Cisco CUPS

IM Logging

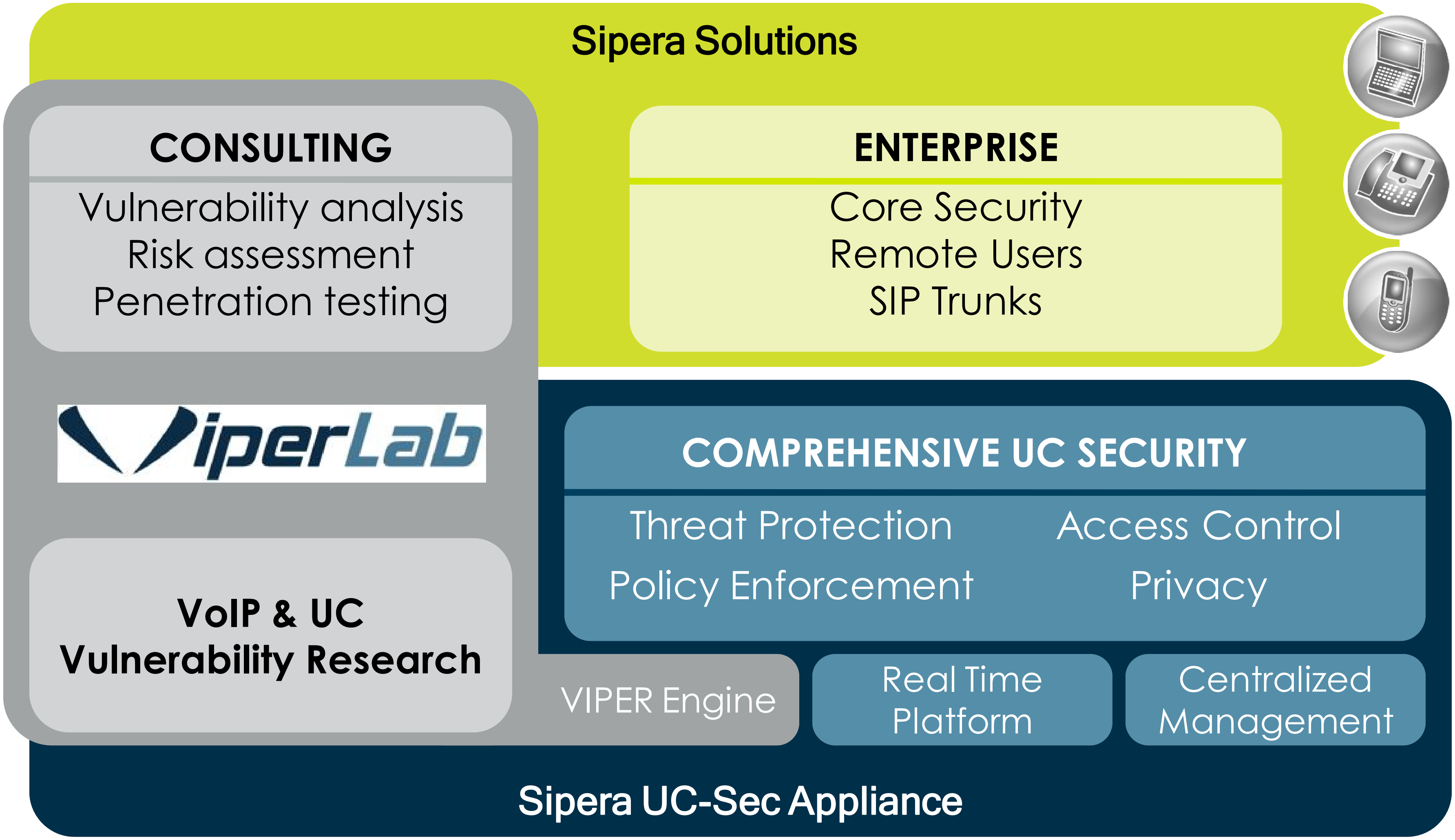
Sipera™ Systems

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

ENTERPRISE

Core Security
Remote Users
SIP Trunks

ViperLab

VoIP & UC Vulnerability Research

COMPREHENSIVE UC SECURITY

Threat Protection
Access Control
Policy Enforcement
Privacy

VIPER Engine

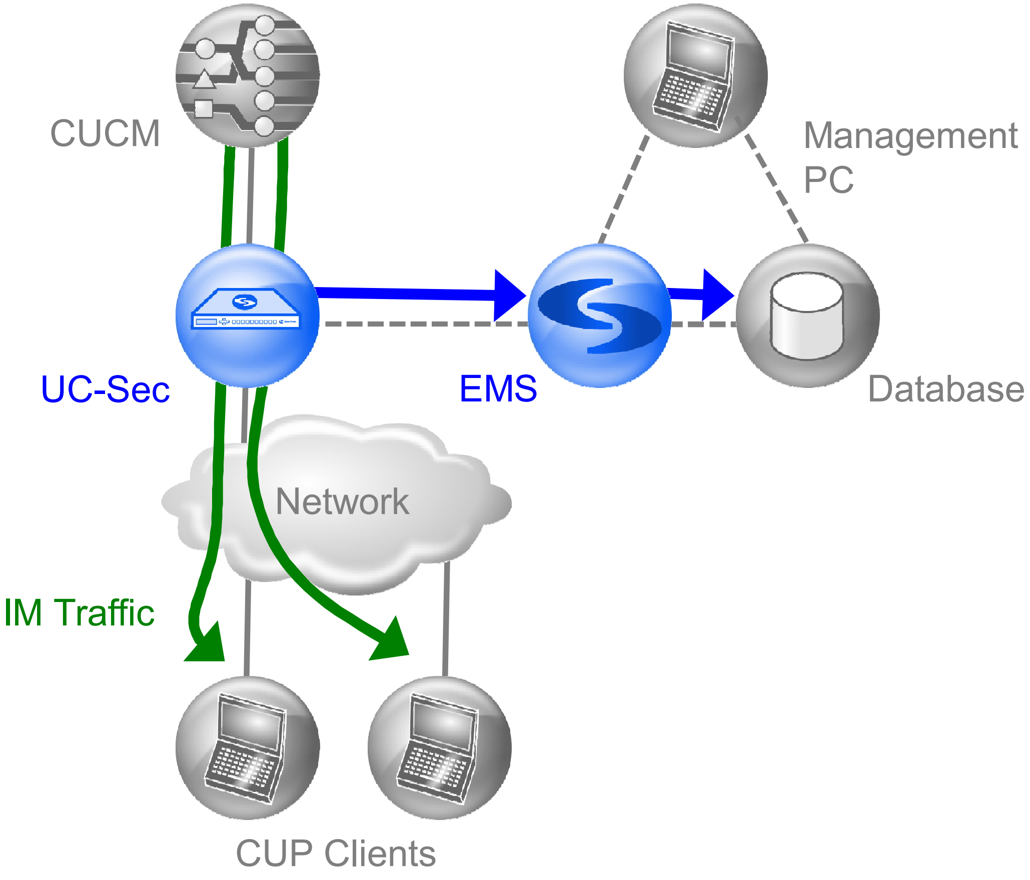
Real Time Platform

Centralized Management

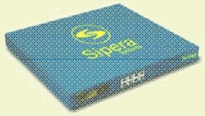
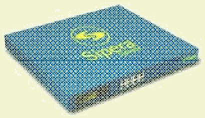
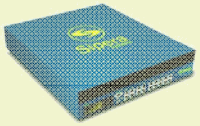
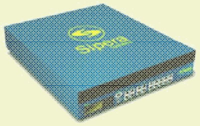
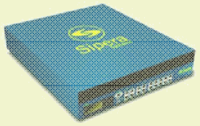
Sipera UC-Sec Appliance

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

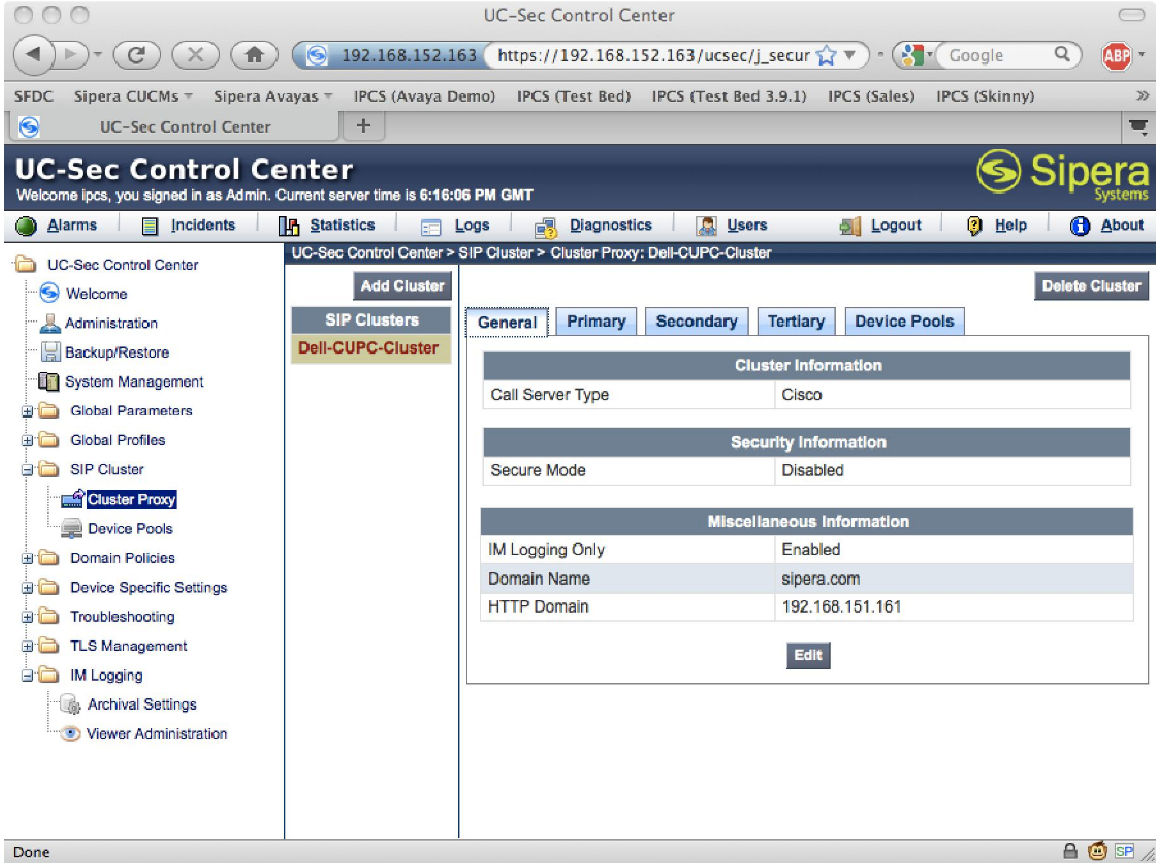
	UC-Sec 100, 200, 500	UC-Sec 1000, 2000	UC-Sec 3000, 5000	UC-Sec 10000	UC-Sec 50000
UC-Sec Appliance					
Target Market	Branch / SMB	Small enterprise	Enterprise, Small Provider	Enterprise, Provider	Big enterprise, Provider
Registered users	100, 200, & 500	1k & 2k	3k & 5k	10,000	50,000
Simultaneous sessions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



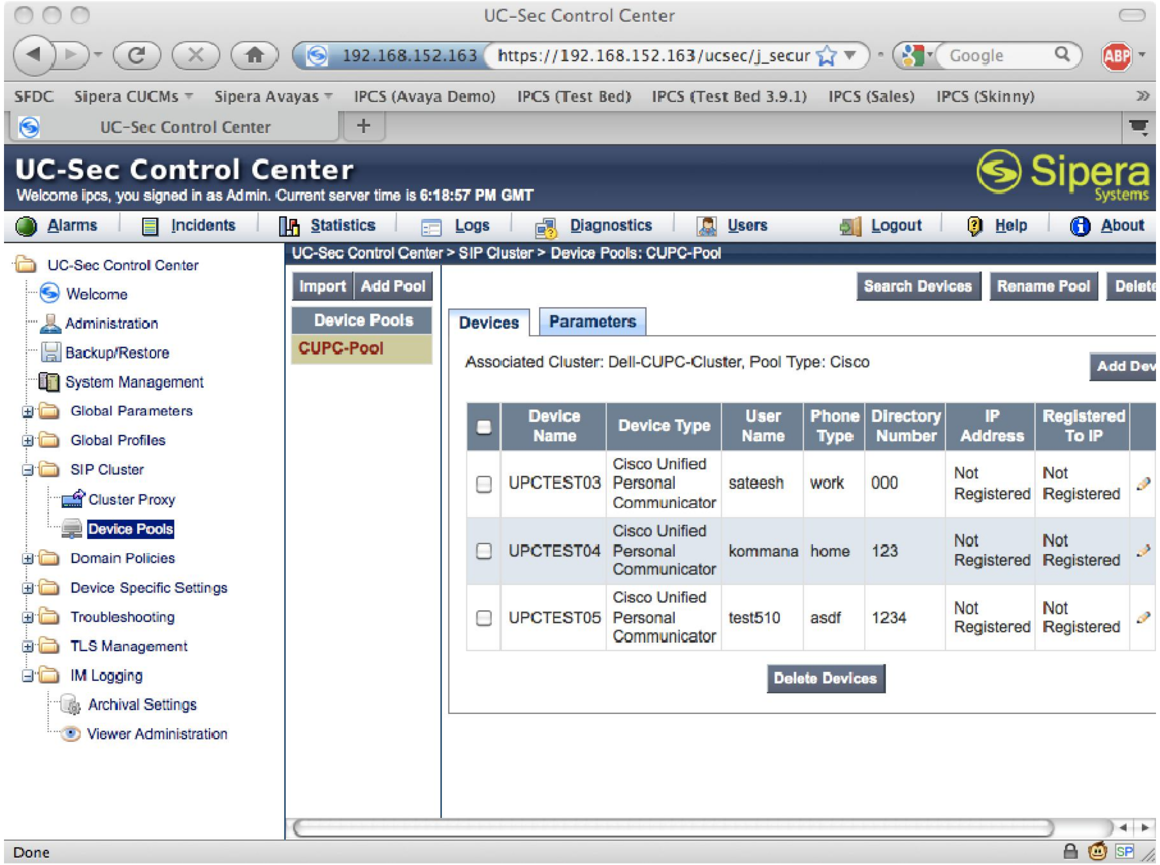
Cluster Information	
Call Server Type	Cisco

Security Information	
Secure Mode	Disabled

Miscellaneous Information	
IM Logging Only	Enabled
Domain Name	sipera.com
HTTP Domain	192.168.151.161

Configure CUCM Device Pools

- Create a device pool
- Add or import devices

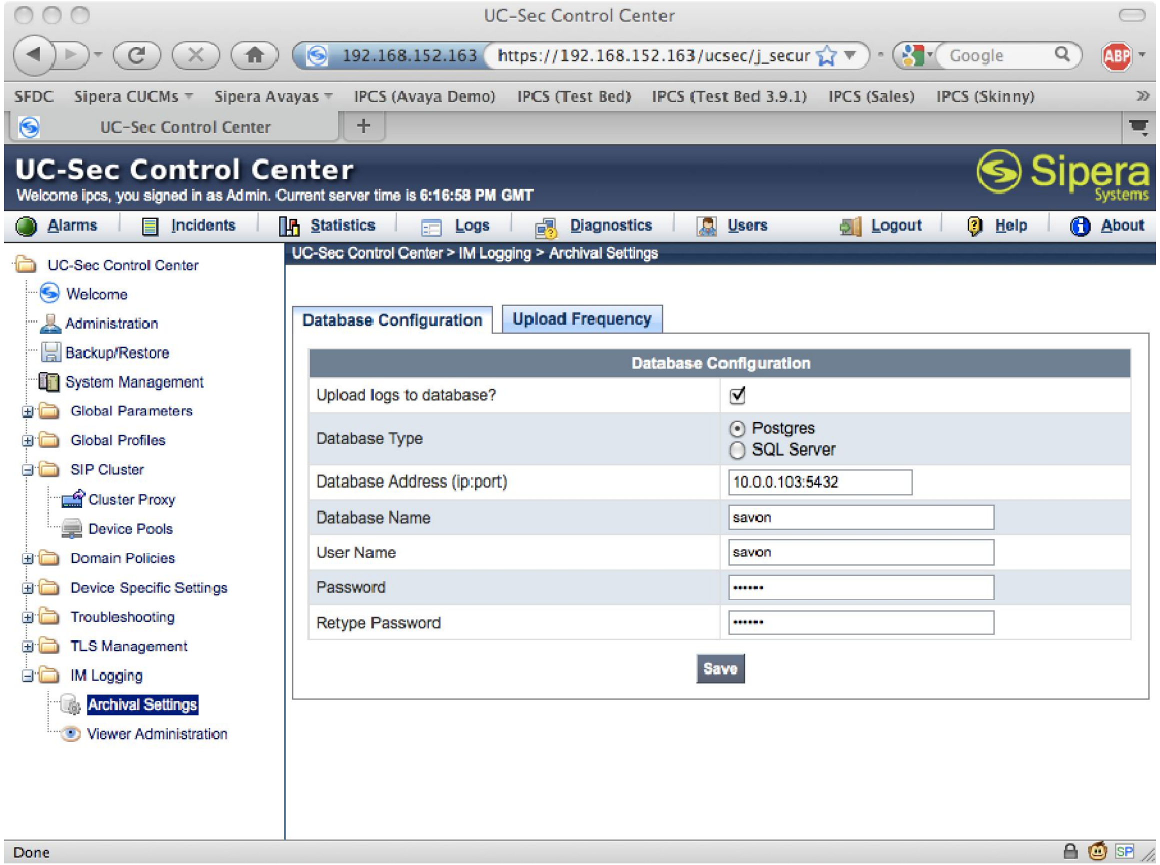


Associated Cluster: Dell-CUPC-Cluster, Pool Type: Cisco

□	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



UC-Sec Control Center

Welcome ipcs, you signed in as Admin. Current server time is 6:16:58 PM GMT

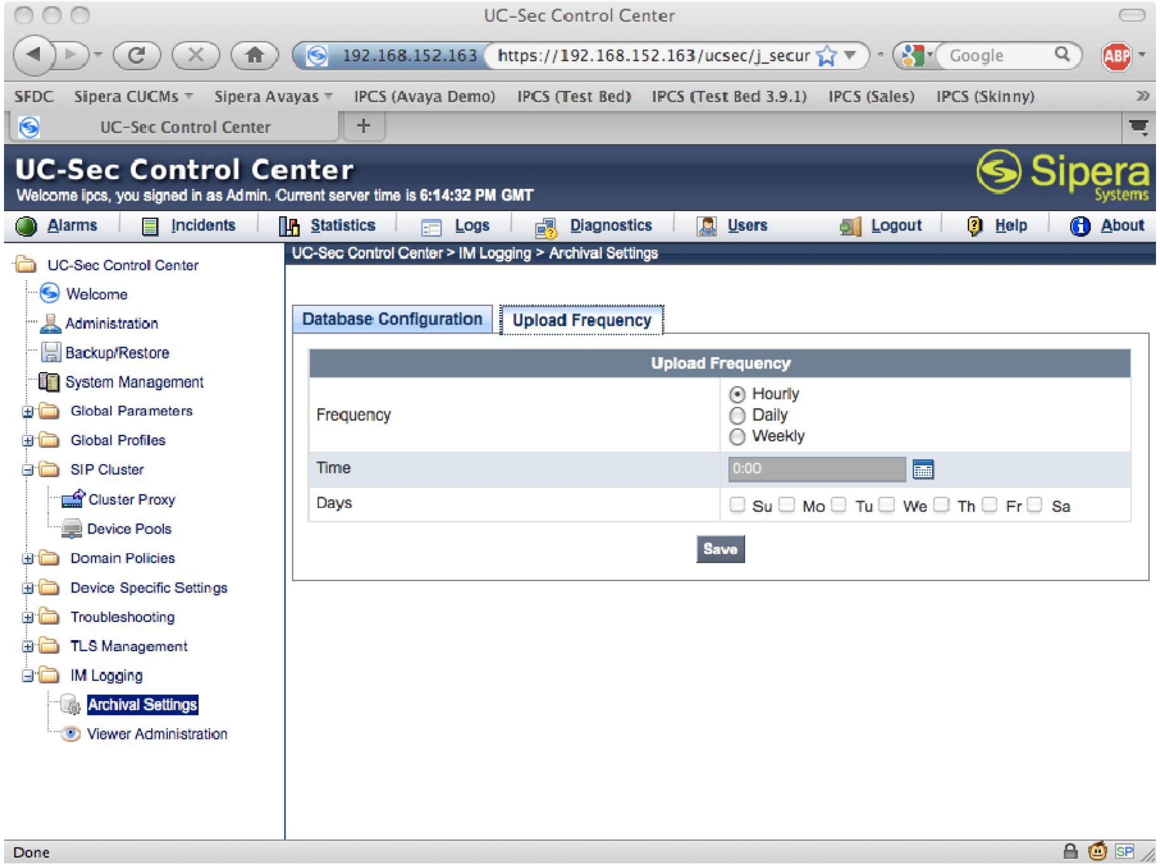
UC-Sec Control Center > IM Logging > Archival Settings

Database Configuration

Upload logs to database?	☑
Database Type	● Postgres ○ SQL Server
Database Address (ip:port)	10.0.0.103:5432
Database Name	savon
User Name	savon
Password	••••••
Retype Password	••••••

Configure Upload Frequency

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



UC-Sec Control Center

Welcome ipcs, you signed in as Admin. Current server time is 6:14:32 PM GMT

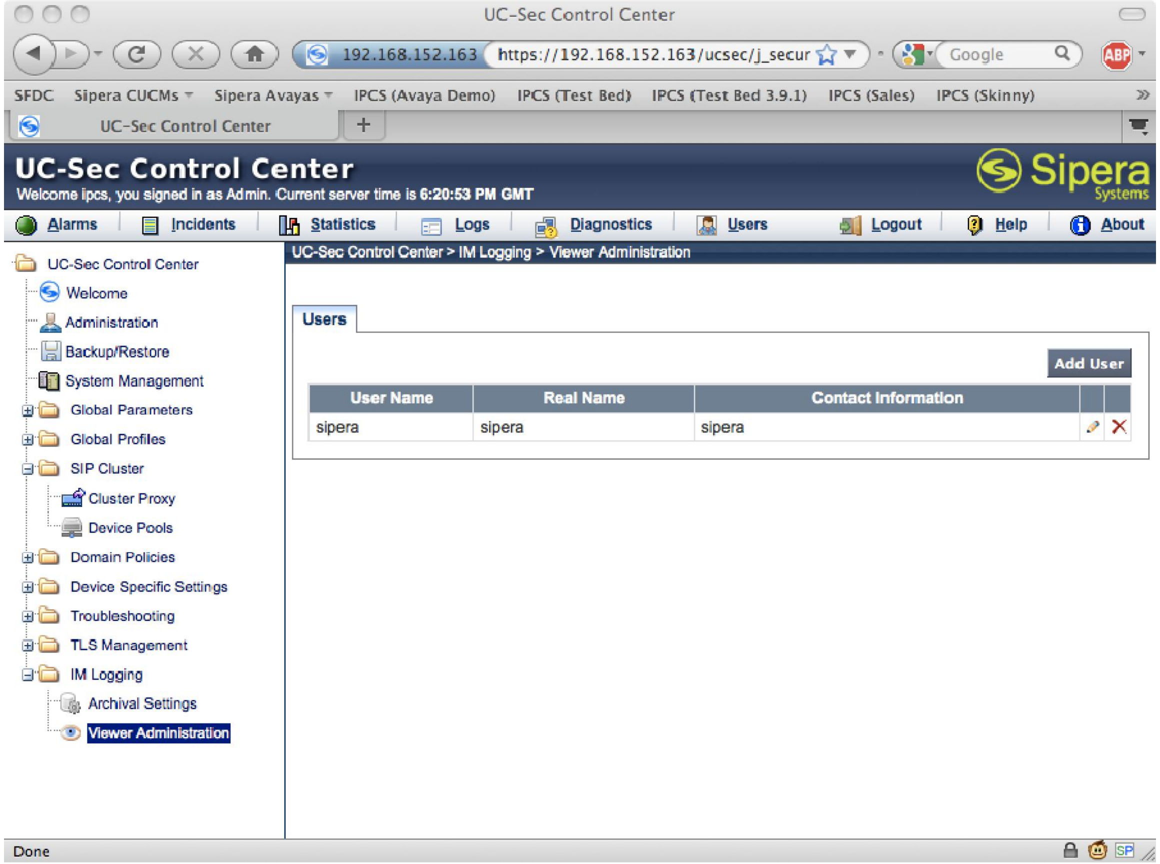
UC-Sec Control Center > IM Logging > Archival Settings

Upload Frequency

Frequency	● Hourly ○ Daily ○ Weekly
Time	0:00
Days	□ Su □ Mo □ Tu □ We □ Th □ Fr □ Sa

Configure IM Log Viewers

- Add users who are allowed to view IMs



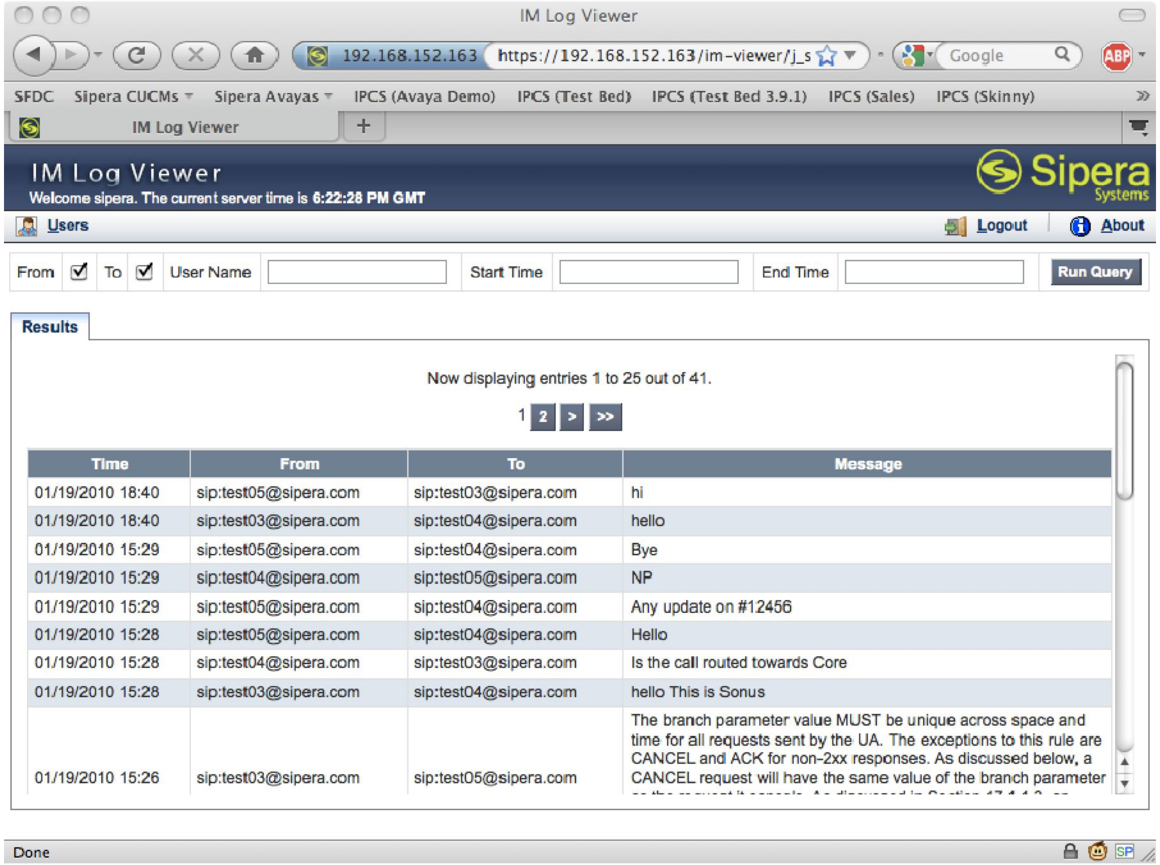
Welcome ipcs, you signed in as Admin. Current server time is 6:20:53 PM GMT

UC-Sec Control Center > IM Logging > Viewer Administration

User Name	Real Name	Contact Information
sipera	sipera	sipera

View IM Logs

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



IM Log Viewer

Welcome sipera. The current server time is 6:22:28 PM GMT

From ☑ To ☑ User Name Start Time End Time

Now displaying entries 1 to 25 out of 41.

1 2 > >>

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

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
```