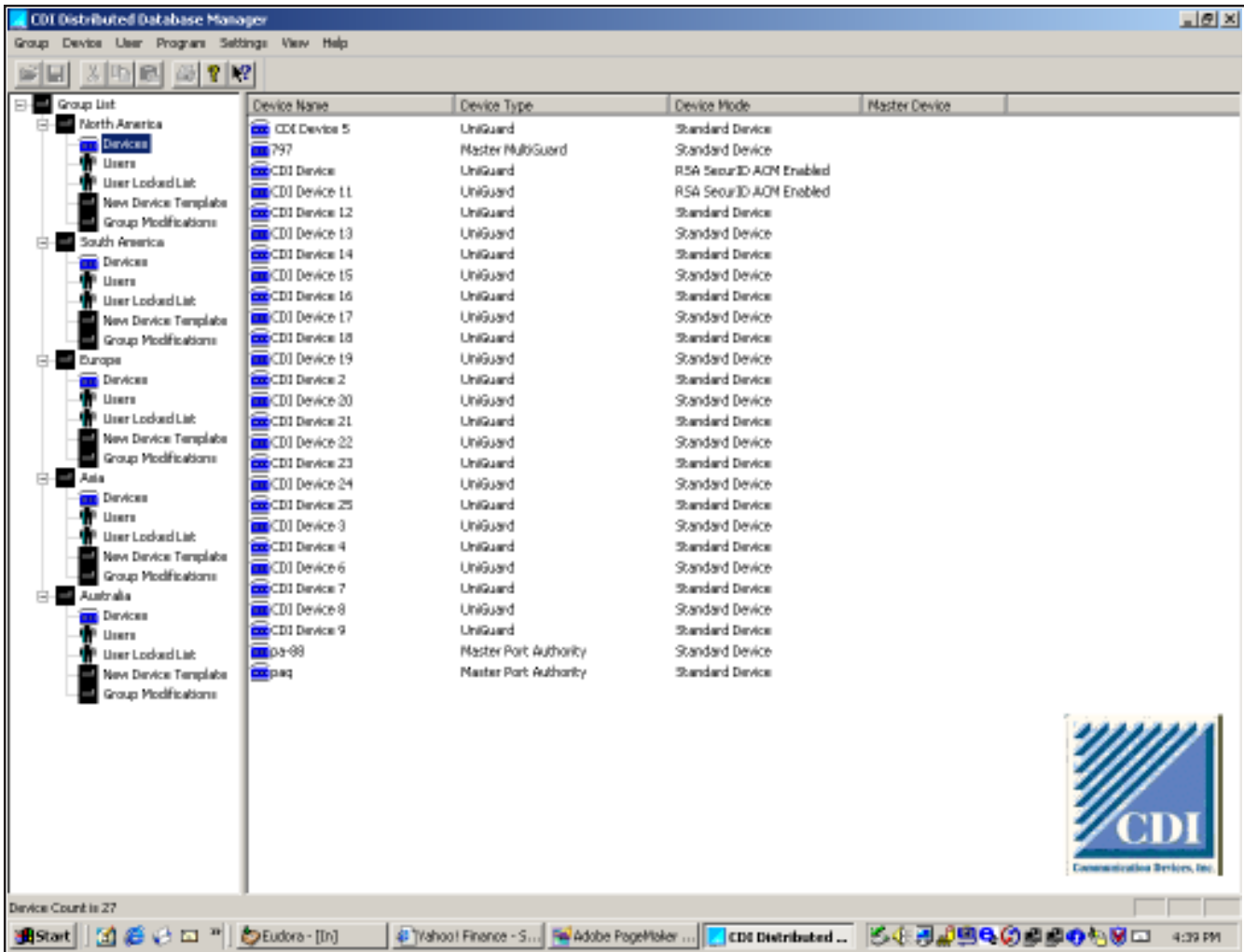
The DDM, Distributed Database Manager, can maintain an unlimited number of CDI devices at remote locations from a single or multiple workstations. This eliminates the need to update each unit individually whenever there is a database change. The system automatically maintains the database of each device and is capable of downloading the entire database of units. This process can be performed manually or set to occur automatically at periodic intervals.

Scalable

The database comes in two scalable formats. An ODBC version for single workstation applications and an SQL version for multiuser and multisite applications (disaster recovery and backup).

Security

Uploads and downloads are fully encrypted using AES encryption to prevent interception of the security credentials for the device.



Application

The above diagram shows the main DDM screen that enables the Security Administrator to enter GROUPS, USERS and DEVICES along with their security information into the Database. The Administrator can also select the information to be monitored in the Audit trail. Simple point, click, drag, and drop are used to make this a very user friendly application. Multiple groups allow for segmenting of the deployed field units. In this case a global network is divided geographically by continent.

The Security Administrator

The Security Administrator needs only to maintain one database at the central site and add or delete users as required from the database in the DDM. Multiple DDM's can access a single database over a network to provide multiple users access to the manager.

The Operations Personnel

Operations personnel can access remote devices through the Secure Session Manager (SSM) which is bundled in with the DDM. The SSM allows Operations personnel to use the database to access remote devices without compromising any of the security credentials. This separates Security from Operations and streamlines the system when remote sites need to be accessed. Multiple simultaneous usage of SSM can be accomplished with additional seat licenses.