WHY ACCUTEL FOR SECURITY »

REGARDING SECURITY MANAGEMENT

- The CONTEX Summit system by Compunetix is an embedded operating system that was designed specifically for collaboration applications. The CONTEX Summit is based on an optimized conferencing platform that was designed from inception to provide high-quality, reliable conferencing under high volume environments.
- The CONTEX Summit applications use a proprietary messaging scheme for communication on designated ports. All other ports are not externally accessible. The VoIP interface is separate from the application data interface to ensure the highest level of security.
- The CONTEX Summit utilizes SSH and SFTP protocols for administration and proprietary protocols for monitoring.
- Maintenance and application passwords are changed on regular intervals based on security best practices.
- The Summit system allows the WOC and MC client software to connect and communicate using TLS encryption. This option improves the security of communications between the CONTEX Summit system, the WOC and MC client applications. In addition, the CONTEX Summit can be configured to choose AES or ARC4 encryption algorithms for communication.
- As a non-window based architecture, the platform is designed to be impenetrable by potential viruses and intruders.
- Security was a top priority in the design of the CONTEX Summit conference bridge.

CONFERENCE SECURITY FEATURES

The CONTEX Summit by Compunetix has a full suite of features that allow conferences to be tailored to the specific needs of the host. Some of these features include:

Different Host and Guest Passcodes

To prevent fraudulent use, the system can be configured so that only the Host passcode allows the conference to begin, acting as the "key" for the conference. Guests dialing into the conference will hear hold music before the Host arrives.

Conference Security

The Host may choose to lock or secure their conference. When a conference is secured, an operator and additional parties attempting to join the conference will not be permitted access. Hosts can secure or unsecure the conference by entering *7 on a touch tone phone.

Double-Passcode Entry

Unattended conferences may be configured to require all parties to enter a passcode for access to the conference and then require the Host to enter a confirmation DTMF key sequence. After the caller has been identified as the Host, they are required to enter an additional passcode to activate the conference. This dramatically reduces the opportunity for fraud or uninvited guests.

Conference Level Passcodes

With this feature, a conference Host can specify a Conference Level Passcode (CLP). The CLP feature increases security by forcing callers to enter a second-level passcode to enter an unattended conference. The conference Host/chairperson of an unattended conference has the ability to uniquely and immediately define this passcode during the conference call, which is particularly useful in recurring conference calls that require exclusivity.

Host Disconnect

The system can be configured to automatically end the conference if the Host disconnects. This feature provides extra security and lost control by not allowing a conference to continue after its Host has disconnected.

Silent Intruder Detection

If a participant does not record their name and company upon entry into the conference, the system plays the message "Name not recorded" to the conference as the party joins, thereby alerting the conference that someone has joined but did not record a name.

Project Codes

The CONTEX Summit supports the ability for the Host of a conference to enter a project code that is saved to the billing file on a per conference basis. The Host can enter the project codes either upon entry into the conference via touch tones or on the web at Accutel.com.

Dial-out Prevention

This feature specifies whether or not an unattended conference Host can dial-out to additional parties. In addition to being able to block this capability, the system also supports the ability to specify whether the Host can dial-out via DTMF on their phone, via the web only, or both.

The CONTEX Summit supports multiple methods for identifying participants that have joined a conference. One method is with Passcode/DNIS Meet-me plus PIN conferences. With passcode/DNIS Meet-Me plus PIN conferences callers must enter a PIN. The PIN is verified against a preset list of names and PINs associated with the conference, and the caller's information is then transferred to the Conference Control window of the WOC.

The CONTEX Summit also supports ANI lookup or blocking. With this feature, the system is configured to query an external database via the CONTEX Real Time Bridge Interface (RTBI) API to determine the associated party details for a particular ANI.
If the caller's ANI is found in the database, the caller details are populated based on the information received from the database. If the caller's ANI is not found in the database, the caller's details are not modified and the treatment for the caller is based on the configuration for invalid ANIs.

The advantage of the CONTEX Summit is its customizable security features that can be set at the company level or by the Host. Accutel understands the importance of privacy and security to our customers.