



INDEX

A

administrative accounts

best practices [4-19](#)

summary of purposes [4-17](#)

Application Administration account [4-18](#)

authentication rules [6-33](#)

C

call signaling, modification threat [3-12](#)

Cisco PCA, securing access to Cisco Unity Connection [9-45](#)

Cisco Unified CM

call signaling modification [3-12](#)

identity theft [3-12](#)

man-in-the-middle attacks on connection to Cisco Unity Connection [3-12](#)

media (RTP) stream modification [3-12](#)

network traffic sniffing (eavesdropping) [3-12](#)

Connection service ports [1-1](#)

E

eavesdropping Cisco Unified CM connections [3-12](#)

I

identity theft

Cisco Unified CM server [3-12](#)

Cisco Unity Connection voice messaging port [3-12](#)

IMAP clients

securing access to Cisco Unity Connection [9-45](#)

security options [10-69](#)

IP phones, network traffic sniffing (eavesdropping) [3-12](#)

M

mailbox-size quotas, customizing for users or templates [10-66](#)

man-in-the-middle attacks for Cisco Unified CM connections [3-12](#)

Media Master, preventing users from saving messages [10-67](#)

media stream, modification threat [3-12](#)

messages

shredding files for secure deletes [10-67](#)

message security

option to disable saves in Media Master [10-67](#)

overview of options [10-61](#)

security options for IMAP client access [10-69](#)

sensitivity options for users and unidentified callers [10-62](#)

N

network traffic sniffing Cisco Unified CM connections [3-12](#)

O

Operating System Administration account [4-18](#)

P

passwords

changing for Connection web application access [5-25, 6-31, 7-39](#)

unique and secure, assigning [6-31](#)

used to access Connection applications [5-24, 6-30, 7-37](#)

PINs

changing Connection phone PINs [5-26, 6-32, 7-39](#)

unique and secure, assigning [6-31](#)

used to access Connection applications [5-24, 6-30, 7-37](#)

ports, voice messaging, and identity theft [3-12](#)

Q

quotas for mailboxes, customizing for users or templates [10-66](#)

R

restriction tables, using to prevent toll fraud [2-9](#)

RTP stream, modification threat [3-12](#)

S

secure deletes, shredding message files for [10-67](#)

securing Cisco PCA and IMAP client access to Cisco Unity Connection [9-45](#)

security

controlling access, distribution, and storage of voice messages [10-61](#)

IMAP client [10-69](#)

user and unidentified caller messages [10-62](#)

server, identity theft [3-12](#)

shredding message files for secure deletes [10-67](#)

SSL certificate, using to secure Cisco PCA and IMAP client access to Cisco Unity Connection [9-45](#)

T

TCP ports

used for inbound connections [1-1](#)

used for outbound connections [1-5](#)

toll fraud [2-9](#)

U

UDP ports

used for inbound connections [1-1](#)

used for outbound connections [1-5](#)

V

voice messaging ports and identity theft [3-12](#)