

---

## CyberData Corporation

2555 Garden Road  
Monterey, CA 93940  
United States  
[www.cyberdata.net](http://www.cyberdata.net)



CyberData Corporation is a manufacturer of peripheral devices for VoIP phone systems. IP Paging Speakers, Paging Gateways, IP Door Entry Control, SIP phone encryption devices, are some of the products we manufacture that add significant value to VoIP phone installations.

Business/Marketing Contact  
Bill Majerczak  
Director of VoIP Product Management  
831-373-2601, ext. 102  
[billm@cyberdata.net](mailto:billm@cyberdata.net)

Technical Contact  
Chris Elliot  
831-373-2601, ext. 122  
[celliott@cyberdata.net](mailto:celliott@cyberdata.net)

### SIP Speakers - Version 3.01

This IP-based paging solution solves the paging from a VoIP phone system problem by allowing you to use network-based paging which is easier to install, maintain, and manage.

<b>Interops with 3Com Platform</b>	<b>Model</b>	<b>SW Ver</b>	<b>HW Ver</b>
IP Telephony	VCX Connect	8.0	100 and 200
IP Telephony	VCX Connect	7.1.13e	100 and 200
IP Telephony	VCX System i	7.2.5	I Series
IP Telephony	VCX Enterprise	7.1.11c	X Series

---

# SIP User Agent Auto-Configuration

August 08

## 1 General Overview

The required SIP UA behaviours include the ability to:

- Locate a provisioning server (FTP, TFTP) via a record stored in the DHCP server .
- Typically the provisioning server IP address string is located at option 66.
- Pull/request a configuration file(s) from the provisioning server:
- Be notified that its configuration has changed and that it should poll the provisioning server to analyze the changes.
- Be software/firmware upgradeable via the provisioning server
- The SIP UA should compare the available firmware in the provisioning server against the firmware version it's currently running to determine if it needs to download and upgrade itself.

## 2 Typical Firmware and Configuration File Set

A SIP UA will typically request the following types of files from the provisioning server after locating its address from DHCP:

- firmware and bootrom file(s)
- system configuration file

- - One file that contains system-wide settings for all of the SIP UA's of that same type - per-phone configuration file
  - Each SIP UA that has been configured will have its own configuration file that contains information like the SIP UA's identity address, authentication, password, etc... - Corporate directory file (optional)
  - Some SIP UA's support downloading of a file that contains information about the corporate directory . - Images, audio (optional)
  - Only if the SIP UA has a display that is capable of displaying images or if it uses a standard set of audio files for notifications or system sounds - Logs (optional, push instead of pull)
  - Some SIP UAs support uploading of log files to the provisioning server for diagnostic purposes.

---

## 3 Provisioning Sequence

The new SIP UA is started and attempts to retrieve its configuration from the provisioning server. There are two cases to consider when the SIP UA contacts the provisioning server for its configuration files:

The provisioning server *does not* contain specific configuration file(s) for that particular device

The provisioning server *does* contain the specific configuration file(s) for that particular device

### 3.1 No previous configuration exists

If a device has not previously been configured using our administration user interface, there will be no specific configuration files in the provisioning server for that particular instance. In this case it will retrieve only the system configuration file(s) – the file(s) which contain general configuration information that applies to all instances of those SIP UAs in the network - which also contains dummy registration information that points the SIP UA to register with UC Server's notification SIP registrar. At this point, UC Server becomes aware of the SIP UA's presence on the network but the SIP UA is not really functional; it is in an "un-configured state". The initial configuration file points the SIP UA to a non-standard UDP Port 6000 for registration on UC Server using a dummy identity. This information is simply used to notify UC Server that a new SIP UA has been connected to the network so that the administrator can apply identities to it using the administration user interface (called UC Client).

### 3.2 A previous configuration exists

If a previous configuration exists, it is because the system administrator has configured an instance of aS IP UA using our administration user interface (see section 3 – Provisioning with UC Client). The SIP UA will simply pull its specific configuration file and load it according to the parameters within.

## 4 Assigning an Identity to a SIP UA using UC Client

SIP UAs can be provisioned automatically using the administration interface in UC Client. When an identity is assigned to a SIP UA using UC Client, the following occurs: 1. UC Server creates a configuration file specific to that instance of the SIP UA and copies it to the predefined provisioning server 2. UC Server notifies the SIP UA that it needs to reload its configuration. It notifies the SIP UA by: o Sending a SIP message to the SIP UA to indicate that it needs to reload its configuration – e.g. SIP NOTIFY with a special key -word used in the « event » flag (preferred) OR o HTTP -get/post sequence to the SIP UA web server to reboot the device so it reloads its configuration \*\*\*Alternate methods could be supported but will require some development effort.

## 5 Removing an identity from a SIP UA using UC Client

The same procedures are followed as in section 3. If, as a result of the identity removal, there are no more identities left on the SIP UA then UC Server will delete the per-instance configuration file in the provisioning server and thus theS IP UA will revert back to an un-configured state.

---

---