

# Cisco CUPS

## IM Logging



Defining UC Security

# About Sipera

- **Leader in real-time Unified Communications (UC) security**
  - Confidently deploy UC over any network
  - Award-winning UC-Sec appliances
- **VIPER Lab**
  - Proactive vulnerability research and assessments
- **Major Partners**
  - Avaya DevConnect Platinum
  - Cisco Development Partner
  - Microsoft Partner
  - Nortel Select Product
  - RSA Secured Partner



# Sipera Overview

## Sipera Solutions

### CONSULTING

Vulnerability analysis  
Risk assessment  
Penetration testing



**VoIP & UC  
Vulnerability Research**

### ENTERPRISE

Core Security  
Remote Users  
SIP Trunks



### COMPREHENSIVE UC SECURITY

Threat Protection	Access Control
Policy Enforcement	Privacy

VIPER Engine

Real Time  
Platform

Centralized  
Management

## Sipera UC-Sec Appliance

# Sipera CUPS Logging Architecture

- **Satisfies requirements for all regulatory compliance**

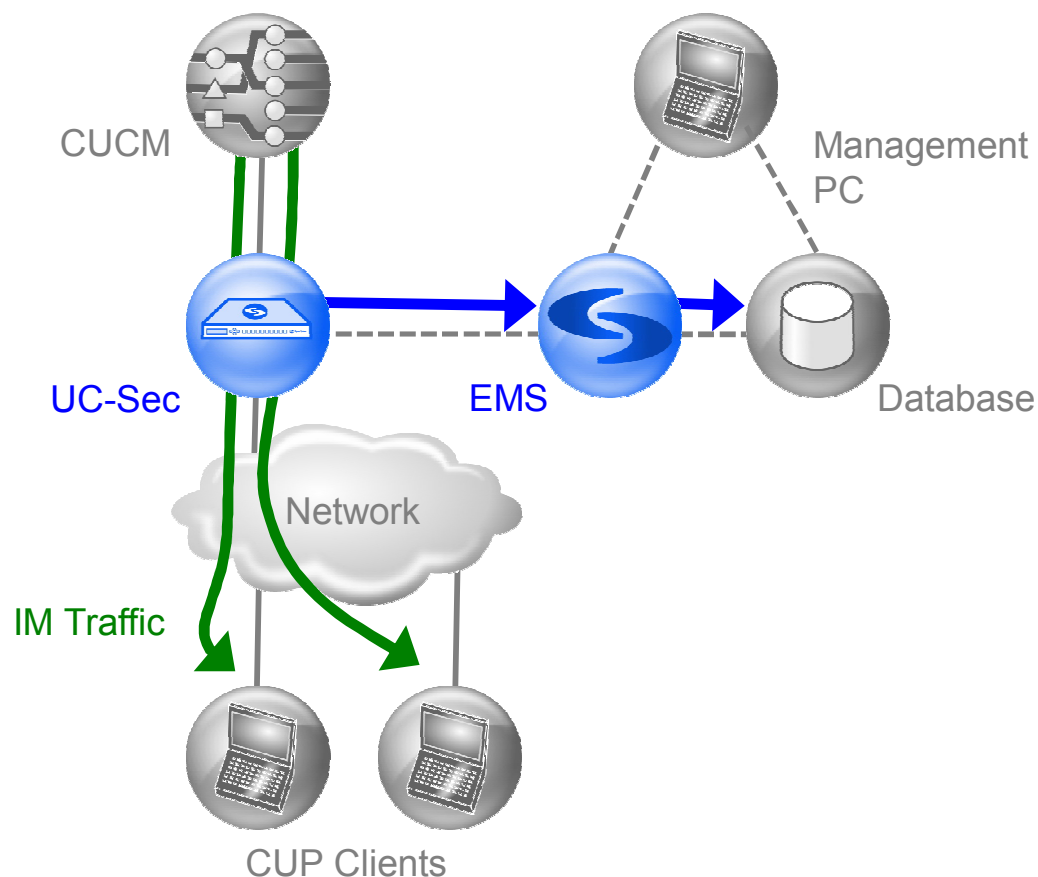
- Sipera UC-Sec is Cisco's only SIP compliance solution
- Logs all Instant Messages
- Has all required data, timestamp, users, communication etc

- **Simplifies Deployment**



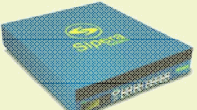
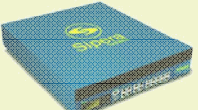
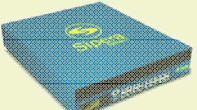
- Deployed between Cisco Unified Presence and Cisco Unified Personal Communicator
- Clients are automatically reconfigured for IM, presence and directory services

- **Simplifies Audits**

- All logs are exported to external SQL database
- GUI based log viewer
- External SQL queries viewer



# Sipera UC-Sec Appliances

	UC-Sec 100, 200, 500	UC-Sec 1000, 2000	UC-Sec 3000, 5000	UC-Sec 10000	UC-Sec 50000
UC-Sec Appliance					
Target Market	Branch / SMB	Small enterprise	Enterprise, Small Provider	Enterprise, Provider	Big enterprise, Provider
Registered users	100, 200, & 500	1k & 2k	3k & 5k	10,000	50,000
Simultaneous sessions	50, 100, & 250	375 & 500	750 & 1,250	2,000	10,000
IM Users	200, 400, & 1k	2k & 4k	6k & 10k	20k	100k

- **Sized based on registered users and simultaneous sessions**
- **Encryption affects sizing**

# Configuring

# Configure CUCM Cluster & Servers

- Add Cisco presence servers
- Configure the CUCM cluster

The screenshot displays the UC-Sec Control Center web interface. The browser address bar shows the URL `https://192.168.152.163/ucsec/j_secur`. The page title is "UC-Sec Control Center" and the user is logged in as "Admin". The current server time is 6:16:06 PM GMT. The interface includes a navigation menu on the left with options like "Welcome", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "SIP Cluster", "Cluster Proxy", "Device Pools", "Domain Policies", "Device Specific Settings", "Troubleshooting", "TLS Management", "IM Logging", "Archival Settings", and "Viewer Administration". The main content area shows the configuration for a SIP Cluster named "Dell-CUPC-Cluster". The "General" tab is selected, and the configuration is organized into sections: "Cluster Information" (Call Server Type: Cisco), "Security Information" (Secure Mode: Disabled), and "Miscellaneous Information" (IM Logging Only: Enabled, Domain Name: sipera.com, HTTP Domain: 192.168.151.161). Buttons for "Add Cluster", "Delete Cluster", and "Edit" are visible.

# Configure CUCM Device Pools

- Create a device pool
- Add or import devices

The screenshot shows the UC-Sec Control Center web interface. The breadcrumb trail indicates the current location: UC-Sec Control Center > SIP Cluster > Device Pools: CUPC-Pool. The interface includes a navigation menu on the left with options like Administration, System Management, and Device Pools. The main content area shows the configuration for the CUPC-Pool, including a table of associated devices.

Device Name	Device Type	User Name	Phone Type	Directory Number	IP Address	Registered To IP
UPCTEST03	Cisco Unified Personal Communicator	sateesh	work	000	Not Registered	Not Registered
UPCTEST04	Cisco Unified Personal Communicator	kommana	home	123	Not Registered	Not Registered
UPCTEST05	Cisco Unified Personal Communicator	test510	asdf	1234	Not Registered	Not Registered



# Configure Database

- Point to a Postgres or generic SQL server

The screenshot shows the UC-Sec Control Center web interface. The browser address bar displays the URL `https://192.168.152.163/ucsec/j_secur`. The page title is "UC-Sec Control Center" and the user is logged in as "Admin". The current server time is 6:16:58 PM GMT. The navigation menu includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Logout, Help, and About. The left sidebar shows a tree view of the system configuration, with "Archival Settings" selected under "IM Logging". The main content area displays the "Database Configuration" page, which includes a "Database Configuration" section with the following fields:

Database Configuration	
Upload logs to database?	<input checked="" type="checkbox"/>
Database Type	<input checked="" type="radio"/> Postgres <input type="radio"/> SQL Server
Database Address (ip:port)	10.0.0.103:5432
Database Name	savon
User Name	savon
Password	*****
Retype Password	*****

A "Save" button is located at the bottom of the form.

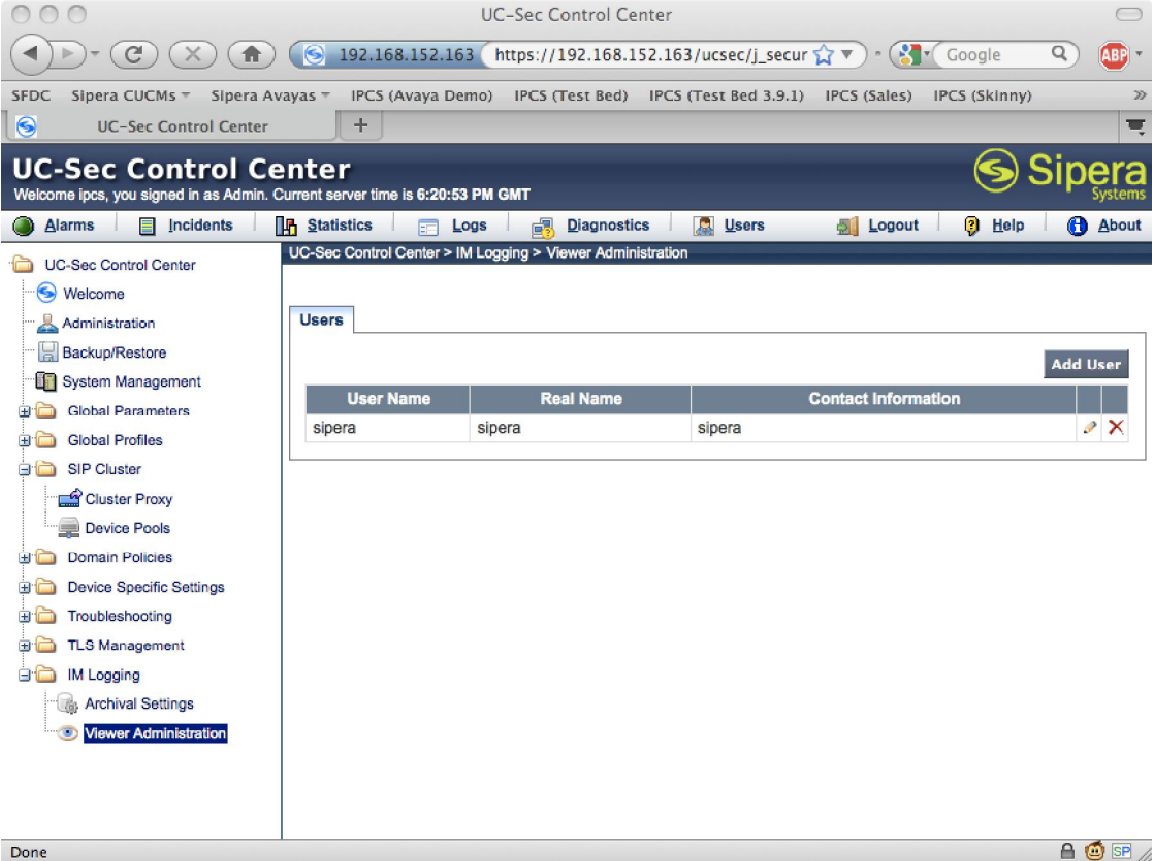
# Configure Upload Frequency

- IMs are transferred from UC-Sec appliances to EMS
- EMS then transfers IMs to database

The screenshot displays the UC-Sec Control Center web interface. The browser address bar shows the URL `https://192.168.152.163/ucsec/j_secur`. The page title is "UC-Sec Control Center" and the user is logged in as "Admin". The current server time is 6:14:32 PM GMT. The navigation menu includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Logout, Help, and About. The left sidebar shows a tree view of the system configuration, with "Archival Settings" selected under "IM Logging". The main content area shows the "Upload Frequency" configuration page, which includes a "Database Configuration" tab and an "Upload Frequency" section. The "Upload Frequency" section has three radio buttons for "Hourly" (selected), "Daily", and "Weekly". The "Time" field is set to "0:00" and the "Days" field has checkboxes for "Su", "Mo", "Tu", "We", "Th", "Fr", and "Sa". A "Save" button is located at the bottom of the configuration area.

# Configure IM Log Viewers

- Add users who are allowed to view IMs



# View IM Logs

- Log on to view IMs
- Filter based on user and / or time
- More complex reports view database queries

The screenshot shows the IM Log Viewer web application. The browser address bar displays the URL [https://192.168.152.163/im-viewer/\\_js](https://192.168.152.163/im-viewer/_js). The application header includes the Siper Systems logo and the text "IM Log Viewer" and "Welcome siper. The current server time is 6:22:28 PM GMT". Below the header, there are navigation links for "Users", "Logout", and "About". A search and filter section contains fields for "From", "To", "User Name", "Start Time", and "End Time", along with a "Run Query" button. The main content area, titled "Results", shows a table of IM logs with columns for "Time", "From", "To", and "Message". The table displays 10 entries, with a note indicating that 41 entries are available in total. The first entry is at 18:40 from sip:test05@sipera.com to sip:test03@sipera.com with the message "hi". The last entry is at 15:26 from sip:test03@sipera.com to sip:test05@sipera.com with a long message about branch parameter values. A "Done" status bar is visible at the bottom of the application window.

Time	From	To	Message
01/19/2010 18:40	sip:test05@sipera.com	sip:test03@sipera.com	hi
01/19/2010 18:40	sip:test03@sipera.com	sip:test04@sipera.com	hello
01/19/2010 15:29	sip:test05@sipera.com	sip:test04@sipera.com	Bye
01/19/2010 15:29	sip:test04@sipera.com	sip:test05@sipera.com	NP
01/19/2010 15:29	sip:test05@sipera.com	sip:test04@sipera.com	Any update on #12456
01/19/2010 15:28	sip:test05@sipera.com	sip:test04@sipera.com	Hello
01/19/2010 15:28	sip:test04@sipera.com	sip:test03@sipera.com	Is the call routed towards Core
01/19/2010 15:28	sip:test03@sipera.com	sip:test04@sipera.com	hello This is Sonus
01/19/2010 15:26	sip:test03@sipera.com	sip:test05@sipera.com	The branch parameter value MUST be unique across space and time for all requests sent by the UA. The exceptions to this rule are CANCEL and ACK for non-2xx responses. As discussed below, a CANCEL request will have the same value of the branch parameter as the request it cancels. As discussed in Section 4.7.4.4.2...

# SIMPLE Example

---

MESSAGE sip:94167601111@192.168.1.36 SIP/2.0

Call-ID: c3eF6f58-363323Cd-8058EB88-10307033@192.168.1.47

Contact: <sip:9057403000@192.168.1.47:5060>

CSeq: 196 MESSAGE

From: <sip:9057403000@192.168.1.47>

To: <sip:94167601111@192.168.1.36>

Via: SIP/2.0/UDP 192.168.1.47:5060;branch=z9hG4bKkdjuw732

Accept: application/sdpMax-Forwards: 70

Content-Type: text/plainContent-Length: 28

This is an Instant Message