INDEX

A

administrative accounts
- summary of purposes 4-1

Application Administration account 4-1

authentication rules 5-5

C

call signaling, modification threat 3-1

Cisco PCA, securing access to Cisco Unity Connection 8-1

Cisco Unified CM
- call signaling modification 3-1
- identity theft 3-2
- man-in-the-middle attacks on connection to Cisco Unity Connection 3-1
- media (RTP) stream modification 3-2
- network traffic sniffing (eavesdropping) 3-1

Connection service ports 1-1

E

eavesdropping Cisco Unified CM connections 3-1

I

identity theft
- Cisco Unified CM server 3-2
- Cisco Unity Connection voice messaging port 3-2

IMAP clients
- securing access to Cisco Unity Connection 8-1
- security options 9-6

IP phones, network traffic sniffing (eavesdropping) 3-1

M

mailbox-size quotas, customizing for users or templates 9-4

man-in-the-middle attacks for Cisco Unified CM connections 3-1

Media Master, preventing users from saving messages 9-4

media stream, modification threat 3-2

messages
- shredding files for secure deletes 9-5

message security
- option to disable saves in Media Master 9-4
- overview of options 9-1
- security options for IMAP client access 9-6
- sensitivity options for users and unidentified callers 9-1

N

network traffic sniffing Cisco Unified CM connections 3-1

O

Operating System Administration account 4-1

P

passwords
- changing for Connection web application access 5-3, 6-3
- unique and secure, assigning 5-2
- used to access Connection applications 5-2, 6-1

PINs

changing Connection phone PINs 5-4, 6-3
unique and secure, assigning 5-2
used to access Connection applications 5-2, 6-1
ports, voice messaging, and identity theft 3-2

Q

quotas for mailboxes, customizing for users or templates 9-4

R

restriction tables, using to prevent toll fraud 2-1
RTP stream, modification threat 3-2

S

sec-01-1 1-1
secure deletes, shredding message files for 9-5
securing Cisco PCA and IMAP client access to Cisco Unity Connection 8-1
security
controlling access, distribution, and storage of voice messages 9-1
IMAP client 9-6
user and unidentified caller messages 9-1
server, identity theft 3-2
shredding message files for secure deletes 9-5
SSL certificate, using to secure Cisco PCA and IMAP client access to Cisco Unity Connection 8-1

T

TCP ports
used for inbound connections 1-1
used for outbound connections 1-6
toll fraud 2-1

U

UDP ports
used for inbound connections 1-1
used for outbound connections 1-6

V

voice messaging ports and identity theft 3-2