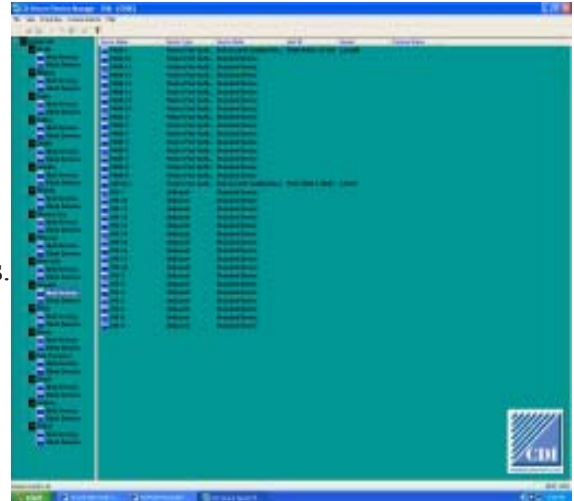




Secure Session Manager

Secure Out Of Band Management Operations Tool

- ✓ Presents authorized technician with a view of all devices in DDM database.
- ✓ Prevents technician from accessing any security credentials in database or devices.
- ✓ Allows technician Secure Out of Band Access to devices in database.
- ✓ Allows Technician to power control remote devices.
- ✓ Provides keystroke logging for Sarbanes Oxley.
- ✓ Multiuser network capable via SQL database.
- ✓ Windows XP/2003 compatible.
- ✓ Allows 3DES/AES Encryption via CDI hardware.
- ✓ Provides remote access via network or dial-up



The problem

To provide “NOC” technicians a quick (point and click) method for access to remote secure out of band management devices without compromising the embedded security credentials in the local DDM database.

The Solution

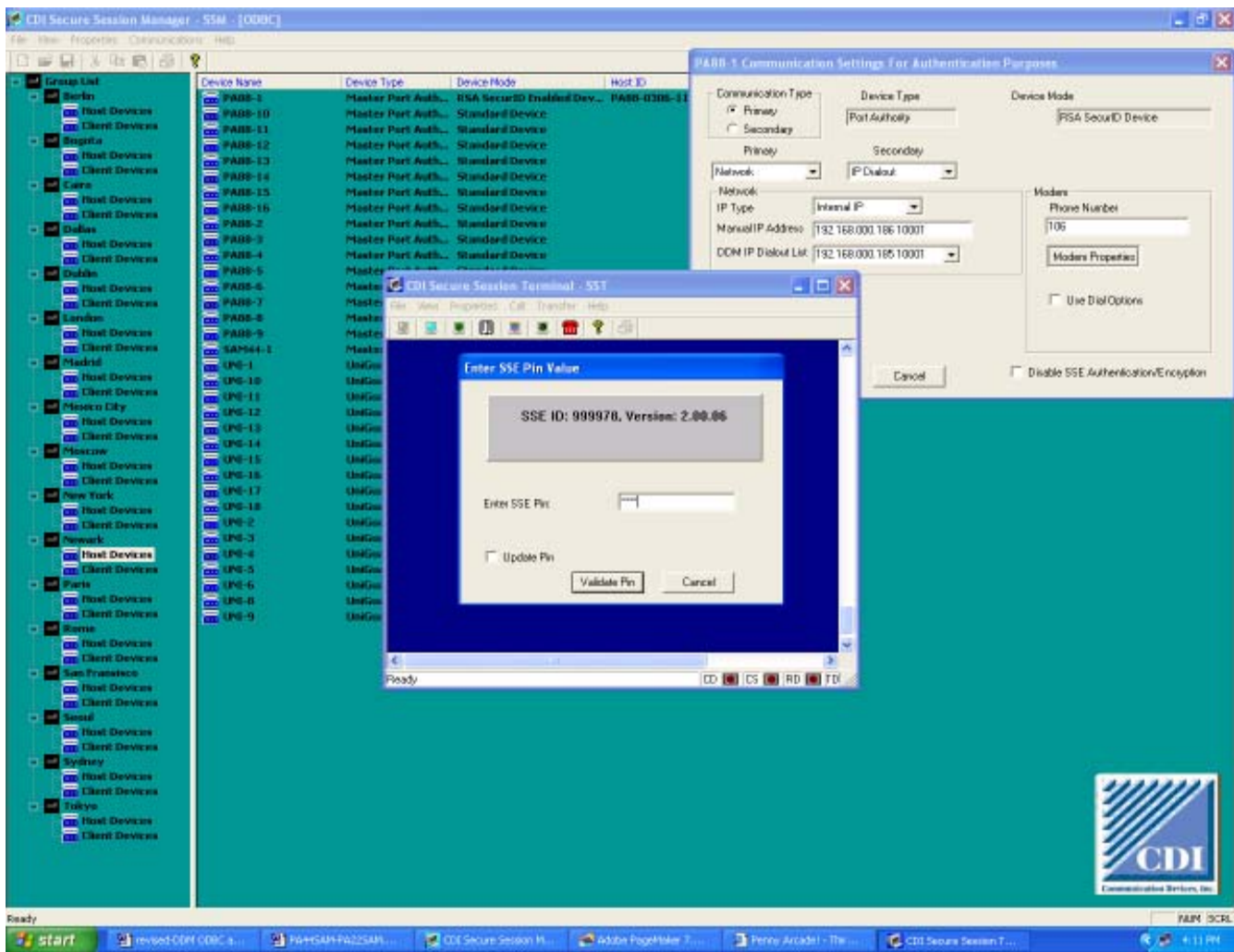
The SSM, Secure Session Manager, is a client based software program that can provide technician access to the secure DDM database, allowing only access to the connection information for the devices. The technician will not be able to view or modify any security credentials concerning the devices or users in the database. This will allow the technician to point and click on any device to establish secure remote access via network or PSTN. The technician still has to go through whatever authentication or possible encryption that has been setup in the device for access.

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

The technician is securely authenticated to the database and to any remote device via pre-established security parameters.



Application

The main SSM screen enables the Technician to access GROUPS and DEVICES by only providing their connection information in the database. The technician can point and click on any device and be prompted for network or dial-up connection using whatever security is defined in each device. Keystroke logging can be enabled for Sarbanes Oxley compliance.

The SSM can communicate securely via hardware 3DES/AES encryption with any CDI device in the database.

The Security Administrator

The security administrator determines what technicians have access to the database and which devices each technician will be allowed access to.

The Operations Personnel

Operations personnel can access remote devices through the Secure Session Manager (SSM) which is bundled in with the DDM. The DDM allows Security personnel to use the database to access security credentials of the devices in the database. 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.