Avaya™ Toll Fraud and Security Handbook

555-025-600
Issue 9
May 2003

Copyright 2003, Avaya Inc.
All Rights Reserved

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following website:
http://www.avaya.com/support

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

How to Get Help

For additional support telephone numbers, go to the Avaya Web site:
http://www.avaya.com/support/

If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices operate within the following parameters:

- Maximum power output: -5 dBm to -8 dBm
- Center Wavelength: 1310 nm to 1360 nm

Luokan 1 Laserlaite
Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

Federal Communications Commission Statement

Part 15:
For MCC1, SCC1, G600, and CMC1 Media Gateways:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For the G700 Media Gateway:

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that radio interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- **Reorient or relocate the receiving antenna.**
- **Increase the separation between the equipment and receiver.**
- **Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.**
- **Consult the dealer or an experienced radio/TV technician for help.**

Part 68: Answer-Supervision Signaling. Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

For MCC1, SCC1, G600, and CMC1 Media Gateways:
This equipment complies with Part 68 of the FCC rules. On the rear of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For the G700 Media Gateway:
This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. Located prominently on this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, G600, and CMC1 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off/On premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A3 channel service unit	04DU9-DN	6.0Y	RJ48C

For the G700 Media Gateway:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	0.5A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

For MCC1, SCC1, G600, and CMC1 Media Gateways:
This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

For the G700 Media Gateway:
This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

DECLARATIONS OF CONFORMITY

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site:
http://www.avaya.com/support

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at:
http://www.part68.org/

by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity



Avaya Inc. declares that the equipment specified in this document bearing the “CE” (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site:
http://www.avaya.com/support/

Japan

For MCC1, SCC1, G600, and CMC1 Media Gateways:
This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

For the G700 Media Gateway:
This is a Class B product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準
に基づくクラスB 情報技術装置です。この装置は、家庭環境で使用すること
を目的としていますが、この装置がラジオやテレビジョン受信機に近接して
使用されると、受信障害を引き起こすことがあります。
取 扱説明書に従って正しい取り扱いをして下さい。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya Web site:
http://www.avaya.com/support/

Contents

1 About this document 1-1

- Overview 1-1
- Reason for reissue 1-3
- Intended audience 1-3
- How this guide is organized 1-4
- Avaya's statement of direction 1-5
- Avaya/customer security roles and responsibilities 1-7
  - Avaya's roles and responsibilities 1-8
  - Customer roles and responsibilities 1-8
- Downloading this book and updates from the Web 1-9
- Related resources 1-9
  - Product documentation 1-9
  - Avaya security offerings 1-10
- Avaya toll fraud and technical assistance 1-11
  - Within the US 1-11
  - International 1-11
- Related documentation 1-11
- Trademarks 1-12
- Sending us comments 1-12

2 Introduction 2-1

- Background 2-1
- Who is the enemy? 2-2
  - Hackers and phreakers 2-2
  - Call sell operations 2-2
  - Drug dealers 2-3
- What is in a loss? 2-3
  - Cost of the phone bill 2-3
  - Lost revenue 2-3
  - Expenses 2-3
- Known toll fraud activity 2-4

Contents

3 IP security 3-1

- Introduction 3-1
- Overview 3-1
- Mission-critical assets 3-2
- Physical security 3-2
- Control networks 3-2
- Firewalls and routing 3-2
- Customer-managed applications 3-2
- Administration and management 3-3
- Software patches and upgrades 3-3
- Additional information 3-4

4 Security risks 4-1

- Overview 4-1
- Remote access 4-2
- Automated attendant 4-3
- Other port security risks 4-3
- Voice messaging systems 4-4
- Administration / maintenance access 4-4
  - Changing default passwords 4-4
  - Choosing passwords 4-5
  - Increasing adjunct access security 4-6
  - Increasing product access (port) security 4-6
- General security measures 4-8
  - Educating users 4-8
  - Establishing a policy 4-9
  - Physical security 4-9
- Security goals tables 4-10

Contents

5 Large business communications systems 5-1

- Keeping unauthorized third parties from entering the system 5-2
  - Protecting the Remote Access feature 5-2
  - Security tips 5-2
  - Disabling/removing the Remote Access feature 5-3
  - Tools to protect the Remote Access feature 5-3
    - Barrier codes 5-5
    - Authorization codes 5-8
    - Feature access code administration 5-9
    - Trunk administration 5-9
    - Remote access dial tone 5-10
    - Night service 5-10
    - Call vectoring (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3) 5-10
    - Protecting vectors that contain call prompting 5-11
  - Command: status remote-access 5-12
  - Logoff screen notification 5-12
- Tools that restrict unauthorized outgoing calls 5-13
  - Class of restriction 5-14
    - Calling party and called party restrictions 5-15
    - COR-to-COR restrictions/calling permissions 5-16
    - Restriction override (3-way COR check) 5-17
  - Class of service 5-17
  - Facility restriction level 5-19
  - Alternate facility restriction levels 5-19
  - Toll analysis (G3 only) 5-19
  - Free call list 5-20
  - AAR/ARS analysis 5-20
  - ARS dial tone 5-20
  - Station restrictions 5-20
  - Recall signaling (switchhook flash) 5-21
  - Attendant - controlled voice terminals 5-21

Contents

Restrictions — individual and group-controlled (Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY G1, G3, and System 75) 5-21

Central office restrictions 5-22

Restricting incoming tie trunks 5-22

Authorization codes 5-22

Trunk-to-trunk transfer 5-23

Forced entry of account code 5-24

World class routing (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G2.2 and G3) 5-24

Digit conversion 5-25

Station security codes 5-25

Personal station access 5-25

Security tips 5-26

Extended user administration of redirected calls 5-27

Remote user administration of call coverage 5-27

- Security measures 5-28

Require passwords 5-28

Restrict who can use remote access and track its usage 5-29

Fully restrict service 5-31

Provide individualized calling privileges using FRLs 5-31

Prevent after-hours calling using time of day routing or alternate FRLs 5-33

Block international calling 5-34

Limit international calling 5-35

Select authorization code time-out to attendant 5-36

Restrict calls to specified area codes 5-37

Allow calling to specified numbers 5-37

Use attendant control of remote access calls (DEFINITY G2 and System 85 only) 5-38

Use attendant control of specific extensions 5-38

Disable direct access to trunks 5-39

Use attendant control of trunk group access 5-40

Contents

Disable facility test calls 5-40
Suppress remote access dial tone 5-42
Disallow trunk-to-trunk transfer 5-43
Disable transfer outgoing trunk to outgoing trunk 5-44
Disallow outgoing calls from tie trunks 5-45
Limit access to tie trunks 5-45
Monitor trunks 5-46
Use terminal translation initialization 5-46
Require account codes 5-47
Assign COR restrictions to adjuncts when using expert agents 5-48
Disable distinctive audible alert 5-48
Remove data origination code 5-48
Use world class routing restrictions 5-49
Change override restrictions on 3-way COR check 5-50

- Detecting toll fraud 5-50

Administration security 5-51
Logins for INADS port 5-51
Forced password aging and administrable logins 5-52
Call detail recording/station message detail recording 5-53
Traffic measurements and performance 5-55
Monitor I 5-55
SAT, Manager I, and G3-MT reporting 5-55
ARS measurement selection 5-56
Automatic circuit assurance 5-56
BCMS measurements (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G1 and G3) 5-58
CMS measurements 5-58
Security violation notification (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3) 5-59
Security Violations Measurement reports 5-62
Remote access barrier code aging/access limits (DEFINITY G3V3 and Later) 5-67

Contents

Recent Change History report (Communication Manager, MultiVantage Software, DEFINITY ECS, and DEFINITY G1 and G3) 5-68
Malicious call trace 5-68
Service observing 5-69
Busy verification 5-70
List call-forwarding command 5-70

6 Small business communications systems 6-1

- Features for the MERLIN systems 6-2
- MERLIN II Communications System 6-5
  - Protecting direct inward system access 6-5
    - Security tips 6-5
- MERLIN LEGEND Communications System 6-7
  - Preventive measures 6-8
  - Protection via star codes and allowed/disallowed lists 6-9
  - Default disallowed list 6-10
  - Assigning a second dial tone timer 6-10
  - Setting facility restriction levels 6-10
    - Security defaults and tips 6-11
  - Protecting the Remote Access feature 6-12
    - Security tips 6-12
  - Protecting remote system programming 6-14
    - Security tips 6-14
  - Protecting remote call forwarding 6-15
- MERLIN LEGEND/MAGIX toll fraud 6-15
  - Why toll fraud happens 6-15
  - Tool fraud warning signs 6-15
  - Tips to prevent toll fraud 6-16
  - Responsibility 6-17
  - Programming tools to prevent fraud 6-17
  - Security of your systems: preventing toll fraud 6-17

Contents

Toll fraud prevention 6-19
Physical security, social engineering, and general security measures 6-19
Security risks associated with transferring through voice messaging systems 6-21
Security risks associated with the Automated Attendant feature of voice messaging systems 6-22
Security risks associated with the Remote Access feature 6-24
Other security hints 6-24
Detecting toll fraud 6-26
Magix R1.5: allowed lists enhancements 6-28
Legend through Magix R1 automatic route selection 6-30
Magix R1.5 automatic route selection enhancements 6-30
Magix R1.5: Wildcard characters in ARS 6-digit tables 6-33
Magix R1.5: Disallowed lists enhancements 6-34
Loop-start reliable disconnect 3 6-35
Disconnect signaling reliability 3 6-36
Marked system speed dial 6-36
Night service group assignment 6-36
Remote Access feature 6-38
Trunk-to-trunk transfer 6-40
Toll fraud investigation: disallow list information 6-40
General information 6-40
Standard disallow list entries 6-41
Questions to ask the customer 6-42
LEGEND/MAGIX toll fraud at a glance 6-43
MERLIN Mail/MERLIN LEGEND Mail/MERLIN messaging toll fraud at a glance 6-45
LEGEND/MAGIX toll fraud check list 6-45
- MERLIN Plus Communications System 6-59
Protecting remote line access (R2 only) 6-59
Security tips 6-59
Protecting remote call forwarding (R2 only) 6-60
- PARTNER II Communications System 6-61

Contents

- PARTNER Plus Communications System 6-61
- System 25 6-62
  - Protecting remote access 6-62
    - Security tips 6-63
  - Protecting remote system administration 6-63
    - Security tips 6-64

7 Voice messaging systems 7-1

- Protecting voice messaging systems 7-2
  - Security tips 7-3
- Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY communications systems, System 75,and System 85 7-4
  - Tools that prevent unauthorized calls 7-5
    - Facility restriction levels 7-6
    - Station-to-trunk restrictions 7-6
    - Class of restriction 7-7
    - Class of service 7-7
    - Toll analysis 7-7
  - Security measures in the PBX 7-8
    - Limit voice mail to internal calling 7-8
    - Restrict the outside calling area 7-8
    - Allow calling only to specified numbers 7-10
  - Detecting voice mail fraud 7-12
    - Call detail recording and / station message detail recording 7-13
    - Call Traffic report 7-14
    - Trunk Group report 7-14
    - SAT, Manager I, and G3-MT reporting 7-14
    - ARS measurement selection 7-15
    - Automatic circuit assurance 7-15
    - Busy verification 7-16
  - Protecting the AUDIX, DEFINITY AUDIX, and Avaya INTUITY voice mail systems 7-16

Contents

Unauthorized system use 7-16
Traffic reports (AUDIX Voice Mail System only) 7-19
Call detail recording (AUDIX Voice Mail System only) 7-19
Protecting passwords 7-22
Security features 7-23
Security measures 7-26
Security tips 7-30
Protecting the AUDIX Voice Power System 7-30
Traffic reports 7-30
Protecting passwords 7-31
Security tips 7-31
Security measures 7-32
Protecting the CONVERSANT Voice Information System 7-33
Protecting passwords 7-33
Security measures 7-34
Security tips 7-35
- MERLIN II Communications System 7-35
Protecting the MERLIN MAIL Voice Messaging System 7-35
Protecting passwords 7-36
Security tips 7-36
- MERLIN LEGEND Communications System 7-38
Protecting the AUDIX Voice Power System 7-39
Protecting passwords 7-39
Security tips 7-39
Security measures 7-40
Protecting the INTUITY Voice Messaging System 7-41
Protecting passwords 7-42
Security tips 7-42
Security measures 7-42
Protecting the MERLIN MAIL, MERLIN MAIL-ML, MERLIN MAIL R3, and MERLIN LEGEND Mail voice messaging systems 7-45
Protecting automated attendant 7-45
Protecting passwords 7-46

Contents

Security tips 7-46

Additional MERLIN MAIL R3 and MERLIN LEGEND Mail Voice Messaging System security features 7-49

- Messaging 2000 System 7-50

Maintaining Message 2000 system security 7-50

Security recommendations for remote access 7-55

- PARTNER II Communications System 7-55

Protecting the PARTNER MAIL and PARTNER MAIL VS systems 7-55

Protecting passwords 7-55

Security tips 7-56

- PARTNER Plus Communications System 7-57

Protecting the PARTNER MAIL and PARTNER MAIL VS systems 7-58

Protecting passwords 7-58

Security tips 7-58

- System 25 7-60

Protecting the AUDIX Voice Power System 7-60

Protecting passwords 7-61

Security tips 7-61

Security measures 7-62

8 Automated attendant 8-1

- Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY communications systems, System 75, and System 85 8-1

Security tips 8-1

Tools that prevent unauthorized calls 8-2

Facility restriction levels 8-2

Station-to-trunk restrictions 8-3

Class of restriction (System 75, DEFINITY G1, and G3, Communication Manager, MultiVantage Software, DEFINITY ECS) 8-3

Contents

Class of service 8-4
Toll analysis 8-5
Security measures 8-5
Limit transfers to internal destinations 8-5
Prevent calls to certain numbers 8-6
Allow calling to specified numbers 8-6
Detecting automated attendant toll fraud 8-8
Call detail recording / station message detail recording 8-9
Call Traffic report 8-10
Trunk Group report 8-10
SAT, Manager I, and G3-MT reporting 8-10
ARS measurement selection 8-11
Automatic circuit assurance 8-11
Busy verification 8-12
Call Traffic report 8-13
Trunk Group report 8-13
Traffic reports 8-13
Call detail recording 8-13
Voice session record 8-14
Outgoing voice call detail record 8-15
Protecting automated attendant on the AUDIX Voice Mail System 8-16
Disallow outside calls 8-16
Protecting automated attendant on the AUDIX Voice Power System 8-17
Protecting automated attendant on the CONVERSANT Voice Information System 8-18
Protecting automated attendant on the DEFINITY AUDIX System 8-18
Protecting automated attendant on the Avaya INTUITY System 8-18
- MERLIN II Communications System R3 8-19

MERLIN MAIL Voice Messaging System 8-19
MERLIN Attendant 8-19

Contents

- MERLIN LEGEND Communications System 8-20
  - AUDIX Voice Power System 8-20
  - MERLIN MAIL, MERLIN MAIL-ML, and MERLIN MAIL R3 voice messaging systems 8-20
  - MERLIN Attendant 8-20
- PARTNER II Communications System 8-21
  - PARTNER MAIL and PARTNER MAIL VS systems 8-21
  - PARTNER Attendant 8-21
- PARTNER Plus Communications System 8-22
  - PARTNER MAIL and PARTNER MAIL VS systems 8-22
  - PARTNER Attendant 8-22
- System 25 8-22
  - AUDIX Voice Power System 8-22

9 Other products and services 9-1

- Call Management System (R3V4) 9-1
  - Security tips 9-1
  - CMS helplines 9-2
- CallMaster PC 9-3
  - Security tips 9-3
- Multipoint Conferencing Unit (MCU)/Conference Reservation and Control System (CRCS) 9-4
- PassageWay Telephony Services for NetWare and Windows NT 9-5
  - Security tips 9-6
- TransTalk 9000 Digital Wireless System 9-9
  - Security tips 9-9

10 Call routing 10-1

- Call routing call flow 10-1

Contents

11 Blocking calls 11-1

- Country codes 11-1
- Blocking toll fraud destinations 11-10
  - Blocking ARS calls on DEFINITY G1 and System 75 11-11
  - Blocking ARS calls on G2.1 and System 85 11-15
  - Blocking WCR calls on DEFINITY G2.2 11-16
  - Blocking ARS calls on G3 11-17
  - Blocking ARS calls on System 25 R3V3 11-19

12 Remote access example (Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY G1, G3, and System 75) 12-1

- Setting up remote access 12-1
- Permanently disabling remote access 12-3

13 Administering features of the DEFINITY G3V3 and later 13-1

- Administering the SVN feature 13-2
  - Administering the login component 13-2
    - Enable/disable a login ID 13-3
    - List the status of a login ID 13-4
  - Administering the barrier code security violations parameters of the SVN feature 13-4
    - Enable/disable remote access code 13-5
    - Administering the Remote Access Kill After N Attempts feature 13-6
    - Administering the Login ID Kill After N Attempts feature 13-7
  - Administering the authorization code component 13-8
  - Administering the station security code component 13-9

Contents

- Administering barrier code aging 13-11
- Administering customer logins and forced password aging 13-13
  - Adding customer logins and assigning initial password 13-13
  - Changing a login's attributes 13-15
  - Administering login command permissions 13-16
    - Display a specified login 13-17
    - List logins 13-17
    - Remove a login 13-18
- Administering the security violations reports 13-18

14 Changing your password 14-1

- AUDIX Voice Mail System 14-1
- AUDIX Voice Power System 14-2
- CONVERSANT Voice Information System 14-2
- DEFINITY AUDIX System 14-4
- Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G1 and G3 14-5
- DEFINITY G2 14-6
- Avaya INTUITY System 14-6
- MERLIN MAIL or MERLIN MAIL-ML Voice Messaging System 14-7
- MERLIN MAIL R3, MERLIN LEGEND Mail, or PARTNER MAIL R3 Voice Messaging System 14-8
- PARTNER MAIL System 14-9
- PARTNER MAIL VS System 14-9
- System 25 14-10
- System 75 14-10
- System 85 14-11

Contents

15 Toll fraud job aids 15-1

- Toll fraud warning signs 15-1
- System security action plan 15-3
- Ten tips to help prevent phone fraud 15-4

16 Special security product and service offers 16-1

- Remote port security device 16-1
  - Key and lock features 16-2
  - Securing DEFINITY Systems (prior to Release 7.2) with the remote port security device 16-3
  - Avaya support 16-4
- Securing DEFINITY systems (Release 7.2 and Later) with Access Security Gateway 16-4
  - Administering the Access Security Gateway 16-5
  - Logging in via Access Security Gateway (session establishment) 16-6
  - Maintaining login IDs 16-7
    - Temporarily disabling Access Security Gateway access for login 16-7
    - Restarting temporarily disabled ASG access for login 16-7
  - Maintaining the ASG history log 16-7
  - Loss of an ASG key 16-8
  - Interactions of ASG 16-8
  - Securing INTUITY AUDIX ports (Release 5.0 and later) with ASG 16-9
  - Logging in with ASG 16-10
  - Maintaining login IDs 16-10
    - Adding an ASG login 16-11
    - Blocking or reinstating access privileges for an ASG login 16-12
    - Changing the encryption key number for an ASG login 16-12

Contents

Displaying ASG login information 16-13
Disabling ASG authentication 16-13
Setting and resolving violation warnings 16-13
Setting notification limits 16-13
Resolving ASG violation alarms 16-14
- Avaya support 16-15
- HackerTracker 16-15
- Security Tune-Up Service 16-15
- Toll fraud contact list 16-16

17 Product security checklists 17-1

- General security procedures 17-2
- AUDIX, DEFINITY AUDIX and INTUITY AUDIX voice messaging systems 17-4
- AUDIX Voice Power System 17-6
- BasicWorks 17-8
- CONVERSANT Voice Information System 17-12
- Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY G1 and G3, and System 75 17-14
- DEFINITY G2 and System 85 17-20
- DIMENSION PBX System 17-24
- MERLIN II Communications System 17-27
- MERLIN LEGEND Communications System 17-29
- MERLIN MAIL Voice Messaging System 17-32
- MERLIN MAIL-ML Voice Messaging System 17-34
- MERLIN MAIL R3 Voice Messaging System 17-36
- MERLIN Plus Communications System 17-39
- Messaging 2000 Voice Mail System 17-40
- Multimedia Communications Exchange Server 17-45
- Multipoint Conferencing Unit /Conference Reservation and Control System 17-46

ESM security checklist 17-48
CRCS Security Checklist 17-50
MSM security checklist 17-51

Contents

- PARTNER, PARTNER II, and PARTNER Plus communications systems, and PARTNER Advanced Communications System (ACS) 17-56
- PARTNER MAIL, PARTNER MAIL VS, and PARTNER Voice Mail (PVM) systems 17-61
- System 25 17-63
- PassageWay Telephony Services 17-66

18 Large business communications systems security tools by release 18-1

19 Non-supported products 19-1

- As of December 31, 2002 19-1
- As of December 31, 2001 19-1
- As of December 31, 2000 19-1
- As of September 30, 2000 19-2
- As of December 31, 1999 19-2

20 Links to additional security information 20-1

- About IP and network security 20-1
- Avaya products to enhance security 20-1
- White papers 20-1
- Books and articles 20-1
- Web sites 20-2

Contents

GL	**Glossary**	**GL-1**
IN	**Index**	**IN-1**

About this document

1

Overview

This handbook discusses security risks and measures that can help prevent external telecommunications fraud involving the following Avaya products:

IP and IP-enabled servers:

- Avaya™ S8100, S8300, and S8700 Media Servers
- DEFINITY® Enterprise Communications Server (ECS) Release 5 and later

PBX systems:

- DEFINITY® Generic 1, 2, and 3 communications systems
- MERLIN® II Communications System
- MERLIN LEGEND® Communications System
- MERLIN® Plus Communications System
- PARTNER® II Communications System
- PARTNER® Plus Communications System
- System 25 Communications System
- System 75 (R1V1, R1V2, R1V3)
- System 85 (R1, R2V2, R2V3, R2V4)

Voice processing systems:

- AUDIX® Voice Mail System
- AUDIX® Voice Power® System
- CONVERSANT® Voice Information System
- DEFINITY® AUDIX® System
- INTUITY™ AUDIX® Voice Messaging System
- INTUITY™ CONVERSANT® Voice Information System

- MERLIN MAIL® Voice Messaging System
- MERLIN MAIL®-ML Voice Messaging System
- MERLIN MAIL® R3 Voice Messaging System
- PARTNER MAIL® System
- PARTNER MAIL VS® System

Other products and services:

- Call Management System (R3V2)
- CallMaster® PC
- Multipoint Conferencing Unit (MCU)
- PassageWay® Telecommunications Interface
- TransTalk™ 9000 Digital Wireless System
- Telephony Services for Netware®

NOTE:
Unless specifically stated otherwise, references in this document to "G3Vx and later" include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

NOTE:
Although the Avaya™ S8100, S8300, and S8700 Media Servers are not covered explicitly in this handbook, the information supplied for DEFINITY ECS applies to these media servers as well.

NOTE:
Although the DIMENSION® Call Management System is not covered explicitly in this handbook, the information supplied for System 85 Release 2 applies to the DIMENSION PBX System as well.

NOTE:
This document describes switch features and how they are related to security. It is not designed to fully describe the capabilities of each feature. For further details about all the security features and their interactions with other system features, refer to the appropriate system manual for your telecommunications system. (See ''Related documentation'' in this chapter for titles and document numbers.)

Reason for reissue

This issue, Issue 9 of the Avaya™ Toll Fraud and Security Handbook*,* refocuses this document to be about toll fraud and related security issues. This update also includes a new section, Chapter 20, ‘‘Links to additional security information’’.

Minor edits and other additions have also been included in this issue.

Intended audience

Telecommunications managers, console operators, and security organizations within a company should be aware of the information in Chapters 1, 2, and 3. Chapter 4 introduces more technical information and is directed at people responsible for implementing and administering the security aspects of systems.

Chapters 10 through 13 expand upon technical information in the handbook and are intended for use by the system administrator. Chapters 13, 15, 16, and 18 have application throughout the organization. Chapter 16 is specifically intended for telecommunications management personnel with responsibilities for implementing a security policy.

How this guide is organized

The Avaya™ Toll Fraud and Security Handbook has the following chapters:

Chapter 1: About this document	Describes the scope, intended audience, and contents of this handbook. Contains Avaya's Statement of Direction. Also defines Avaya's and the customer's roles and responsibilities.
Chapter 2: Introduction	Provides a background for toll fraud.
Chapter 3: IP security	Provides a summary of toll fraud security issues that are introduced in a converged voice and data network environment.
Chapter 4: Security risks	Discusses the major areas in which customer premises equipment-based systems are vulnerable, and introduces available security measures.
Chapter 5: Large business communications systems	Provides information on protecting the DEFINITY ECS Release 5 and later, DEFINITY Communications System Generic 1, Generic 2, and Generic 3, System 75, and System 85. Details how Remote Access is vulnerable to toll fraud, explains numerous system security features, and provides detailed procedures.
Chapter 6: Small business communications systems	Provides information on protecting the MERLIN II, MERLIN LEGEND, MERLIN Plus, PARTNER II, PARTNER Plus, and System 25 communications systems. Details product features that are vulnerable to toll fraud, such as Remote Access and Remote Call Forwarding, and recommends security measures.
Chapter 7: Voice messaging systems	Provides information on protecting voice messaging systems. Explains the tools available and recommends security measures.
Chapter 8: Automated attendant	Provides information on protecting automated attendant systems. Explains the features available and recommends security measures.
Chapter 9: Other products and services	Provides information to protect other Avaya products and services from toll fraud.
Chapter 10: Call routing	Details call flow through a customer premises equipment-based system.
Chapter 11: Blocking calls	Provides procedures for blocking calls to common toll fraud destinations.

Chapter 12: Remote Access example (G1, G3, and System 75)	Offers an example of how to set up Remote Access and an example of how to disable it.
Chapter 13: Administering features of the DEFINITY G3V3 and later	Provides information on administering features available in DEFINITY Releases G3V3 and later, including the DEFINITY ECS Release 5 and 6.
Chapter 14: Changing your password	Tells how to change passwords for systems in the handbook.
Chapter 15: Toll fraud job aids	Provides job aids to help prevent toll fraud.
Chapter 16: Special security product and service offers	Details special product and service offers and provides a toll fraud contact list.
Chapter 17: Product security checklists	Lists the available security features and tips by product.
Chapter 18: Large business communications systems security tools by release	Details security tools referenced in this guide, for the System 75, System 85, DEFINITY ECS, and DEFINITY communications systems by release.
Chapter 19: Non-supported products	Lists the non-supported products.
Chapter 20: Links to additional resources	Provides links to additional information sources for security issues.

Avaya's statement of direction

The telecommunications industry is faced with a significant and growing problem of theft of customer services. To aid in combating these crimes, Avaya intends to strengthen relationships with its customers and its support of law enforcement officials in apprehending and successfully prosecuting those responsible.

No telecommunications system can be entirely free from the risk of unauthorized use. However, diligent attention to system management and to security can reduce that risk considerably. Often, a trade-off is required between reduced risk and ease of use and flexibility. Customers who use and administer their systems make this trade-off decision. They know how to best tailor the system to meet their unique needs and, necessarily, are in the best position to protect the system from unauthorized use. Because the customer has ultimate control over the configuration and use of Avaya services and products it purchases, the customer properly bears responsibility for fraudulent uses of those services and products.

To help customers use and manage their systems in light of the trade-off decisions they make and to ensure the greatest security possible, Avaya commits to the following:

- Avaya products and services will offer the widest range of options available in the industry to help customers secure their communications systems in ways consistent with their telecommunications needs.
- Avaya is committed to developing and offering services that, for a fee, reduce or eliminate customer liability for PBX toll fraud, provided the customer implements prescribed security requirements in its telecommunications systems.
- Avaya's product and service literature, marketing information and contractual documents will address, wherever practical, the security features of our offerings and their limitations, and the responsibility our customers have for preventing fraudulent use of their Avaya products and services.
- Avaya sales and service people will be the best informed in the industry on how to help customers manage their systems securely. In their continuing contact with customers, they will provide the latest information on how to do that most effectively.
- Avaya will train its sales, installation and maintenance, and technical support people to focus customers on known toll fraud risks; to describe mechanisms that reduce those risks; to discuss the trade-offs between enhanced security and diminished ease of use and flexibility; and to ensure that customers understand their role in the decision-making process and their corresponding financial responsibility for fraudulent use of their telecommunications system.
- Avaya will provide education programs for internal and external customers to keep them apprised of emerging technologies, trends, and options in the area of telecommunications fraud.
- As new fraudulent schemes develop, Avaya will promptly initiate ways to impede those schemes, share our learning with our customers, and work with law enforcement officials to identify and prosecute fraudulent users whenever possible.

We are committed to meeting and exceeding our customers' expectations, and to providing services and products that are easy to use and high in value. This fundamental principle drives Avaya's renewed assault on the fraudulent use by third parties of our customers' communications services and products.

Avaya/customer security roles and responsibilities

The purchase of a telecommunications system is a complicated process involving many phases, including system selection, design, ordering, implementation, and assurance testing. Throughout these phases customers, vendors, and their agents each have specific roles and responsibilities. Insuring that systems are designed, ordered, installed, and maintained in a secure fashion is a responsibility each organization must understand.

Avaya, seeking to be our customers' Partner of Choice, clearly defined its mission in this area in a Statement of Direction issued in May, 1992. (See the preceding section.) More specifically, Avaya recognized four areas where we or our agents have specific responsibilities to our customers. These areas, and our responsibilities in each area, are detailed in the next section, ''Avaya's roles and responsibilities''.

In addition, customers have specific responsibilities to ensure the system they are installing is as secure as their requirements dictate. The following quote is from *A Cooperative Solution to the Fraud that Targets Telecom Systems*, a position paper developed by the Toll Fraud Prevention Committee (TFPC) of the Alliance for Telecommunications Industry Solutions:

> "It is necessary to stress that the business owner, the owner or lessee of the CPE [Customer Premises Equipment], has the primary and paramount care, custody, and control of the CPE. The owner has the responsibility to protect this asset, the telecommunications system equally as well as other financial assets of the business."

This document attempts to define industry standards for the roles and responsibilities of the various organizations involved in a system implementation. Portions of this document are applicable to this document and are quoted throughout. Customers interested in the entire document can receive copies by contacting:

> Alliance for Telecommunications Industry Solutions
> 1200 G Street, NW
> Suite 500
> Washington, DC 20005
> http://www.atis.org/

Avaya's roles and responsibilities

- Avaya, as a manufacturer, has the responsibility to **provide** the customer with securable technology, the information resources (product documentation) to understand the capabilities of the technology, and the configuration of the equipment when it shipped from the factory.
- Avaya, as a sales organization, has the responsibility to **inform** the customer of potential toll fraud, how it can happen, and what roles and responsibilities Avaya and the customer need to accept to work together in reducing the customer's potential for toll fraud.
- Avaya, as a provisioning organization, has the responsibility to **assist** the customer in understanding the risks inherent in the use of certain equipment features, and the methods available to minimize those risks. Together with the customer, Avaya must come to an agreement on the desired configuration and ensure that customers' requests are carried out correctly.
- Avaya, as a maintenance provider, has the responsibility to **ensure** that no action taken by us serves to introduce risk to the customer's system. At the very least we must ensure the customer is as secure after our assistance as they were before it.

Customer roles and responsibilities

The customer as the business owner has the responsibility to **select and manage** the security of their system. Specifically, according to the Telecommunications Fraud Prevention Committee (TFPC) of the Alliance for Telecommunications:

> "The basic responsibility of the business owner is to devote adequate resources (time, talent, capital, etc.) to the selection of CPE and to its management, including fraud prevention, detection and deterrence. It is an essential part of managing the business. The owner must demand that the internal staff and supporting external professionals, such as consultants, include security concerns in the evaluation, design, and operation of the telecommunications environment for his/her business."

Downloading this book and updates from the Web

You can download the latest version of the Avaya™ Toll Fraud and Security Handbook*,* 555-025-600, from the Avaya Web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya Web site.

To download the latest version of this book:

1. Access the Avaya web site at http://www.avaya.com/support.
2. Click **Product Documentation**.
3. In the **Search Support Centre** field, type **555-025-600** and click **Go**.

   The system displays the Product Documentation Search Results page.
4. Scroll down to find the latest issue number, and then click the book title that is to the right of the latest issue number.
5. On the next page, scroll down and click one of the following options:
   - **PDF Format** to download the book in regular PDF format
   - **ZIP Format** to download the book in zipped PDF format

Related resources

This section describes additional documentation and security resources.

Product documentation

The security risks and preventive measures presented in this document relate specifically to toll fraud. This handbook is designed to work with the documentation provided for the products described in this document, and it is not intended as a replacement for the product documentation.

To obtain product documentation, please visit the Avaya support website at http://www.avaya.com/support.

Avaya security offerings

Avaya has developed a variety of offerings to assist in maximizing the security of your system. These offerings include:

- Security Tune-up Service (see Chapter 16).
- Toll Fraud Crisis Intervention Service (see ‘‘Avaya toll fraud and technical assistance’’ in this section).
- The Product Security Kit, 555-025-601, includes this document (Avaya™ Toll Fraud and Security Handbook). This provides customers with valuable information on recognizing and defending against toll fraud.
- The HackerTracker™ Call Accounting package that calls you when preset types and thresholds of calls are established (see ‘‘HackerTracker’’ in Chapter 16).
- Remote Port Security Device (RPSD) that makes it difficult for computer hackers to access the remote maintenance ports (see Chapter 16).
- Integrated Lock for Security Toolkit (or Access Security Gateway) feature (see Chapter 16). This feature provides many of the same options as the RPSD listed above, but whereas the RPSD is a hardware device, the SoftLock feature is a software interface that can be installed directly in the DEFINITY ECS software base. This software can be used only with the DEFINITY ECS Release 7.0 and later.
- Software that can identify the exact digits passed through the voice mail system (AUDIX Data Acquisition Package [ADAP]). See your account representative.

Avaya toll fraud and technical assistance

Avaya provides the following resources for technical assistance.

Within the US

Toll Fraud Intervention Hotline	**1 800 643-2353**
Call this number if you suspect you are being victimized by toll fraud or theft of service, call the appropriate Avaya service.	
Avaya Corporate Security	**1 800 822-9009**
Call this number for assistance with other security issues.	
Avaya DEFINITY Hotline	**800 225-7585**
Call this number for assistance with feature administration and system applications.	
Avaya National Customer Care Support Line	**1 800 242-2121**
Call this number for assistance with maintenance and repair issues.	

International

For all non-US resources, contact your local Avaya authorized dealer.

NOTE:
These services are available 24 hours a day, 365 days a year. Consultation charges may apply. Intervention services are performed at no charge for equipment covered by warranty or service agreement.

Related documentation

The security risks and preventive measures presented in this document relate specifically to toll fraud. This handbook is designed to work with the documentation provided for the products described in this document, and it is not intended as a replacement for the product documentation.

Trademarks

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Sending us comments

Avaya welcomes your comments about this book.

To reach us by:

- Mail, send your comments to:

  Avaya Inc.
  Product Documentation Group
  Room B3-H13
  1300 W. 120 St.
  Westminster, CO 80234 USA

- E-mail, send your comments to:

  document@avaya.com

- Fax, send your comments to:

  1-303-538-1741

Ensure that you mention the name and number of this book, Avaya™ Toll Fraud and Security Handbook, 555-025-600.

Introduction

2

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

Background

Telecommunications fraud is the unauthorized use of a company’s telecommunications service. This type of fraud has been in existence since the 1950s when Direct Distance Dialing (DDD) was first introduced.

In the 1970s, remote access capabilities became a target for individuals seeking unauthorized network access. Now, with the added capabilities of voice mail and automated attendant services, customer premises equipment-based toll fraud has expanded as a new type of communications abuse.

Today, security problems are not just limited to toll fraud. There have been sharp increases in reported incidents of hackers: criminals skilled in reprogramming computer systems, accessing telecommunications systems through remote administration or maintenance ports. These ports cannot be used to place phone calls, but hackers can gain control over the setup of the system. Through these ports, hackers create security “holes” to allow unauthorized calling — a serious form of electronic vandalism.

A company’s “information resources” are yet another target for modern criminals. They are invading voice mailboxes and eavesdropping on cellular phone calls to obtain proprietary information about your products or your customers.

Who is the enemy?

Hackers and phreakers

Hackers and “phreakers” (**ph**one f**reaks**) use personal computers, random number generators, and password-cracking programs to break into even the most sophisticated customer premises equipment-based system if it has not been adequately secured. Once a hacker penetrates a network and provides instructions to toll call sellers, large volumes of unauthorized calls can be made from the switch. Severe cases of communications abuse can also reduce revenue and productivity when employees are unable to dial out and customers are unable to call in.

These people are criminals, as defined by the United States Secret Service and Title 18 Section 1029 of the United States Criminal Code. They attempt to find your weakest link and break it. Once they have compromised your system, they will use your system resources to break into another system, and/or advertise that they have broken your system and how they did it. They will also sell this information to a call sell operator. Some hackers command up to $10,000.00 a week for stolen codes.

Call sell operations

Most of the high-dollar theft comes from call sell operations. These operations vary from a pay phone thief, who stands next to a pay phone and “sells” discount calls through **your system**, to a full-blown call sell operation.

A full-blown operation might involve a one-room apartment (rented under an assumed name) with 30 to 40 phones (lines from the phone company are under the same assumed name). The general pitch is that for a flat fee you can call anywhere in the world and talk as long as you like. The seller takes the money and places the call for the buyer, and then walks away so he will not get caught. Needless to say, a victimized company is paying for the actual call.

The call sell operation is open round-the-clock, and when the victimized company stops the abuse, the call sell operator moves on to the next number. In a month or two the call sell operator just disappears (and will usually resurface at another apartment with another 30 phones and a way into **your system**).

The toll fraud industry is growing fast. Originally, the majority of toll fraud was based in New York, NY. Now call sell operations are springing up in Miami, FL; Chicago, IL; Los Angeles and San Francisco, CA; and other locations around the country, even throughout the world.

Call sell operations are dependent on calling card numbers or other means to fraudulently use a customer premises equipment-based system. The major calling card vendors monitor calling card usage and shut down in a matter of minutes after detecting the fraud. However, call sell operators know that the traffic on most customer premises equipment-based systems is not monitored.

That is why a calling card on the street sells for $30.00 and a customer premises equipment-based system code (called a Montevello) sells for up to $3,000.00.

Drug dealers

Drug dealers want phone lines that are difficult to trace so they can conduct their illicit narcotic dealings. For this reason, drug dealers are more likely to route their calls through two or more communications systems (PBXs) or voice mail systems before a call is completed. This is called “looping.” Law enforcement officers believe that drug dealers and other criminals make up a sizeable chunk of toll fraud.

What is in a loss?

Cost of the phone bill

There are no real numbers showing exactly how much money companies have lost due to toll fraud. Since some companies are not willing to disclose this information, it is difficult to know who has been hit and at what cost. Both small and large companies have been victims of what is one of the nation’s most expensive corporate crimes.

Lost revenue

The cost of operational impact may be more severe than the toll charges. Employees cannot get outbound lines, and customers cannot call in. Both scenarios result in potential loss of business.

Expenses

Additional expenses may be incurred, such as changing well-known, advertised numbers, service interruptions, and loss of customer confidence.

Known toll fraud activity

Understanding how hackers penetrate your system is the first step in learning what to do to protect your company. Be aware that hackers communicate very well, are extremely resourceful, and are persistent. The following is a list of known methods hackers use to break into systems.

- PBX-based activity
  - **Maintenance port**

    Maintenance ports are the most recent target of abuse. In this scenario, hackers find a PBX maintenance port number with their "war dialer," a device that randomly dials telephone numbers until a modem or dial tone is obtained. They then "hack" the user ID and password, sometimes just by using the PBX default passwords, to enter your system. Good password selection decreases the possibility of being hacked via the maintenance port to virtually zero.

    This is the most dangerous type of abuse because once in your system, the hackers have control over all the administrative commands. While in your system, they have been known to:

    - Turn on Remote Access or Direct Inward System Access (DISA). (On some communications systems, this is a "yes" or "no" option.) These situations can be difficult to detect.

      Hackers have been known to change the system at 8:00 p.m. to allow fraudulent calls. Then, at 3:00 a.m., they reprogram the system back to its original configuration. One company was hit three weekends in a row before they realized what was happening.

    - Turn off Call Detail Recording (CDR) or Station Message Detail Recording (SMDR) and hack your system all weekend, and then turn it back on before Monday morning. This is especially disturbing to managers who are security conscious and check the CDR/SMDR reports every morning looking for suspicious activity. They will not see records of the calls because CDR/SMDR was turned off by the hackers. The administrator may notice the absence of CDR/SMDR records for evening, night, and weekend calls made by employees.

— **Voice mail**

There are two types of voice mail fraud. The first type, which is responsible for the bulk of equipment-related toll fraud loss, relies on misuse of the call transfer capabilities of voice mail systems. Once thieves transfer to dial tone, they may dial a Trunk Access Code (TAC), Feature Access Code or Facility Access Code (FAC), or extension number.

If the system is not properly secured, thieves can make fraudulent long distance calls or request a company employee to transfer them to a long distance number.

The second type of voice mail fraud occurs when a hacker accesses a mailbox to either take it over or simply access the information stored within it.

In the first situation, a hacker dials either 9 or a TAC that allows the call to be transferred to the outgoing facilities. In the second situation, a hacker typically hacks the mail password and changes it along with the greeting. This gives the hacker access to proprietary corporate information.

— **Automated attendant**

Auto attendants are used by many companies to augment or replace a switchboard operator. When an automated attendant answers, the caller is generally given several options. A typical greeting is: “Hello, you’ve reached XYZ Bank. Please enter **1** for Auto Loans, **2** for Home Mortgages. If you know the number of the person you are calling, please enter that now.”

In some Auto Attendants, option 9 is to access dial tone. In addition, when asked to enter an extension, the hacker enters 9180 or 9011. If the system is not properly configured, the automated attendant passes the call back to the PBX. The PBX reacts to 9 as a request for a dial tone. The 180 becomes the first numbers of a 1-809 call to the Dominican Republic. The 011 is treated as the first digits of an international call. The hacker then enters the remaining digits of the phone number and the call is completed. You, the PBX owner, pay for it. This hacker scenario works the same way with a voice mail system.

— **Remote access/direct inward system access (DISA)**

Remote access or DISA is designed to allow remote users to access a PBX to place long distance calls as if they were at the same site as the PBX. Because of the potential cost savings, many PBX owners use DISA instead of calling cards; however, remote access capability opens the door for fraudulent calls by thieves.

Hackers are able to locate the DISA feature with the use of a war dialer, explained previously. After finding a number, the device searches for barrier codes.

If the system allows uninterrupted, continuous access, a war dialer can crack a 6-digit code within 6 hours. The codes are then distributed via bulletin boards or pirated voice mailboxes, or are sold to call sell operators. Some systems hang up after a specified number of invalid access attempts, thereby extending the amount of time required to crack the code. However even if a hacker is disconnected, he or she may call back repeatedly in an attempt to crack the code.

- Network-based activities

  — **Shoulder surfing**

  Network hackers use video cameras in airports supposedly to take pictures of their family, but they are actually taking pictures of people using their calling cards. Hackers may also use an audio tape recorder to capture calling card numbers as they are spoken to an operator. This technique is known as “shoulder surfing.”

  — **Social engineering**

  “Social engineering” is a con game hackers frequently use. It is sometimes referred to as “operator deceit.” The success of this con requires gullibility or laxity on the part of the operator or employee, of which the hacker takes full advantage.

  For example, hackers call an employee, claim to have the wrong extension number, and ask to be transferred back to the operator. The call looks to the operator like an internal call. The hacker then asks for an outside line. Often, because operators do not know any better, they will connect the hacker to an outside line.

  Another example of social engineering is a hacker calling the operator and pretending to be a telephone maintenance repair person. They make statements like: “I am a qualified telephone repairman testing your lines. Please transfer me to 900 or 9#;” or “I need to verify your DID number range.” An untrained operator may provide the requested transfer or information, giving the hacker more ammunition with which to crack your system.

  — **Dumpster diving**

  Hackers obtain switch and security information by browsing through company trash cans. They are looking for discarded phone bills, corporate phone directories, and access codes. The “found” information can be used to make fraudulent calls.

  — **Alternate carrier access**

  If your system is not secure, hackers can dial out by using carrier codes that bypass routing restrictions you have placed on your primary carrier’s features.

— **Looping**

Looping is a method that call sell operators use to circumvent restrictions that IXCs (Interexchange Carriers) put in the networks to control calling card fraud. All carriers block calling card calls bound for the 809 area code (to the Dominican Republic) that originate in New York, NY. This is because the Dominican Republic is a common destination for stolen phone calls. If call sell operators are able to obtain a dial tone from a PBX but are not able to dial 809 or 011 directly, they will revert to looping. They could dial an 800 number outbound from the PBX. The 800 number could be to another PBX or could be a calling card or operator access number. Examples include, but are not limited to the following 800 numbers: 1 800 COLLECT, 1 800 CALLATT, and 1 800 GETINFO. They could also dial 950 carrier access numbers.

Lastly, they can dial various 101xxxx carrier access codes. In any case, they can still use the PBX to place a fraudulent call. If the PBX is not in New York, NY, they can use the calling card. Use of the 101xxxx codes could allow for direct billing to the PBX. It is not uncommon for hackers to “loop” through as many as five communications systems before completing the fraudulent call.

— **Call diverters**

A call diverter is a device used to forward calls to a different location, usually after business hours. These are normally used for smaller businesses who forward their calls to an answering service after hours.

When hackers find a number they suspect is using a call diverter, they call the number. When the call is answered, the hacker claims to have misdialed or remains silent. Then when the caller hangs up, the call diverter sometimes gives the hacker dial tone before the disconnect is completed. The hacker then seizes the dial tone and uses it to place fraudulent long distance calls.

— **Beeper and/or pager scam**

A scam directed at pagers and beepers is as follows. Many of the Local Exchange Carriers (LECs) have run out of numbers in the 976 prefix, so they are using other prefixes that work the same as 976. That is, the calling party gets charged for the call at a rate set by the owner of the number.

The fee charged for calling these numbers can range upwards of $250 per call. As already stated, the fee is set by the owner of the number. Unscrupulous people who own these numbers call around the country inserting these numbers into pagers to get the users to return the call so that they can collect the fee. The 976-look-alike numbers are constantly changing and expanding. Consult your LEC for a list of 976-look-alike numbers in your exchange.

This same scam could also easily apply to messages left on voice mail. The person could state, “I’m John Doe calling from XYZ. Please return my call at 212-540-xxxx.” When you return the call, you are charged $50.00.

Another slant to this scam is carried out by messengers who deliver parcels to your office. They will ask to use your company’s phone to call their office. Then they call one of these 976-look-alike numbers and stay on the line for a minute or two. Your company then gets the bill for a $250 call that lasted only a couple of minutes.

— **Internal abuse**

Unfortunately, not all toll fraud is generated from “outsiders.” Many times it can be traced to internal employees who either sell the information or abuse the system for their own gain.

— **Call forwarding off-premises**

Call forwarding can be programmed to forward calls internally (within the PBX) or off-premises. If off-premises call forwarding is allowed, unscrupulous employees can take advantage of it. They forward the phone to a number (usually their home number). They tell their friends and family to call the company’s 800 number and insert the employee’s extension number. The call is forwarded to the employee’s home phone, and the company foots the bill for the call.

IP security

3

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

Introduction

This section summarizes some of the security issues that arise in a converged data and telephony network environment. It also recommends some of the practices that can minimize the risk of toll fraud and other security breaches in a converged network.

More information about network security can be found on the Avaya support website at http://www.avaya.com/support.

In addition, refer to Chapter 20, ‘‘Links to additional security information’’.

Overview

As IP networks and telephony converge, companies may need to consider changes to their computer network to minimize the opportunity for perpetrators to compromise their IP telephony server or commit toll fraud. These changes range from simply monitoring IP traffic to physically isolating the IP telephony network from all other networks in the enterprise.

Although no network is perfectly protected from compromise by individuals with unethical intentions, there are practices that Avaya recommends to customers to assist in minimizing the chance of “crimes of opportunity” when a IP telephony server is placed on the enterprise network.

Mission-critical assets

Unlike a regular PC or print server on the network, the telephony server represents a mission-critical piece of equipment to the enterprise. As such, it needs to be treated in a manner that is commensurate with any other piece of equipment on the network that is needed for the ongoing operation of the enterprise.

Physical security

The telephony server should be kept in secure environment. Placing the server in a location that allows free access by any employee also allows those individuals the opportunity for disruption of the server and consequently the service. Keep the server isolated from all except those who need access.

Control networks

Avaya's telephony servers use private control networks. These networks transfer vital information for the ongoing operation of the server between it and its gateways or redundant systems. Do not integrate these private networks with any other networks on your enterprise. Physical separation is always best. In the case of VLANs, logical separation needs to be maintained.

Firewalls and routing

The telephony server provides the ability for administration of extensions and other user information via the network. The protocols and services of the server that are necessary to accomplish this should not be accessible to each telephony user in the enterprise. Company-managed firewalls and routers can restrict access to these administrative services to only certain compartments of the network or particular IP addresses. Firewalls, routers, and switches should be implemented in a way to compartmentalize the server from unauthorized access.

Customer-managed applications

The telephony servers have been customized to provide telephony services under the demands of telephony users. Additionally, high-availability has been a focus in the design of the server architecture. As part of the effort to provide a server that effectively works all of the time, Avaya has taken steps to remove software that is not mission-critical or necessary for the normal operation of the server. Incorporation of additional software (such as mail servers or virus scanners) and use of installed software for purposed not intended by Avaya is strongly discouraged.

Although Avaya appreciates the benefits of installing software that conforms to a company's security policy, we strongly recommend that no additional software be loaded onto the Avaya telephony server that could potentially disrupt the performance or operation of the server. The addition of third-party software could even provide for an opportunity compromise that was not previously present.

Administration and management

Companies can be provided administrative accounts to administer and manage the assignment of extensions and their class of service for the telephony system. Practices regarding administrative accounts of any mission-critical or proprietary enterprise system should similarly be pursued with respect the to the telephony server.

The number of accounts should be minimized. Passwords should be changed frequently. Accounts that are created should be assigned the lowest level of privileges necessary to accomplish their task. With respect to user accounts and extensions, all extensions should be reduced to the lowest level of service whenever an extension is not assigned to an employee or when an employee is suspected of toll fraud or leaves the company.

Software patches and upgrades

Avaya implements practices and procedures to ensure the products that are delivered are well designed and tested for quality. However, vulnerabilities may be discovered in software design or implementation that would represent an increased risk of compromise of the server. The best defense against these discovered vulnerabilities, and the best way to keep them from impacting the enterprise, is a proactive effort of education and currency of software.

Work with your Avaya representatives to understand the software that resides on your system. Stay abreast of advisories relative to the technologies that were used in the development of the telephony server. Work with your Avaya support organization to ensure that they have the ability to keep your server current with all upgrades and patches that are offered by Avaya.

These recommendations should be considered as good practice for minimizing the risk of compromise. They should be followed but they are not the only practices that should be considered because each company's network represents different challenges and different needs. You should constantly review the security practices your company pursues to minimize the opportunities of compromise. In addition, you should stay abreast of current practices in the computer industry for maintaining or improving security.

Additional information

For more information on update practices, recommendations or security advisories, please visit http://www.avaya.com/support.

Also refer to Chapter 20, ‘‘Links to additional security information’’ for information about security-related white papers, websites, and reference books.

Security risks

4

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

Overview

In order for your system to be secure against toll fraud, you need to address access, egress, and system administration. This handbook addresses those concerns. In addition, the risk of PBX-based toll fraud increases when any of the following products and features are used:

- Remote Access
- Automated Attendant
- Other port security risks
- Voice Messaging
- Administration and maintenance access
- Vectors associated with the DEFINITY ECS and DEFINITY communications systems

All these features offer benefits which allow companies to increase their availability to their customers and the productivity of their workforce. However, this chapter takes a look at these features from a different point-of-view: how can these features, when combined with other outgoing features, such as dial access to trunks, make a PBX system more vulnerable to toll fraud?

The remainder of this chapter discusses general security measures you can take to protect your system. Chapters 3 through 6 discuss the specific actions that help prevent these features from being the target of unauthorized use.

Remote access

Remote access, or direct inward system access (DISA), permits callers from the public network to access a customer premises equipment-based system to use its features and services. Callers dial into the system using CO, FX, DID, or 800 service trunks.

After accessing the feature, the user hears system dial tone, and, for system security, may be required to dial a barrier code, depending on the system. If a valid barrier code is dialed, the user again hears dial tone, and can place calls the same as an on-premises user.

For the DEFINITY ECS, DEFINITY G1 and G3, and for the System 75, incoming calls are routed to a remote access extension. For DEFINITY G2 and System 85, callers are connected to the Remote Access feature when they dial the number for an incoming remote access trunk group.

Different product releases have different restrictions, as follows. When a remote access call is answered, the caller can be requested to enter either a barrier code or an authorization code (the DEFINITY ECS, DEFINITY G1, G2.2 Issue 3.0 and later), G3, and System 75 R1V3 can require both) before calls are processed. When both maximum length barrier codes and authorization codes are required, hackers need to decipher up to 14 digits to gain access to the feature.

Hackers frequently call toll-free 800 numbers to enter customer premises equipment-based PBX systems so that they do not pay for the inbound calls. After they are connected, hackers use random number generators and password cracking programs to find a combination of numbers that gives them access to an outside facility.

Unprotected remote access numbers (those that do not require barrier codes or authorization codes) are favorite targets of hackers. After being connected to the system through the Remote Access feature, a hacker may make an unauthorized call by simply dialing 9 and the telephone number. Even when the Remote Access feature is protected, hackers try to decipher the codes. When the right combination of digits is discovered (accidentally or otherwise), hackers can then make and sell calls to the public.

For these reasons, all switches in the network should be protected. Refer to Chapter 5 for more information on remote access for the DEFINITY ECS, DEFINITY communications systems, System 75, and System 85. Refer to Chapter 6 for more information on remote access for the MERLIN II, MERLIN LEGEND, MERLIN Plus, PARTNER II, PARTNER Plus, and System 25 communications systems.

Automated attendant

Automated attendant systems direct calls to pre-designated stations by offering callers a menu of available options. Automated attendant devices are connected to a port on the main system and provide the necessary signaling to the switch when a call is being transferred. When hackers connect to an automated attendant system, they try to find a menu choice (even one that is unannounced) that leads to an outside facility.

Hackers also may try entering a portion of the toll number they are trying to call to see if the automated attendant system passes the digits directly to the switch. To do this, the hacker matches the length of a valid extension number by dialing only a portion of the long distance telephone number. For example, if extension numbers are four digits long, the hacker enters the first four digits of the long distance number. After the automated attendant sends those numbers to the switch and disconnects from the call, the hacker provides the switch with the remaining digits of the number.

Many voice messaging systems incorporate automated attendant features. The security risks associated with automated attendant systems are common to voice messaging systems as well. Refer to Chapter 8 for more information on securing automated attendant systems.

Other port security risks

Many of the security risks from voice mail, remote access, and automated attendant arise from allowing incoming callers to access outside facilities. However, there are other endpoints within your system that should also be denied to incoming callers. Many of these endpoints can be dialed as internal calls within the system, and can be reached from either voice mail, Auto Attendant, or Remote Access.

For example, the NETCON (Network Control) data channels provide internal access to the system management capabilities of the system and can be reached on a call transfer from an AUDIX Voice Mail System if not protected by appropriate restrictions. [See ‘‘Increasing product access (port) security’’ on page 4-6.] Any features or endpoints that can be dialed, but are to be denied to incoming callers, should be placed in restriction groups that cannot be reached from the incoming facility or from endpoints that could transfer a call.

Sophisticated modems being used today, if not protected, offer incoming callers the ability to remotely request the modem to flash switch-hook, returning second dial tone to the incoming caller. Modem pool ports need to be appropriately protected or otherwise denied access to second (recall) dial tone. Outgoing-only modem pools are at risk if they can be dialed as extensions from any of the remote access or voice mail ports as in the example above. (See ‘‘Recall signaling (switchhook flash)’’ on page 5-21.)

Voice messaging systems

Voice messaging systems provide a variety of voice messaging applications; operating similarly to an electronic answering machine. Callers can leave messages for employees (subscribers) who have voice mailboxes assigned to them. Subscribers can play, forward, save, repeat, and delete the messages in their mailboxes. Many voice messaging systems allow callers to transfer out of voice mailboxes and back into the PBX system.

When hackers connect to the voice messaging system, they try to enter digits that connect them to an outside facility. For example, hackers enter a transfer command (the AUDIX Voice Mail System uses * T), followed by an outgoing trunk access number for an outside trunk. Most hackers do not realize how they gained access to an outside facility; they only need to know the right combination of digits. See Chapter 7 for information on securing your voice messaging system.

Sometimes hackers are not even looking for an outside facility. They enter a voice messaging system to find unassigned voice mailboxes. When they are successful, they assign the mailboxes to themselves, relatives, and friends, and use them to exchange toll-free messages. Hackers can even use cellular phones to break into voice mailboxes. (See ''Protecting voice messaging systems'' on page 7-2.) In addition, unauthorized access to voice messaging systems can allow hackers to access the switch and change administration data. See ''Increasing product access (port) security'' on page 4-6.

Administration/maintenance access

Expert toll hackers target the administration and maintenance capabilities of customer premises equipment-based systems. Once criminals gain access to the administration port, they are able to change system features and parameters so that fraudulent calls can be made. The following measures can be taken to prevent high level access to system administration.

Changing default passwords

To simplify initial setup and allow for immediate operation, either the switch and adjuncts are assigned default administration passwords, or passwords are disabled, depending on the date of installation. Hackers who have obtained copies of customer premises equipment-based and adjunct system documentation circulate the known default passwords to try to gain entry into systems. To date, the vast majority of hacker access to maintenance ports has been through default customer passwords. Be sure to change or void all default passwords to end this opportunity for hackers.

The following is a list of customer logins for systems in this handbook that provide login capabilities. For information on password parameters, see the applicable system chapter. For information on how to change passwords, see Chapter 14.

- AUDIX Voice Mail System: **cust**
- AUDIX Voice Power System: **audix** (or **is** on the Integrated Solution-equipped system)
- DEFINITY AUDIX System: **cust**
- DEFINITY ECS, DEFINITY G1, G3V1, G3V2, and System 75: **cust, rcust, bcms**[1]**, browse*, NMS***
- Avaya INTUITY System: **sa**, **vm**
- MERLIN LEGEND Communications System: **admin** on Integrated Voice Response platform-supported systems
- MERLIN MAIL and MERLIN MAIL-ML Voice Messaging Systems: **1234**
- PARTNER MAIL and PARTNER MAIL VS Systems: **1234**
- System 25: **systemx5**

Choosing passwords

Follow the guidelines listed below when choosing passwords.

- Passwords should be as long as allowed. See the section specific to your system for maximum password length information.
- Passwords should be hard to guess and should not contain:
  - all the same characters (for example, 1111, xxxx)
  - sequential characters (for example, 1234, abcd)
  - character strings that can be associated with you or your business, such as your name, birthday, business name, phone number, or social security number
  - words and commonly-used names. Many of the war dialers used by hackers are programmed to try all of the names from books listing potential baby names. In one documented case, the contents of an entire dictionary were used to try and crack passwords.
- Passwords should use as great a variety of characters as possible. For example, if both numbers and letters are permitted, the password should contain both.
- Passwords should be changed regularly, at least on a quarterly basis. Recycling old passwords is not recommended.

1. Not available in System 75 R1V1 (**bcms** is not available in System 75 at all.)

Increasing adjunct access security

Since system adjuncts can be used to log in to otherwise “protected” systems, you also should secure access to the following products:

- G3 Management Applications (G3-MA)
- CSM (Centralized System Management)
- CMS (Call Management System)
- Manager III/IV
- Trouble Tracker
- VMAAP

Logins and passwords should be changed and managed in the same manner as the system being managed (for example, the switch or the AUDIX Voice Mail System). See ‘‘Administration security’’ on page 5-51 for additional information.

Increasing product access (port) security

You need to protect your security measures from being changed by the hacker who gains access to the administration or maintenance ports of your customer premises equipment-based system or its adjuncts. See ‘‘Logins for INADS port’’ on page 5-51.

If you use PC-based emulation programs to access administration capabilities, never store dial-up numbers, logins, or passwords as part of an automatically executed script.

For greater security, you may want to purchase and use the optional Remote Port Security Device (RPSD). The RPSD consists of two modem-sized devices, a lock, installed on the receiving modem (for example, at the PBX), and a key, which is placed on the originating modem (for example, at the remote administration terminal). The lock and key must match before a communication pathway is opened. Refer to Chapter 16 for more information.

The Access Security Gateway (ASG) software interface was integrated into the DEFINITY ECS Release 7.2 and included in all later releases, as well as the Intuity Release 5 software base. For more information on ASG, refer to Chapter 16.

Another area that may be vulnerable to toll fraud is the System 75 and the DEFINITY ECS, DEFINITY G1 and G3 (except G3r) NETCON data channel — the internal extension number that can be used for administration and maintenance access. If the NETCON data channel is not restricted, a hacker can do a valid transfer from the voice mail port (or other ports in the system) to the network extension, get dial tone, and connect to and log into the administrative port, bypassing any port protection device, such as an RPSD. In a modem pool or NETCON modem installation, this would permit a hacker to transfer to a NETCON extension, get data tone, and get a login prompt. In a modem pool installation, this would also permit the hacker to transfer out to make toll calls.

Use COR-to-COR restrictions to restrict stations from calling the NETCON so that only CORs allowed to access the maintenance port are able to do so. For example, if voice mail extensions have a COR of 9, and extensions assigned to NETCON channels have a COR of 2, ensure that COR 9 does not have access to COR 2. Anyone not authorized to use the NETCON channel should not be able to access it.

NOTE:
To determine how the NETCON channels have been assigned, use the **list data-module** command. The output from this command identifies the modules in your system. If NETCON extensions are administered, they will be listed as NETCON, along with the four 3- or 4-digit extension numbers associated with the data channel(s).

NOTE:
NETCON extensions may also be contained in a hunt group. If **list data-module** does not list the NETCON extensions, use **list hunt-group** to see if the NETCON data channels are in a hunt group.

NOTE:
For verification purposes, you may also enter **list data-module <extension>**, if you think you know the extension that is associated with the NETCON data channel. This command will list the COR, COS, Tenant Number, and name of the data module (for example, NETCON, TDM) associated with the extension you entered.

In addition, the modem port used for voice mail maintenance or administrative access is often a switch extension. It should be restricted in the same manner as the NETCON channel.

General security measures

General security measures can be taken system-wide to discourage unauthorized use.

Educating users

Everyone in your company who uses the telephone system is responsible for system security. Users and attendants need to be aware of how to recognize and react to potential hacker activity. Informed people are more likely to cooperate with security measures that often make the system less flexible and more difficult to use.

- Never program passwords or authorization codes onto auto dial buttons. Display phones reveal the programmed numbers and internal abusers can use the auto dial buttons to originate unauthorized calls.
- Discourage the practice of writing down passwords. If a password needs to be written down, keep it in a secure place and never discard it while it is active.
- Attendants should tell their system manager if they answer a series of calls where there is silence on the other end or the caller hangs up.
- Users who are assigned voice mailboxes should frequently change personal passwords and should not choose obvious passwords (see ‘‘Choosing passwords’’ on page 4-5).
- Advise users with special telephone privileges (such as remote access, voice mail outcalling, and call forwarding off-switch) of the potential risks and responsibilities.
- Be suspicious of any caller who claims to be with the telephone company and wants to check an outside line. Ask for a callback number, hang up, and confirm the caller’s identity.
- Never distribute the office telephone directory to anyone outside the company; be careful when discarding it.
- Never accept collect phone calls.
- Never discuss your telephone system’s numbering plan with anyone outside the company.

Establishing a policy

As a safeguard against toll fraud, follow these guidelines:

- Change passwords frequently (at least quarterly). Set password expiration times and tell users when the changes go into effect. Changing passwords routinely on a specific date (such as the first of the month) helps users to remember to do so.
- Establish well-controlled procedures for resetting passwords.
- Limit the number of invalid attempts to access a voice mail to five or less.
- Monitor access to the dial-up maintenance port. Change the access password regularly and issue it only to authorized personnel. Consider using the Remote Port Security Device. (Refer to Chapter 16 for additional information.)
- Create a PBX system management policy concerning employee turnover and include these actions:
  - — Delete all unused voice mailboxes in the voice mail system.
  - — If an employee is terminated, immediately delete any voice mailboxes belonging to that employee.
  - — If a terminated employee had remote access calling privileges and a personal authorization code, remove the authorization code immediately.
  - — If barrier codes and/or authorization codes were shared by the terminated employee, these should be changed immediately. Notify the remaining users as well.
  - — If the terminated employee had access to the system administration interface, their login ID should be removed (G3V3 or later). Any associated passwords should be changed immediately.
- Back up system files regularly to ensure a timely recovery should it be required. Schedule regular, off-site backups.

Physical security

You should always limit access to the system console and supporting documentation. The following are some recommendations:

- Keep the attendant console and supporting documentation in an office that is secured with a changeable combination lock. Provide the combination only to those individuals having a real need to enter the office.
- Keep telephone wiring closets and equipment rooms locked.
- Keep telephone logs and printed reports in locations that only authorized personnel can enter.
- Design distributed reports so they do not reveal password or trunk access code information.

Security goals tables

The following tables list the security goals for each communications system, and provide an overview of the methods and steps that are offered through the switches to minimize the risk of unauthorized use of the system.

- Table 4-1 on page 4-10 provides information for the DEFINITY ECS, DEFINITY communications systems, System 75, and System 85.
- Table 4-2 on page 4-14 provides information for the MERLIN II, MERLIN LEGEND, MERLIN Plus, and System 25 communications systems.
- Table 4-3 on page 4-19 provides information for the PARTNER II and PARTNER Plus communications systems.

Table 4-1. Security goals: DEFINITY ECS, DEFINITY communications systems, System 75 and System 85

Security Goal	Method	Security Tool	Steps
Protect Remote Access feature	Limit access to authorized users	Barrier codes	Set to maximum length Set COR/COS
		Authorization codes	Set to maximum length Set FRL on COR
	Use VDNs to route calls	Call vectoring (G2 and G3 only)	Administer call vectoring (G3 only) Use CORs to restrict calling privileges of VDNs
	Limit times when Remote Access is available	Night service (G1, G2, G3, and System 75 only)	Administer night service
		Shared trunk group (System 85 only)	Assign shared trunk group

Continued on next page

Table 4-1. Security goals: DEFINITY ECS, DEFINITY communications systems, System 75 and System 85 — *Continued*

Security Goal	Method	Security Tool	Steps
	Suppress dial tone after barrier code entered	Suppress remote access dial tone — (G1, G3 and System 75 R1V3 require the concurrent use of authorization codes)	Turn off dial tone (See Remote Access screen)
Prevent unauthorized outgoing calls	Limit calling area	AAR/ARS Analysis	Set FRL Set COR
		Digit conversion (G1, G2, G3, and System 85 only)	Administer digit conversion
		Toll analysis (G1, G3, and System 75 only)	Identify toll areas to be restricted
		FRLs	Limit access to AAR/ARS route patterns by setting to lowest possible value
Prevent unauthorized outgoing calls (continued)	Restrict phones from making outbound calls	Attendant-controlled voice terminals (G2 and System 85 only)	Place phones in attendant-controlled group
	Limit outgoing calls	FRLs	Restrict tie trunk usage Deny access to AAR/ARS/WCR
		Authorization codes	Set to maximum length Set FRL on COR

Continued on next page

Table 4-1. Security goals: DEFINITY ECS, DEFINITY communications systems, System 75 and System 85 — *Continued*

Security Goal	Method	Security Tool	Steps
	Limit calling permissions	COS (G2 and System 85 only)	Set COS restrictions
		COR (G1, G3, and System 75 only)	Set FRL Set calling party restrictions or outward restrictions Set COR to COR restrictions
	Require account code before calls	Forced entry of account code	Set account code length Administer as required
	Create time-dependent limits on access to route patterns	Alternate FRL (G2 and G3r only)	Set lowest value possible
	Suppress dial tone after ARS/WCR feature access code	Suppress dial tone	Turn off ARS/WCR dial tone
	Screen all AAR/ARS calls	World class routing (G2.2 and G3 only)	Administer all capabilities

Continued on next page

Table 4-1. Security goals: DEFINITY ECS, DEFINITY communications systems, System 75 and System 85 — *Continued*

Security Goal	Method	Security Tool	Steps
Prevent exit from voice messaging system	Limit calling permissions	COR (G1, G3, and System 75 only)	Set low FRL Set calling party restrictions or outward restrictions Set COR to COR restrictions
		COS (G2 and System 85 only)	Set calling party restrictions
	Restrict outgoing toll calls	Toll analysis (G1, G3, and System 75 only)	Identify toll areas to be restricted
	Prevent transfer to dial tone[1] (for AUDIX, DEFINITY AUDIX, and Avaya INTUITY voice mail systems only)	Station restrictions	Turn off transfer feature
		Enhanced Transfer (G1 Issue 5.0, G2, G3, System 75 R1V3 Issue 2.0 and later, and System 85 R2V4 and later)	Set Transfer Type= "Enhanced" (only for Avaya PBX switches)
		Basic transfer	Set Transfer Restriction= "Subscribers"[2]

Continued on next page

Table 4-1. Security goals: DEFINITY ECS, DEFINITY communications systems, System 75 and System 85 — *Continued*

Security Goal	Method	Security Tool	Steps
Prevent exit from automated attendant service	Limit calling permissions	COR (G1, G3, and System 75 only)	Set low FRL Set calling party restrictions or outward restrictions Set COR to COR restrictions
		COS (G2 and System 85 only)	Set COS restrictions
	Limit exit to outgoing trunks	FRL	Set lowest possible value
	Restrict outgoing toll calls	Toll Analysis (G1, G3, and System 75 only)	Identify toll areas to be restricted

1. Methods are listed in decreasing order of importance, relative to security.
2. Basic transfer with Transfer Restriction = Digits allows access to dial tone.

Table 4-2. Security goals: MERLIN II, MERLIN LEGEND, MERLIN Plus, and System 25 communications systems

Security Goal	Method	Security Tool	Steps
Protect Remote Access feature	Limit access	Barrier codes	Set max length
		Authorization codes (MERLIN LEGEND Communications System R3 only)	Set max length
	Turn off Remote Access when not needed	Remote access administration	Deactivate feature

Continued on next page

Table 4-2. Security goals: MERLIN II, MERLIN LEGEND, MERLIN Plus, and System 25 communications systems — *Continued*

Security Goal	Method	Security Tool	Steps
Prevent unauthorized outgoing calls	Limit calling permissions	Switch dial restrictions	Set outward/toll restrictions Set allowed/ disallowed lists
	Limit access to ARS route patterns	Facility restriction level (FRL) (System 25 and MERLIN LEGEND Communications System only)	Set lowest possible value
	Ensure the integrity of assigned call restrictions on loop start facilities	Automatic call restriction reset (MERLIN Plus Communications System only)	Activate feature
	Turn off Remote Access when not needed	Remote access administration (System 25 and MERLIN LEGEND Communications System only)	Deactivate feature
		Deactivate feature (MERLIN Plus Communications System R2 only)	Program feature button
		Remote access administration (MERLIN II Communications System only)	Deactivate feature from administration

Continued on next page

Table 4-2. Security goals: MERLIN II, MERLIN LEGEND, MERLIN Plus, and System 25 communications systems — *Continued*

Security Goal	Method	Security Tool	Steps
Protect remote system programming	Require password to access system programming	System programming password (MERLIN LEGEND Communications System and System 25 only)	Set password
Protect remote call forwarding	Set limit for how long a forwarded call can last	Automatic timeout (MERLIN Plus Communications System R2 only)	Administer a time limit
	Turn off remote call forwarding when not needed	Deactivate feature (MERLIN Plus Communications System R2 only)	Turn off feature from administration
	Drop outgoing line at end of call	Ground start facilities (MERLIN LEGEND Communications System and System 25 only)	Install/administer ground start facilities

Continued on next page

Table 4-2. Security goals: MERLIN II, MERLIN LEGEND, MERLIN Plus, and System 25 communications systems — *Continued*

Security Goal	Method	Security Tool	Steps
Prevent exit from voice messaging system	Limit calling permissions	Switch dial restrictions (System 25, MERLIN II, and MERLIN LEGEND communications systems only)	Set outward/toll restrictions Set allowed/ disallowed lists
		FRLs (System 25 and MERLIN LEGEND communications systems only)	Set lowest possible value
	Restrict transfer to registered subscribers only	Transfer restrictions (MERLIN MAIL R3 Voice Messaging System only)	Choose the Transfer to Subscribers Only option
Prevent unauthorized use of facilities	Limit access to ARS route patterns	FRLs	Set lowest possible value
	Restrict who can use outcalling	COS (MERLIN MAIL, MERLIN MAIL-ML, and MERLIN MAIL R3 voice messaging systems only)	Select a COS that does not permit outcalling

Continued on next page

Table 4-2. Security goals: MERLIN II, MERLIN LEGEND, MERLIN Plus, and System 25 communications systems — *Continued*

Security Goal	Method	Security Tool	Steps
Prevent theft of information via voice messaging system	Assign secure passwords	Passwords	Encourage users to select non-trivial, maximum-length passwords
	Administer minimum password length	Passwords (MERLIN MAIL R3 Voice Messaging System only)	Administer a minimum password length of at least 6 digits
	Set number of consecutive unsuccessful login attempts before mailbox is locked	Security violation notification (MERLIN MAIL R3 Voice Messaging System only)	Use the Mailbox Lock or Warning Message option, set to a low threshold

Table 4-3. Security Goals: PARTNER II and PARTNER Plus communications systems

Security Goal	Method	Security Tool	Steps
Protect Remote Access[1]	Do not use unattended mode	Attended mode (RAU)	None (Attended mode is system default)
Prevent exit from voice messaging system	Restrict who can dial out	Switch dial restrictions	Use line access restrictions, outgoing call restrictions, allowed lists, and disallowed lists

Continued on next page

Table 4-3. Security Goals: PARTNER II and PARTNER Plus communications systems — *Continued*

Security Goal	Method	Security Tool	Steps
Prevent theft of information via voice messaging system	Assign secure passwords	Passwords (PARTNER Plus Communications System R3.1 and later, and PARTNER II Communications System R3 and later)	Encourage users to select non-trivial, maximum-length passwords
	Administer minimum password length	Passwords (MERLIN MAIL R3 Voice Messaging System only)	Administer a minimum password length of at least 6 digits
	Restrict who can use outcalling	COS	Select a COS that does not permit outcalling
	Set number of consecutive unsuccessful login attempts before mailbox is locked	Security Violation Notification (MERLIN MAIL R3 Voice Messaging System only)	Use the Mailbox Lock or Warning Message option, set to a low threshold
Prevent unauthorized use of facilities	Restrict who can dial out	Switch dial restrictions	Use line access restrictions, outgoing call restrictions, allowed lists, and disallowed lists; assign to VMS hunt group extensions

1. The risk of toll fraud applies only if the Remote Administration Unit (RAU) is installed with the PARTNER II or PARTNER Plus Communications System.

Large business communications systems

5

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

This chapter provides information on protecting the following:

- Communications Manager
- MultiVantage™ Software
- DEFINITY ECS Release 5 and later
- DEFINITY communications systems
- System 75
- System 85

The first section of this chapter, ‘‘Keeping unauthorized third parties from entering the system’’ details the major ways third parties enter the system and tells how to keep them from doing so. The second section, ‘‘Tools that restrict unauthorized outgoing calls’’details features within the system that prevent unauthorized egress from the system. The third section, ‘‘Security measures’’ tells how to use the tools described in the preceding section. The final section, ‘‘Detecting toll fraud’’ details methods for monitoring the system and determining the effectiveness of the security measures you implemented.

Other chapters detail additional security measures to protect your equipment:

- Chapter 7 contains security measures to protect the attached voice messaging system. For general security measures, refer to ‘‘Protecting voice messaging systems’’ on page 7-2. For product-specific security measures, refer to ‘‘Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY communications systems, System 75,and System 85’’ on page 7-4.

- Chapter 8 contains security measures to protect the Automated Attendant feature of your communications system. See “Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.” on page 8-1.
- Chapter 13 provides instructions for administering the features of the DEFINITY G3V3 and later, specifically designed to provide protection from toll fraud.
- Chapter 16 describes “Securing DEFINITY systems (Release 7.2 and Later) with Access Security Gateway” on page 16-4.

Keeping unauthorized third parties from entering the system

The major ways in which unauthorized third parties gain entry into the system are as follows:

- Remote access
- Remote maintenance port
- Vectors
- Transfers from adjunct systems, including voice mail systems, call prompters, and voice response systems

Protecting the Remote Access feature

Remote access, or direct inward system access (DISA), allows callers to call into the PBX from a remote location (for example, a satellite office or while traveling) and use the system facilities to make calls. When properly secured, the Remote Access feature is both cost-efficient and convenient. However, every security measure has an offsetting level of inconvenience for the user. These inconveniences must be weighed against the possible risk of toll fraud.

Security tips

- Evaluate the necessity for remote access. If this feature is not vital to your organization, consider deactivating the feature. If you need the feature, use as many of the security measures presented in this chapter as you can.
- Use a unpublished telephone number for this feature. Professional hackers scan telephone directories for local numbers and 800 numbers used for remote access. Keeping your remote access number out of the phone book helps prevent it from getting into the wrong hands. Avoid administering a night service destination to remote access on any published number.
- Keep an authorized user list and reevaluate it on a need-to-have basis.

- If possible, administer remote access (Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75) so no dial-tone prompt is supplied for entry of the authorization code. No dial tone after a remote access call is connected discourages most hackers who listen for dial tone or use modems to detect dial tone.
- Restrict the bands or area code sets when you offer remote access on an 800 number. If all your authorized users are on the east coast, for example, do not provide trunks that allow calling in from San Francisco.
- Require maximum length barrier codes and authorization codes. For System 75 R1V1 and R1V2, require the entry of a barrier code. For System 85 and releases of DEFINITY G2.1 and G2.2 prior to 3.0, require either a barrier code or an authorization code. For DEFINITY G2 and System 85, require the entry of 11 digits (4-digit barrier code and 7-digit authorization code). For DEFINITY G1, G2.2 Issue 3.0 and later, DEFINITY G3, Communication Manager, MultiVantage™ Software, DEFINITY ECS, and System 75 R1V3, require the entry of 14 digits (a 7-digit barrier code and a 7-digit authorization code) before users can gain access to the feature.
- Do not assign barrier codes or authorization codes in sequential order. Assign random number barrier codes and authorization codes to users so if a hacker deciphers one code, it will not lead to the next code.
- Since most toll fraud happens after hours and on week-ends, restrict the hours that remote access is available.

Disabling/removing the Remote Access feature

For the “n” versions of DEFINITY G1, G2.2 Issue 3.0 and later, DEFINITY G3, Communication Manager, MultiVantage™ Software, DEFINITY ECS, System 85 R2V4n, and System 75 R1V3, as an additional step to ensure system security, the Remote Access feature may be “permanently” disabled if there is no current or anticipated need for it. Permanent removal protects against unauthorized usage even if criminals break into the maintenance port. Once this feature is permanently disabled, however, it will require Avaya maintenance personnel intervention to reactivate the feature.

See your account representative for information on the North American dialing plan, and on the “n” upgrade. See Chapter 12 for procedures to permanently disable the Remote Access feature.

Tools to protect the Remote Access feature

You can help prevent unauthorized users from gaining access to the PBX system by using the following tools. (See Table 5-1.)

Table 5-1. Security tools for Remote Access feature

Security Tool	Switch	Page #
Barrier code	All	5-5
Authorization code	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 85, and System 75 (R1V3)	5-8
Feature access code administration	All	5-9
Trunk administration	All	5-9
Remote access dial tone	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 85, and System 75 (R1V3)	5-10
Night service	All	5-10
Call vectoring	Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3	5-10
Call prompting/ASAI*	Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G2 and G3	5-11
Barrier code aging/access limits	DEFINITY G3V3 and later	5-67

Continued on next page

Table 5-1. Security tools for Remote Access feature — *Continued*

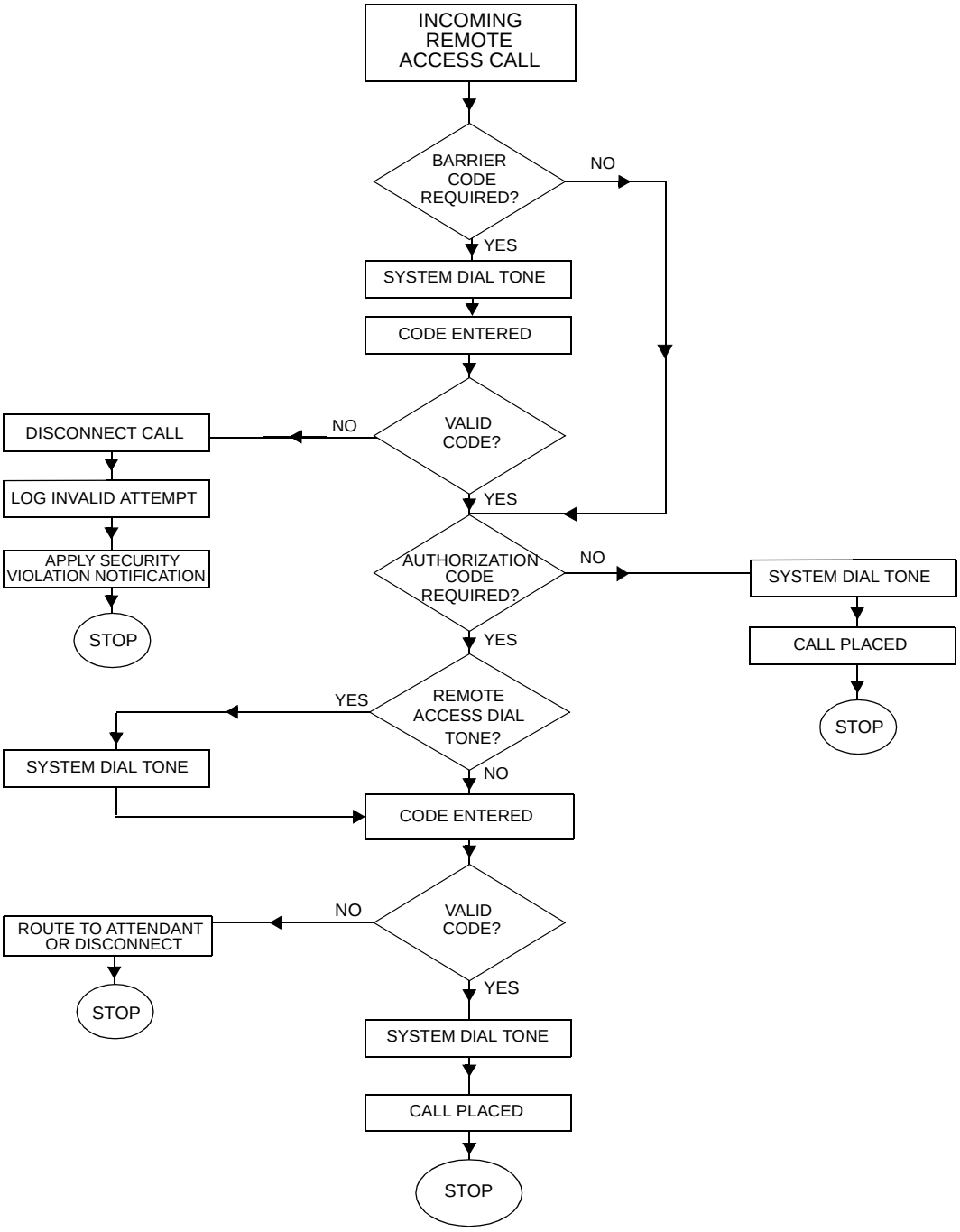
Security Tool	Switch	Page #
Security violation notification (SVN)	Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3	5-59
status remote-access command	DEFINITY G3V4 and later	5-12
Logoff screen enhancements	DEFINITY G3V4 and later	5-12

*For ASAI, see the applicable product feature description.

Barrier codes

Figure 5-1 illustrates how barrier codes and/or authorization codes can provide added security for remote access calls. Refer to this flowchart as necessary throughout the sections on barrier codes and authorization codes.

Figure 5-1. Remote access call path



For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, you can assign up to 10 barrier codes to provide the first checkpoint. When barrier codes are required for remote access, callers hear a special dial tone, and then must enter a valid barrier code before they can access the PBX system.

NOTE:
With Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75 R1V3, you can require the entry of an authorization code after the barrier code prior to callers receiving system dial tone for placing calls.

Barrier codes can be up to seven digits (use all seven for maximum security). Each barrier code can be assigned a different Class of Restriction (COR) and Class of Service (COS) to identify the calling privileges available to the user who enters it. For remote access calls, dialing a barrier code overrides the COR set for the incoming facility; if no barrier code is required, the default COR on the trunk group is used.

NOTE:
The COS assigned to the barrier code should be set to `console permission =` **n**.

For DEFINITY G3V3 and later, the Remote Access Barrier Code Aging feature provides a means of limiting the time that remote access barrier codes are valid, and/or specifying the number of remote access calls that can be placed per barrier code. The ability to define a barrier code's lifespan and automatically retire it at the end of its usefulness, or to specify the number of times it can be used before it is retired can significantly reduce the opportunity for unauthorized, fraudulent use of the Remote Access feature. For more information, see ''Remote access barrier code aging/access limits (DEFINITY G3V3 and Later)'' on page 5-67, and ''Administering barrier code aging'' on page 13-11.

For DEFINITY G3V3 and later, the security violation notification feature alerts the switch administrator of a login violation. When a violation is detected for a valid login ID, the login ID is disabled, prohibiting its further use until the security violation is investigated and the login ID re-enabled. For more information, see ''Administering the Login ID Kill After N Attempts feature'' on page 13-7.

For DEFINITY G3V4 and later, the Remote Access Notification feature provides automatic reporting when remote access is in use. For more information, see ''Adding customer logins and assigning initial password'' on page 13-13.

For DEFINITY G2 and System 85, either a barrier code or an authorization code (see below) can be required before callers can access switch features or trunks. There is only one 4-digit barrier code for the Remote Access feature. This can be changed using a feature access code, and is normally assigned by the attendant. When callers enter the wrong barrier code, the calls are given intercept treatment. (When no barrier code is entered, the call can be routed to an attendant.) A barrier code should be used to screen entry into this feature; authorization codes can then be used to screen outgoing calls on Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), and World Class Routing (WCR) (G2.2) trunks.

Authorization codes[1]

NOTE:
For all systems, once established, the number of digits (four to seven) in the authorization code remains fixed unless all codes are removed and re-entered. All authorization codes used in the system must be the same length.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75 R1V3, the calling privileges of an authorization code overrides the privileges established by the barrier code. With remote access calls, dialing an authorization code overrides the COR set for the barrier code. Individual users should be assigned unique authorization codes from four to seven digits (use all seven for maximum security).

Authorization codes serve as a second layer of protection when combined with barrier codes for the Remote Access feature. When authorization codes are required, the caller hears a special dial tone (optional) and must then enter a valid authorization code to access the system.

NOTE:
If a remote access caller is to be restricted from long distance but allowed other ARS calls (for example, local), then the authorization code COR should have an appropriately low FRL.

NOTE:
Authorization codes are also recorded by the PBX's call detail recording feature (SMDR/CDR), allowing for call verification by the individual assigned the authorization code. Proper security must be followed to protect any printed copies of the call records.

1. Authorization codes are standard only in System 85 and DEFINITY G2. They are an option for System 75 R1V3, DEFINITY G1, and G3, Communication Manager, MultiVantage™ Software, and DEFINITY ECS require the customer to purchase the appropriate right to use.

For DEFINITY G2 and System 85, authorization codes can replace barrier codes on incoming remote access facilities or can be used to screen outgoing calls on AAR/ARS/WCR trunks. Only authorization codes with the Network Access Flag set are permitted to make outgoing calls.

The authorization code option requires that the caller enter a valid authorization code to receive switch dial tone. The authorization code used for remote access has an FRL value used by AAR/ARS/WCR trunks for outgoing calls [see "Facility restriction level" on page 5-19]. Up to 5,000 authorization codes can be issued to System 75 R1V3 and DEFINITY G1 users, and up to 90,000 for System 85, DEFINITY G2, and G3 users. However, it is best to keep the number of authorized users to a minimum.

To maximize the security of the system, follow these steps:

- When assigning authorization codes, give the users the lowest possible FRL needed for their calling requirements.
- Be sure to remove any unused authorization codes from the system, including those assigned to employees who have changed assignments or left the company.
- Assign each authorization code the minimum level of calling permissions required.
- Make authorization codes nonconsecutive (random).
- Administer each authorization code to the maximum length allowed by the system (7 digits).

NOTE:
When a call directed to a VDN points to a vector containing a Route To step, and that Route To step attempts to utilize an authorization code, the call will be denied.

Feature access code administration

Certain feature access codes may facilitate egress from the system and should be used with care. These include: Data Origination, Data Privacy, Data Restriction, Abbreviated Dialing, ARS/AAR, Call Forwarding, and Facility Test Calls.

Trunk administration

When trunk groups are administered, they are assigned a Trunk Access Code (TAC). Unless they are needed, prohibit both direct-dial access and facility test call access to trunk groups. This prevents callers from using TACs to obtain an outgoing trunk.

Remote access dial tone

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75 R1V3, when a user reaches the remote access port, if authorization codes are administered and barrier codes are not used, the system can be administered so the caller will hear a dial tone, a remote access tone, or silence as a prompt for the authorization code.

Night service

You can control the time of day the Remote Access feature is available by using the Night Service feature. This limits the amount of time remote access is available and thus reduces risks.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, trunks translated for remote access can be given a night service destination. Although it is not recommended, trunks accessing the system can be assigned a remote access extension as a night service destination. The system will change to either allow or deny access for a feature. A night service button can be assigned to implement this capability. When night service is activated for these trunk groups, the Remote Access feature is available. When night service is deactivated, calls can be routed to an attendant for handling.

For DEFINITY G2 and System 85, when the Remote Access feature is “shared” with Listed Directory Number (LDN) service, a remote access call is routed to the attendant under normal (business hours) conditions, and the attendant extends the call like any other LDN call. When Unattended Console Service is active, “shared” non-DID LDN service becomes inactive, and remote access calls are handled as direct dialed access calls. In effect, with “shared” non-DID LDN service, the Remote Access feature is turned off while the attendant is on duty. This provides a degree of security for remote access during normal business hours by allowing the attendant to screen remote access calls before extending them.

Call vectoring (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3)

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, administering access to the Remote Access feature through the use of Vector Directory Numbers (VDNs) can help make the feature more secure. Call vectoring allows incoming and internal calls to be processed according to a programmed set of vector commands.

To restrict the use of the Remote Access feature at night, a DID/DNIS VDN can be translated to route to a vector that has a step to route to the remote access extension. The vector can check time of day and day of week to route the call to an announcement or intercept tone if remote access is not allowed at certain times.

Protecting vectors that contain call prompting

Hackers try to enter unanticipated digit strings and deceive the switch into transferring the call to a dial tone source. The Call Prompting feature can collect digits from the user and route calls to a destination specified by those digits and/or do conditional processing according to the digits dialed. Examples of destinations include:

- On-premises or off-premises destinations
- A hunt group or split
- A specific call treatment such as an announcement, forced disconnect or delay treatment

Calls access call vectors, or the different destinations, by means of VDNs, “soft” switch extensions not assigned to a physical equipment location but having many of the properties of a normal extension number, including a COR. The VDN, when dialed (or inferred), routes calls to the vector. ***Calls processed by the vector carry the permissions and restrictions associated with the COR of the VDN***.

In order to deny incoming callers access to outgoing facilities, including tie lines, configure the COR of the VDN to prohibit outgoing access. To do this, follow the steps listed below. Also see ‘‘Trunk-to-trunk transfer’’ on page 5-23.

- Assign a Calling Party Restriction of “Outward” and deny Facility Test Call capability.
- Lower the FRL in the COR to the lowest acceptable value and use COR-to-COR restrictions to deny access to specific outgoing trunk groups. (FRL=0 would deny access to network routing preferences.)
- Block access to specific CORs assigned to outgoing trunk groups by using the Calling Permissions section of the Class of Restriction screen.

For Communication Manager, MultiVantage™ Software, Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, use of Call Vectoring with Prompting for remote access allows the PBX to require a touch-tone response before the caller hears a remote access dial tone. If no response is given, the call can be routed to an attendant, announcement, or intercept tone. This makes it more difficult for hackers to detect a remote access port.

NOTE:
Avaya strongly recommends, for both security and performance reasons, that the Ethernet connectivity between the MFB and the set of hosts with which it will communicate be a separate LAN segment. Otherwise, an unscrupulous person could gain unauthorized access to the DEFINITY LAN Gateway application in order to commit toll fraud and/or tamper with the real-time aspects of CTI applications.

For additional information, refer to *CallVisor ASAI Over the DEFINITY LAN Gateway*, 555-230-223.

Command: status remote-access

For DEFINITY G3V4 and later, the **status remote-access** command provides the status of the Remote Access feature. The display provides data on whether or not a barrier code has expired, the expiration date and time of the barrier code, the cause of the expiration, whether remote access is disabled (SVN or command), the time and date when it was disabled, and barrier codes.

Logoff screen notification

For DEFINITY G3V4 and later, a notification is provided on the logoff screen that identifies when remote access is enabled and when the Facility Test Call feature access code is active. The user has the option of acknowledging these notifications.

Use of the acknowledgment option is strongly recommended for those systems utilizing both the Remote Access and Facility Test Call (for notification if the feature is inadvertently left enabled) features, or those systems requiring notification if Facility Test Call is linked to hacking activity.

Tools that restrict unauthorized outgoing calls

Use the following tools to prevent fraudulent calls and monitor long distance usage. (See Table 5-2.)

Table 5-2. Security tools for outgoing calls

Security Tool	Switch	Page
Class of restriction	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75	5-14
Class of service	All	5-17
Facility restriction levels	All	5-19
Alternate facility restriction levels	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G2, G3, and System 85	5-19
Toll analysis	Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3	5-19
Free call list	All	5-20
AAR/ARS analysis	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2.1, G3, System 75, System 85	5-20
ARS dial tone	All	5-20
Station restrictions	All	5-20
Fully restricted service	All	5-31
Recall signaling	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75	5-21
Attendant-controlled voice terminals	All	5-21

Continued on next page

Table 5-2. Security tools for outgoing calls — *Continued*

Security Tool	Switch	Page
Restrictions—individual and group-controlled	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75	5-21
Central office restrictions	All	5-22
Restricting incoming tie trunks	All	5-22
Monitoring trunks	Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1 and G3	5-46
Terminal translation initialization	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G2, G3r, G3V2, System 85	5-46
Authorization codes	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 75 (R1V3), System 85	5-22

Class of restriction

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, the class of restriction (COR) places calling permissions and restrictions on both the calling party and the called extension. Up to 64 CORs can be defined in the system.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G3rV1, G3i-Global, and G3V2, the number of CORs has been increased to 96. For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3V3, each COR may be assigned a unique name via the Class of Restriction screen. CORs are assigned to trunks, stations, authorization codes, attendant consoles (as a group), remote access barrier codes, and loudspeaker paging access zones. CORs provide or prevent the ability to make specific types of calls or calls to trunks and stations with other specified CORs.

You can use the COR calling permissions (COR-to-COR restrictions) that set calling permissions on the COR to disallow stations to access trunks, and to disallow trunk groups to access other trunk groups. The COR also assigns FRLs for use by WCR/AAR/ARS routing.

NOTE:
When a call is routed to a VDN, the COR of the VDN determines where the call can be routed. If the COR is not restricted and the vector contains a collect digit step, the caller could dial 9 or a TAC and be routed out of the system to the network.

For DEFINITY G3 systems prior to DEFINITY ECS Release 5, as well as for G1 and System 75 systems, the default value of the FRL field on the COR screen is 7. Starting with DEFINITY ECS Release 5, the default value of the field is **0**. This is true for all CORs except for CORs 10 through 17, whose defaults are **0** through **7**, respectively. These defaults help ensure that FRLs with greater calling privileges are assigned only when appropriate.

To help maximize system security, follow these steps:

- Assign a separate COR to incoming and outgoing trunk groups, and then restrict calling between the two groups.
- Limit the calling permissions as much as possible by setting appropriate calling party restrictions and FRLs.
- Restrict the port COR of adjuncts from accessing the trunk group CORs.

Calling party and called party restrictions

For DEFINITY G3 systems prior to DEFINITY ECS Release 5, as well as for G1 and System 75 systems, the default value of the `Calling Party Restriction` field on the COR screen is **none**. Starting with DEFINITY ECS Release 5, the default value of the field is **outward**. This default ensures that the ability to place calls that access public network facilities is assigned only when appropriate.

The following restrictions can be placed on the originating station or trunk:

- Outward Restricted: cannot make public network calls via AAR/ARS or TACs. Calls can be placed to internal stations, to tie trunks via TACs, and off-switch via the Uniform Dial Plan (UDP).

  NOTE:
  Some states require that all telephones be able to dial emergency numbers, such as 911.

- Toll Restriction: cannot make toll calls unless the numbers are specified on an unrestricted call list. For G3, you can specify if the restriction applies to all toll calls or only TAC toll calls over CO/FX trunks.

  NOTE:
  The switch identifies all public network calls with 0 or 1 as the first or second digit as toll calls. For G3, toll calls and private network calls are defined on the Toll Analysis screen. For G2.2, only the first digit, 0 or 1, identifies it as a toll call.

- Code Restriction: for DEFINITY G1 and System 75, denies outgoing calls to selected office and area codes administered in the code table.
- Fully Restricted: for Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, denies outgoing calls, including dial access to trunks. Allows no incoming calls via public network trunks. See also "Fully restrict service" on page 5-31.

COR-to-COR restrictions/calling permissions

If it is not practical to dial-access-restrict outgoing or two-way trunk groups, then COR-to-COR restrictions should be used to prevent direct access to those trunk groups. These restrictions can give no calling permissions to CORs assigned to trunk groups or data stations.

The following options are available:

- Voice terminal—Public Restriction: restricts callers at specified voice terminals from receiving public network calls. A denied call is routed to an intercept tone, a recorded announcement, or the attendant.

  Calls can redirect to a public-restricted voice terminal. The COR of the originally called extension number is the only one checked.

- Voice Terminal—Termination Restriction: restricts voice terminal users on specified extension numbers from receiving any calls. However, voice terminal users can originate calls. Direct inward dialing or advanced private line termination calls are routed to a recorded announcement or the attendant.

  NOTE:
  When a call is to a VDN extension, the COR of the caller and the VDN are compared to determine if the associated call vector can be accessed. After the vector is accessed, the COR of the VDN is used for further call permission checking. See also "Restriction override (3-way COR check)" on page 5-17.

Restriction override (3-way COR check)

The Restriction Override feature, which is available only with DEFINITY G3i-Global and G3V2 and later, determines whether or not there is a 3-way COR check made on conference and transfer calls.

For DEFINITY G3 systems prior to DEFINITY ECS Release 5, as well as for G1 and System 75 systems, the default value of the `Restriction Override` field on the COR screen is **all**. Starting with DEFINITY ECS Release 5, the default value of the field is **none** for all CORs. This helps ensure that the feature is assigned only when appropriate.

If `Restriction Override`=**all**, only the controlling party's COR is checked against the CORs of all other parties on the conference and/or transfer call for station-controlled transfers and conferences, not attendant-controlled conferences and attendant-extended calls. If `Restriction Override`=**none**, the new party's COR is always checked against the CORs of all other parties on attendant extended calls and attendant-controlled conferences, as well as on all station-controlled conferences and transfers.

Class of service

For DEFINITY G2 and System 85, station access to various switch features is controlled by options in the Class of Service (COS) associated with the extension number. The following COS options are related to toll fraud prevention:

- Call Forward Off-Net: allows a user to call forward outside the switch to non-toll locations (G2.1). In G2.2, the user may be allowed to forward to a toll location (including international destinations), depending on the permissions and restrictions for that extension, as defined in **PROC000, WORD3, FIELD7**.
- Call Forward Follow Me: allows a user to forward calls outside the switch when other options are set.
- Miscellaneous Trunk Restrictions: restricts certain stations from calling certain trunk groups via dial access codes.
- APLT Off-Net: allows callers to dial public network numbers over the EPSCS private network.
- Terminal-to-Terminal Restriction: restricts the user from placing or receiving any calls except to and from other stations on the switch.
- Outward Restriction: restricts the user from placing calls over the CO, FX, or WATS trunks using dial access codes to trunks. Outward restriction also restricts the user from placing calls via ARS/WCR. Use ARS/WCR with WCR toll restrictions instead.
- Toll Restriction: prevents users from placing toll calls over CO, FX, or WATS trunks using dial access codes to trunks. Use ARS/WCR with WCR toll restrictions instead.

- ARS/WCR Toll Restriction: restricts users from dialing the ARS or WCR Network I toll access code or from completing a toll call over ARS/WCR.
- FRL: establishes the user's access to AAR/ARS/WCR routes.
- CDR Account Code: requires the entry of an account code before an ARS/WCR call is processed or before completing a TAC call to a toll destination.

NOTE:
Account code entries are not validated.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, COS identifies the calling features available to a station, such as auto callback and priority calling. It also provides for the assignment of console permissions; these should be assigned sparingly, and only to terminals that require them. It is especially important that console permissions *not* be assigned to remote access extensions.

For DEFINITY G3V2 and later releases, which includes Communication Manager, MultiVantage™ Software, and DEFINITY ECS, an additional COS option is available:

- Call Forward Off/On-Net: allows a user to call forward outside the switch (Off-Net), or inside and outside the switch to non-toll locations (Off/On-Net).

For DEFINITY G3V4, the **list call-forwarding** command displays all stations with Call Forwarding On/Off Net Call Forwarding and Busy/Don't Answer (BY/DA). This display includes the initiating station and destination address.

For DEFINITY ECS Release 5, a default is in place that should help limit accessibility to the Call Forwarding Off-Net capability. Specifically, the default value for the `Restrict Call Fwd-Off Net` field on the COS screen is **y** for every COS.

Also for DEFINITY ECS Release 5, COS can control the Extended User Administration of Redirected Calls feature. To this purpose, the COS screen contains two fields: `Extended Forwarding All` and `Extended Forwarding B/DA`. The default for both fields is **n**.

Facility restriction level

Facility restriction levels (FRLs) provide up to eight levels of restrictions (0 through 7) for users of AAR/ARS/WCR. FRLs identify where calls can be made and what facilities are used. If the FRL of the originating facility is greater than or equal to the FRL of the route pattern selected, the trunk group is accessible. The lower number FRLs are the most restrictive for stations; FRL 0 can be implemented to provide no outside access.

NOTE:
ARS/WRC route patterns should never be assigned an FRL of 0 (zero).

The FRL is used by AAR/ARS/WCR to determine call access to an outgoing trunk group. Outgoing call routing is determined by a comparison of the FRLs in the AAR/ARS/WCR routing pattern with the FRL associated with the originating endpoint.

Authorization codes provide users with an FRL value high enough to give them the calling privileges they require. Only users who enter a valid authorization code with the appropriate calling privileges can override the lower FRL to gain access to a long distance destination.

NOTE:
FRLs are not used if trunk groups have dial access allowed.

Alternate facility restriction levels

For DEFINITY G2, G3r, and System 85, this tool is used with or without authorization codes to replace originating FRL values (the COS FRL versus the AAR/ARS/WCR pattern preference FRL) with an alternate set of values. This allows FRLs to be set to a lower value outside of normal business hours so more restrictions are placed on after-hours calling.

NOTE:
A button is assigned to the attendant console to activate alternate FRLs.

Toll analysis (G3 only)

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, the Toll Analysis screen allows you to specify the toll calls you want to assign to a restricted call list (that is, disallowed), such as 900 numbers, or to an unrestricted (that is, allowed) call list, such as an out-of-area number to a supplier. Call lists can be specified for CO/FX/WATS, TAC, and ARS calls, but not for tie TAC or AAR calls.

Free call list

For DEFINITY G2 and System 85, you can identify up to ten 3-digit telephone numbers that can be called on otherwise-toll-restricted ports. This list allows toll restricted phones to call emergency numbers, such as 911. This option can only be used with TAC calls, not AAR/ARS calls.

NOTE:
This feature should be used only when CO trunks are obtained using TACs. The preferred arrangement is always to use ARS/WCR.

AAR/ARS analysis

ARS routing allows calls to be routed based on the number dialed and the routing plan in effect. The routing is normally to the lowest-cost facility. Different Time of Day plans can be implemented to allow or prohibit calling at certain times.

NOTE:
Never route public network calls (leading digit = 0 or 1) via AAR analysis; always cross over to ARS. (This happens automatically in G2 and System 85 with ETN.)

Some long-distance area codes may start with the same digits as your local exchanges. Be cautious when blocking access to those long-distance area codes, so that access to required local exchanges is not simultaneously blocked. Since COR/COS-to-COR/COS restrictions do not apply to AAR/ARS trunks, use FRLs to limit the calling area [see "Facility restriction level" on page 5-19 for further information].

ARS dial tone

For all switches, the dial tone after the ARS feature access code is optional and can be eliminated to confuse hackers who listen for it. Conversely, its elimination may also confuse authorized users who are accustomed to the second dial tone.

Station restrictions

If access to trunks via TACs is necessary for certain users to allow direct dial access to specific facilities, use the appropriate restrictions. For DEFINITY G2 and System 85, assign miscellaneous trunk restriction groups (MTRGs) to all trunk groups that allow dial access, then deny access to the MTRGs on the COS. For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, if all trunk groups have their own unique COR, then restrict the station CORs from accessing the trunk group CORs. For those stations and all trunk-originated calls, always use ARS/WCR for outside calling.

Recall signaling (switchhook flash)

Recall signaling allows analog station users to place a call on hold and consult with another party or activate a feature. After consulting with the third party, the user can conference the third party with the original party by another recall signal, or return to the original party by pressing **Recall** twice or by flashing the switchhook twice.

However, hackers have been able to activate recall signaling to gain second dial tone and conference incoming and outgoing paths together. To prevent this, administer switchhook flash to **n** (administered by means of the Add or Change Station screen) for FAX machines and modems.

Attendant-controlled voice terminals

When telephones are located in easily-accessible locations (such as lobbies) that do not provide protection against abuse, you can assign them to an attendant-controlled voice terminal group. Calls from the group can be connected to an attendant who screens the calls. As part of the night shut down procedure, the attendant can activate outgoing call restrictions on the group.

Restrictions — individual and group-controlled (Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY G1, G3, and System 75)

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, individual and group-controlled restrictions allow an attendant or voice terminal user with console permission to activate and deactivate the following restrictions for an individual terminal or a group of voice terminals:

- Outward — The voice terminals cannot be used for placing calls to the public network. Such call attempts receive intercept tone.
- Total — The voice terminals cannot be used for placing or receiving calls. DID calls are routed to the attendant or a recorded announcement. All other calls receive intercept tone. As an exception, the following call types are allowed: calls to a remote access extension, terminating trunk transmission tests, and emergency access to attendant calls.
- Station-to-station — The voice terminal cannot receive or place station-to-station calls. Such call attempts receive intercept tone.
- Termination — The voice terminal cannot receive any calls. Incoming calls are routed to the attendant, are directed via call coverage, or receive intercept treatment.

All voice terminals with the same COR are affected by a group restriction. When a call is placed, both the individual and group restrictions are checked.

To activate the desired controlled restriction, the attendant or voice terminal user with console permission dials the feature access code for either the extension or the group, followed by either 1 for Outward, 2 for Total, 3 for Termination, or 4 for Station-to-Station, and then dials the voice terminal extension number (Attendant Control — Extension) or the COR for a group of voice terminals (Attendant Control — COR).

This feature is especially helpful in businesses such as hotels, where you might want to restrict phones in empty conference rooms or in guest rooms after a client has checked out. You might also want to restrict phones in an entire wing of a building at times.

Central office restrictions

Some Central Offices offer additional services that screen long distance calls, such as 0 + calls and 101xxxx+ calls. Contact your local telephone company for details.

Restricting incoming tie trunks

You can deny access to AAR/ARS/WCR trunks when the caller is on an incoming tie trunk. For all the switches, you can force the caller to enter an authorization code when AAR/ARS/WCR is used.

Use the COR of the incoming tie trunk to restrict calls from accessing the network. Set the calling party restriction to **outward**, set the FRL to **0**, and specify **n** for all other trunk group CORs on the calling permissions screen.

Authorization codes

Authorization codes can be used to protect outgoing trunks if an unauthorized caller gains entry into the Remote Access feature. Authorization codes are also used to override originating FRLs to allow access to restricted AAR/ARS/WCR facilities. They can be recorded on SMDR/CAS to check against abuse. Refer to the description of authorization codes in “Authorization codes” on page 5-8.

The **list** command can be used to display all administered authorization codes.

Trunk-to-trunk transfer

Trunk-to-trunk transfer allows a station to connect an incoming trunk to an outgoing trunk and then drop the connection. When this feature is disabled, it prevents stations from transferring an incoming trunk call to an outgoing trunk. Then if the controlling station drops off the call, the call is torn down.

NOTE:
Hackers use this to convince unsuspecting employees to transfer them to 9# or 900. If trunk-to-trunk transfer is allowed, the station can transfer the incoming trunk call to an outgoing trunk and hang up, leaving the trunks still connected.

System 75, System 85, Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3V1, and G3V2 can either allow or disallow trunk-to-trunk transfer. This is for public network trunks only. DS1 and WATS trunks assigned as tielines are not considered public network trunks.

DEFINITY G3V3 and later releases, including DEFINITY ECS Release 5 and later, offer three options:

- **all** — All trunks are transferred.
- **restricted** — Public network trunks are not transferred.
- **none** — No trunks are transferred.

NOTE:
Starting with DEFINITY ECS Release 5, trunk-to-trunk transfer is automatically restricted via administration. To this end, the `Restriction Override` field in the Class of Restriction screen is set to **none** by default.

To disallow this feature, refer to the procedure provided in "Disallow trunk-to-trunk transfer" on page 5-43.

NOTE:
When conferencing calls, to prevent inadvertent trunk-to-trunk transfers, always conference together two outgoing calls. When the calling station disconnects, it forces the trunks to disconnect as well.

NOTE:
When the trunk-to-trunk transfer feature is disabled, the attendant console can continue to pass dial-tone to an inbound trunk caller by pressing **Start 9 Release.**

Forced entry of account code

To maximize system security, it is recommended that the Forced Entry of Account Code feature be enabled and administered on the system.

NOTE:
For DEFINITY G2, Call Detail Recording (CDR) is required with this option. See "Call detail recording/station message detail recording" on page 5-53 for more information. Depending on the required length, the account code may replace other data in the CDR report.

An entry of an account number (1 to 15 digits) can be required for the originating station COR/COS, toll calls, or WCR network calls. If an account number is not entered when required, the call is denied. Although the account number is not verified, callers must enter the appropriate number of digits set by the system administrator. This adds another level of digit entry that a hacker must crack to gain access to an outside line.

World class routing (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G2.2 and G3)

The World Class Routing (WCR) feature replaces and enhances the AAR/ARS feature. Specific digit strings are assigned to either allow or deny calls. The 900 look-alike numbers can be routed for interception. The 800 numbers for ICX carriers can be blocked. This still allows normal 800 numbers to be dialed. Specific international numbers can also be blocked.

You may also route 0 or 00 calls to a local attendant for handling. In addition, 101xxxx + calls can be restricted. Certain laws and regulations may prevent you from blocking these calls, however. Check with your local or long distance carrier for applicable laws and regulations.

If possible, use WCR to shut down toll routes during out-of-business hours by using Time-of-Day routing.

Digit conversion

Digit conversion allows you to identify numbers, area codes, or countries you do not want called. Whenever the numbers entered correspond to the numbers on the conversion list, the numbers are given a different value, such as 0, and then forwarded to the new destination, such as the attendant console.

- For DEFINITY G1 and G3i, the conversion can be to “blank” (intercept tone), or to a Route Number Index (RNX) private network number, where Private Network Access (PNA) software is required to route the call through AAR.
- For DEFINITY G2 and System 85, the conversion is to an RNX private network number, and AAR software is required.
- For DEFINITY G1, G2, G3i, and System 85, once the call is sent to AAR software, the RNX can be translated as “local,” and the call can be directed to an internal station or to the attendant console.

Station security codes

Station security codes (SSCs) are used with two features: Personal Station Access and Extended User Administration of Redirected Calls. Starting with DEFINITY ECS Release 5, the Security Violations Status report shows the 16 most recent invalid attempts of SSC use. The report is refreshed every 16 seconds, and it shows the date, time, port/extension, FAC, and dialed digits for each invalid attempt. Enter the **monitor security-violations station-security-codes** command at the prompt to access this report.

SSC violations are summarized in the Security Violations Summary report. Enter the **list measurements security-violations summary** command to access this report.

SSC input entry has a pre-administered security capability. For details, refer to the ‘‘Personal station access’’ section in this chapter.

Finally, SSCs should be changed about once every six months.

Personal station access

The Personal Station Access (PSA) feature allows multiple users to work at the same voice terminal location at different times. PSA provides capabilities that are similar to TTI, but for a single station. This feature is available starting with DEFINITY ECS Release 5.

Each PSA user must have a station security code (SSC), which includes as many as eight digits.

The feature has a pre-administered security feature regarding input entry by the user. Once the user enters his or her extension at the appropriate time, a “no response” feedback is provided whether or not the entered extension is valid. For an invalid extension, the system simply waits, without responding, until it reaches a timeout threshold. As such, an unauthorized user does not know that input entry is the cause of the error. The same security feature is in effect whenever the user enters the SSC at the appropriate time.

The dissociate function within PSA allows a user to restrict the features available to a voice terminal. Whenever a terminal is dissociated via PSA, it can be used only to call an attendant, accept a TTI merge request, or accept a PSA associate request.

Security tips

PSA/TTI transactions are recorded in the history log, which can be accessed by entering the **list history** command at the prompt. If there is a concern about unauthorized PSA/TTI usage, refer to the history log for verification. To enable recording PSA/TTI transactions, access the Feature-Related System Parameters screen by entering the **change system-parameters features** command at the prompt. Then ensure that the `Record CTA/PSA/TTI Transactions in History Log` field is set to **y**. (Sometimes this flag is set to **n** if CTA/PSA/TTI entries tend to flood the history log, therefore making it difficult to find other entries.) The default for the field is **y**.

A COS for the user’s extension must be administered to have access to PSA. However, be sure to limit PSA COS assignments to stations that need to access PSA.

Once a PSA station is associated with a terminal, anyone using that terminal has all the privileges and capabilities of that station. Therefore, use of the dissociate facility access code is recommended whenever the terminal is not in use.

If PSA and DCP extenders are used to permit remote DCP access, the security provided may not be adequate. A user connecting via DCP extenders must provide a password. However, once the user is connected, the remote DCP station has the capabilities and permissions of whatever station is associated or merged with the local DCP extender port unless the station has been dissociated or separated. Therefore, PSA users should dissociate before they disconnect from a DCP extender.

PSA security violations are recorded by SVN software, if enabled. Refer to the SVN feature description and to the following two documents for security report information:

- *Hardware Guide for Avaya™ Communication Manager*,
- *Administrator’s Guide for Avaya™ Communication Manager,* 555-233-506

Extended user administration of redirected calls

This feature allows station users to select one of two previously administered call coverage paths assigned to them (for example, a work location coverage path or a remote work location coverage path) from any on-site extension or from a remote location (for example, home). Also provided is the ability to activate, change, or deactivate the Call Forward Add or Call Forward Busy/Don't Answer features from any on-site extension or from a remote location.

For security purposes, each user of this feature is administered a SSC. Users must enter an SSC to use this feature. In addition, the COS and COR for the user's extension must be administered to have access to this feature. Any attempt by an invalid extension or invalid SSC to use the feature is recorded as a security violation.

For remote users, an additional security precaution for feature access is provided via the telecommuting access extension. This extension provides access only to this feature; access to any other system features or functions via this extension is denied.

Access to the extended forwarding capability provided by this feature is controlled by the `Extended Forwarding All` and `Extended Forwarding B/DA` fields in the COS screen. To access the screen, enter the **change cos** command.

Remote user administration of call coverage

NOTE:
This feature requires one SSC for every user or extension. SSCs should be changed about once every six months.

The system allows calls that are forwarded off of the network (that is, off-net) to be tracked for busy or no-answer conditions and to be brought back for further call coverage processing in such cases. However, ensure that the principal has a coverage path; otherwise, the system will not track the call, and the call will be left at the off-net destination regardless of whether it is answered or busy.

If the principal has Send All Calls (SAC) activated, the system will not attempt Call Forwarding Off-Net, except for priority calls. Likewise, except for priority calls, the system will not attempt Call Forwarding Off-Net for coverage paths that specify Cover All.

Invalid attempts to change the coverage path or the call forwarding destination are recorded by the SVN.

To identify unauthorized activation of the Call Forwarding features, use the **list call-forwarding** command. The command output includes stations that have Call Forwarding All Calls and Call Forwarding Busy/Don't Answer active. Also displayed are the number and name of the extensions that have the feature active as well as the "forwarded-to" destination.

Security measures

The following procedures explain how to use security tools to create restrictions that help prevent unauthorized access to your PBX system's facilities.

Require passwords

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, passwords may be up to 7 alphanumeric characters (11 for G3V3 and later). For System 85 and DEFINITY G2, the security code may be up to 6 digits.

Change passwords for system logins frequently according to the guidelines listed below.

- For DEFINITY G1 and System 75, routinely change logins for Network Management Systems (NMS), "cust," "rcust," "browse," and "bcms."
- Disable any unused login. Except for System 75 R1V1, to disable a login, type **VOID** in the `Password` field. (Note that VOID must be typed in uppercase.)

  NOTE:
  "NMS," browse," and "bcms" are not available in System 75 R1V1; "NMS" is not available in System 75 R1V2; "bcms" is not available in System 75.

  NOTE:
  Do not use **VOID** to disable logins in System 75 R1V1; it will not work. In this release, if the password has been set to `VOID`, typing **VOID** when prompted for the password will result in a successful login. It is not possible to disable logins for this release. Instead, you can change all permissions on logins, change the password, select carefully constructed passwords, change passwords frequently, and purchase the Remote Port Security Device (RPSD) hardware for added security.

  NOTE:
  System 75 R1V2 customers should contact the Avaya Technical Service Center for "browse" password administration procedures.

  — For System 75 R1V3N and the DEFINITY G1.1N and G3V2, systems are shipped with the customer logins disabled.

  CAUTION:
  Systems upgraded from earlier versions will have the logins and passwords of its previous version. This applies to "N" loads and Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3.

DEFINITY G3V3 and later systems are shipped without any customer logins. Customer logins must be assigned when installing the system. Also, DEFINITY G3V2 and later releases provide additional restrictions on logins. For each login, you can limit up to 20 (40 for DEFINITY G3V3 and later) objects (for example, stations or trunks) from being administered.

— For systems covered by warranty, lease, or maintenance contract, Avaya will routinely change Avaya-controlled logins.

- DEFINITY G2 and System 85 have one security code. Use **PROC497 WORD3 FIELD5** to change it. Customers must notify Avaya prior to changing the code to ensure ongoing maintenance.

  See Chapter 14 for information on how to change passwords.

Restrict who can use remote access and track its usage

For maximum security, barrier codes and authorization codes must be given only to the people who have a need to use the feature. For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2.2 Release 3.0, G3, and System 75 R1V3, use both codes. For DEFINITY G2 and System 85, use a barrier code to access the feature, and then use authorization codes to screen outbound calls.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75 R1V3:

- Use **change system-parameters feature** to display the Feature-Related System Parameters screen.
  - If the software has been purchased, enter **y** in the `Authorization Code Enabled` field.
  - Enter **7** in the `Authorization Code Length` field.
  - Enter **#** or **1** in the `Authorization Code Cancellation Symbol` field.
  - When providing attendant coverage, enter **y** in the `Timeout to Attendant` field. Invalid entries of authorization codes and failure to enter an authorization code result in a transfer to an attendant.
- Use **change remote-access** to display the Remote Access Status screen.
  - If not already assigned, enter the appropriate extension number in the `Remote Access Extension` field.
  - Enter **7** in the `Barrier Code Length` field.
  - If you are using authorization codes, enter **y** in the `Authorization Code Required` field, and press **Enter**. Enter **n** in the subsequently-displayed `Remote Access Dial Tone` field.

- Enter up to 10 barrier codes (use all seven digits) and assign each a COR and COS that allow only necessary calls. The COR should be restricted so that even if a hacker deciphers the barrier code, a valid authorization code is still needed to make a call.

  NOTE:
  Use the Remote Access feature only on an as-needed basis, and assign a unique COR to each barrier code. Change the barrier codes periodically. See ''Remote access barrier code aging/access limits (DEFINITY G3V3 and Later)'' on page 5-67.

- When assigning authorization codes used only to upgrade FRLs, use an outward-restricted COR with the appropriate FRL. Use **change authorization-code <code>** to display the Authorization Code-COR Mapping screen.

  NOTE:
  Be sure to remove the authorization code whenever an authorized user leaves the company or no longer needs the Remote Access feature.

- Consider using a special partition group for the remote access COR, and then administer the AAR/ARS tables only for those external locations you allow remote access users to call. Use **change cor** to specify either the Time-of-Day routing or partition group. Use **change ars analysis partition** to define the appropriate partition group.
- Monitor authorization code usage with CDR. See ''Call detail recording/station message detail recording'' on page 5-53 for further details.

For DEFINITY G2 and System 85:

- Use **PROC010 WORD1-4** to set COS 31 for remote access.
- Use **PROC285 WORD1 FIELD1** to require a barrier code for remote access.

  NOTE:
  As an alternative, you can require an authorization code. However, since only one code can be used to gain access to remote access, more protection is provided when you require a barrier code to enter remote access and then an authorization code to dial out of the system.

- Use **PROC350 WORD2 FIELD1 = 26** to assign an access code that allows you to change the barrier code using the attendant console.
- When authorization codes are assigned, use **PROC282 WORD1 FIELD2** to administer the lowest FRL you can.

- Use **PROC286 WORD1 FIELD16** to send calls to an intercept tone, a CAS attendant, or a local attendant when the caller does not enter a code.
- Use **PROC289**, Programmable Intercept Treatment, to transfer calls to an attendant when the caller enters an invalid trunk access code, feature access code, or extension.
- Turn on CDR for incoming calls by entering **PROC275 WORD1 FIELD14**. Also turn on CDR for the remote access trunk group using **PROC101 WORD1 FIELD8**. See "Call detail recording/station message detail recording" on page 5-53 for more information on CDR.

Fully restrict service

Fully restricted service is assigned to a COR that prevents assigned stations from having access to either incoming or outgoing public network calls. Stations have access to internal calls only. In addition, fully restricted station users cannot use authorization codes to deactivate this feature.

Any calls from the public network to a station with fully restricted service are redirected to intercept treatment or to the attendant. If the call is redirected to the attendant, the attendant's display indicates the call is being redirected because of fully restricted service. The reason-code displayed is FULL.

When the call is redirected to the attendant, the following may be appropriate actions:

- The attendant connected with a CO may call or intrude on the called station user.
- The attendant cannot extend, conference, or bridge the redirected call.
- The attendant can place a CO call on hold and call the station with fully restricted service for consultation.

Provide individualized calling privileges using FRLs

FRLs are used to allow or deny calls when AAR/ARS/WCR route patterns are accessed. An originating FRL assigned to a station or tie-line trunk group must be equal to or greater than the terminating route pattern FRL for the call to be completed. A COR or COS assigned an FRL of 7 is allowed to complete a call on any route pattern. A COR or COS assigned an FRL of 2 can only access route patterns assigned an FRL of 0, 1, 2, or 3. A low FRL should be assigned to analog stations used for voice mail, remote access barrier codes, VDNs, and tie-lines from other systems. Refer to Table 5-3 for a list of suggested FRL values.

NOTE:
If dial access is allowed for a trunk group, the caller can bypass the FRL restrictions and directly access the trunk group.

NOTE:
FRLs 1 through 7 include the capabilities of the lower FRLs.

Table 5-3. Suggested values for FRLs

FRL	Suggested Value
0	No outgoing (off-switch) calls permitted.
1	Allow local calls only; deny 0+ and 1 800 calls.
2	Allow local calls, 0+, and 1 800 calls.
3	Allow local calls plus calls on FX and WATS trunks.
4	Allow toll calls within the home NPA.
5	Allow calls to certain destinations within the continental USA.
6	Allow calls throughout the continental USA.
7	Allow international calling. Assign Attendant Console FRL 7.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3 and System 75:

- Use **change cor** to display the Class of Restriction screen.
- Enter the FRL number (**0** through **7**) in the FRL field.
- Use **change route-pattern** to display the Route Pattern screen.
- Assign the appropriate FRL to the route pattern defined by ARS/WCR.

For DEFINITY G2 and System 85:

- Use **PROC010 WORD3 FIELD23** to assign FRLs to a station originator's COS for use with AAR/ARS/WCR trunks. (COS 31 is used for Remote Access.)
- Use **PROC103 WORD1 FIELD2** to assign FRLs to an incoming trunk.
- Use **PROC309 WORD1 FIELD3** to assign FRLs to an ARS route pattern.
- Use **PROC321 WORD1 FIELD4** to assign FRLs to an AAR pattern.
- On DEFINITY G2.2, use **PROC318 WORD1 FIELD4** to assign FRLs on WCR.

Prevent after-hours calling using time of day routing or alternate FRLs

You can regulate the days of the week and specific times that outgoing calls can be made. Depending on the time of day and day of the week, calls can be blocked or routed to the least-costly facility available. Since late evenings and weekends are particularly vulnerable times for toll hacking, set up separate plans with the most restrictive plan reserved for evenings and weekends. If you do not want toll calls made after hours, block them during those times. You can also use call vectoring to route to different trunk groups; for example, after hours you may want only 50 trunks available instead of 200.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1 and G3:

- Use **change ars analysis partition x** to define an ARS analysis table to be used for after-hours calling.
- Use **change time-of-day y** to select and define a time of day plan.
- Administer the times you want to offer remote access and the times you do not.
- Use **change cor xx** to assign the time of day plan to the COR for barrier codes or authorization codes.

For DEFINITY G3r:

- Use **change attendant <attendant_number>** to display the Attendant Console screen.
- In an available `Feature Button Assignments` field, enter **alt-frl** to administer an alternate FRL button on the attendant console. This button is used to activate lower FRLs after business hours so the calling area is limited.
- Use **change alternate-frl** to assign the alternate FRL that will replace each original FRL when the attendant activates the feature.

For DEFINITY G2 and System 85:

- There are three Time of Day plans (seven for G2.2). Use **PROC316 WORD1** to set day, hour and minute, and plan number.
- When using WCR, enter **PROC311** to separate toll and non-toll numbers into different routing indices. Use **PROC314** for tenant services to separate toll and non-toll numbers into different routing indices.
- Use **PROC311**, **PROC316**, and **PROC317** to shut down toll routes outside of business hours.
- Use **PROC286 WORD1 FIELD5-12** to lower FRLs after hours to make them more restrictive.

- Enter **PROC203 WORD1 Button Type 19** to set the **alternate FRL** button on the attendant console. This allows attendants to manually change to alternate FRLs.

Block international calling

If your company does not do business overseas, deny everyone the ability to directly dial international calls; in other words, block calling the international dial prefix, for example, 011. However, this will impact your company's ability to reach the "Telco" operator since 0+ dialing is blocked. This can affect credit card calls, collect calls, third party calls, and special use (0700+) numbers.

For DEFINITY G1 and System 75:

- Enter **change ars fnpa 000** to display the ARS FNPA Table screen.

ARS Routing Table

Operator	0
Toll operator	00
International operator	010
International direct dial	011
Toll operator direct dial	
International operator assistance	012
Operator assistance	001

- Leave the following FNPA fields for international calling **blank**, or, for older versions of software, assign them to an unused route pattern (for example, 254) with no trunk assignments.

Digits Dialed	FNPA Translator Table
011	11
010	10
10xxx011	111
001	4
010n	12
101xxxx010	110
101xxxx01	112

NOTE:
As a reminder, not all international calls follow this pattern. For example, Canada uses standard area codes.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3:

- Enter **change ars analysis** partition to display the ARS Analysis screen.
- Make the route pattern **DEN** to deny for the following numbers:
  - 01 = international operator
  - 010 = international calls, operator-assisted
  - 011 = international calls, direct
  - 101xxxx01 = international operator
  - 101xxxx011 = international calls, direct

For DEFINITY G2 and System 85:

- For DEFINITY G2.1 and System 85, block international calls by not assigning a routing designator in **PROC311 WORD1** for office code “1” or assign “01” to Pattern 1.
- For DEFINITY G2.2, use digit conversion to reroute international calls to an attendant or do not administer international calling prefixes. Use **PROC314 WORD1** to route 010 and 011 (7 to 16 digits) to VNI 0.
- For System 85 R2V4n and DEFINITY G2.12.0, route both 01 and 011 to pattern 1 in **PROC311 WORD1**.

Limit international calling

If your company does business overseas with certain countries, you can allow calls to those countries while blocking calls to other countries.

For DEFINITY G1 and System 75:

For 000, 011, and each country code to be blocked:

- Enter **change ars fnpa nnn** (where *nnn* is either **000**, **011**, or the country code to be blocked) to display the ARS FNPA Table screen.
- For each country where calls are allowed, enter the appropriate routing pattern (**r1** through **r32**).
- Enter **change rhnpa** to screen on the next three digits.
- Disable DAC/FAC dialing (see “Disable direct access to trunks” on page 5-39).

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3:

- Enter **change ars analysis** to display the ARS Analysis screen.
- Specify the telephone numbers in the `Dial String` field that you do not want dialed by entering **blank** in the routing pattern or routing to a pattern that contains a high FRL.
- Disable TAC/DAC dialing (see "Disable direct access to trunks" on page 5-39).
- To block calls to countries in the North American dial plan, enter the area code plus any required prefix digit (**0** and **1**). Be sure to define possible variations of the number. For example, to block calls to the 809 area code, enter **1809** and **0809** with **11** in both the `Min` and `Max` fields. If you do not include a prefix digit, enter **10** in both the `Min` and `Max` fields.

For DEFINITY G2 and System 85:

- For DEFINITY G2.1 and System 85 R2V4, assign numbers to the Unauthorized Call Control feature using **PROC313 WORD1**. The FRL for unauthorized call control is assigned in **PROC275 WORD3 FIELD10**. It should be assigned FRL 7.
- For DEFINITY G2.2, use digit conversion to reroute abused telephone numbers to an attendant or to VNI 0. Enter **PROC314 WORD1**.

NOTE:
Make sure remote access barrier codes have properly assigned CORs with FRLs set low to restrict access to the network, and use COR-to-COR restrictions to prevent access to trunk groups.

Select authorization code time-out to attendant

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, you can send calls to an attendant if the caller fails to enter a required authorization code within 10 seconds. For DEFINITY G2 and System 85, you can route calls to an attendant when callers fail to enter a required telephone number or authorization code within 10 seconds.

For all switches:

- Select the Timeout to Attendant feature when you administer authorization codes.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use the System-Parameters screen to request authorization code timeout.

Restrict calls to specified area codes

If your business does not make calls to certain area codes, you can prevent users from entering numbers within those area codes.

For DEFINITY G1 and System 75: See "Allow calling to specified numbers" on page 5-37.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3:

- Enter **change ars analysis** to display the ARS Analysis screen.
- Specify the telephone numbers in the `Dial String` field that you do not want dialed. Either leave the field blank, enter **den** (for **deny**) in the routing pattern, or use a pattern that contains a high FRL.
- Disable TAC dialing (see "Disable direct access to trunks" on page 5-39).

For DEFINITY G2.1 and System 85:

- Enter **PROC311 WORD1** to send calls for specific area codes to route pattern 1.

For DEFINITY G2.2:

- Enter **PROC314** to route calls for specific area codes to VNI 0.

Allow calling to specified numbers

A reverse strategy to preventing calls is to allow outbound calls only to certain numbers. For DEFINITY G1 and System 75, you must specify both the area code and the office code of the allowable numbers. For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, you can specify the area codes or telephone numbers of calls you allow.

For DEFINITY G1 and System 75:

- Enter **change ars fnpa xxx**, where xxx is the area code, to display the ARS FNPA Tables screen.
- Assign RHNPA table r1-r32 to the area code. For example, enter **change ars fnpa r1:**, where r1 is NXX.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3:

- Enter **change ars analysis** to display the ARS Analysis screen.
- Enter the area codes or telephone numbers you want to allow and assign an available routing pattern to each of them. Remote HNPAs can also be used.

For DEFINITY G2.2:

- Use WCR with **PROC314 WORD1** and **WORD2** and permit only certain numbers. Consider using Network 3, which contains only those numbers, to reduce the administrative clutter in your outgoing calling network.

Use attendant control of remote access calls (DEFINITY G2 and System 85 only)

Instead of allowing remote access callers to dial numbers directly, an attendant can handle the calls. This “shared” option disables the Remote Access feature during business hours when an attendant is available to handle the calls.

For DEFINITY G2 and System 85:

- Enter **PROC275 WORD2 FIELD10** to specify that the remote access trunks are shared. In this case, Remote Access is available only when the switch is in Unattended Console Service (night mode).
- Assign remote access time-out to the attendant using **PROC286 WORD1 FIELD16.**

Use attendant control of specific extensions

Phones that are in easily-accessible areas (such as lobbies) can be placed in an attendant-controlled group. The attendant can change the restrictions on these phones from the console.

For System 75, Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, and DEFINITY G3:

- Enter **change feature-access-codes** to display the FAC screen.
- In the `User-Control Restrict Activation/Deactivation` fields, enter a valid FAC.
- Enter **change system-parameters feature** to display the Feature-Related System Parameters screen.
- Specify the type of intercept treatment (**announcement, attendant, extension**, or **tone**) the controlled stations will receive.
- Enter **change COS** to display the Class of Service screen.
- Enter **y** in the `Console Permissions` field.
- Enter **change station** or **change attendant** to assign the COS to the station handling the controlled restrictions.

For DEFINITY G2 and System 85:

- Enter **PROC000 WORDD2 FIELD5** to assign an extension to a group that can be placed under attendant control.
- Have the attendant activate restrictions on these phones as part of the business day closing procedure.

Disable direct access to trunks

All outside calling should be done through AAR/ARS/WCR and never with direct trunk access via DACs. To disable the ability to use DACs for outgoing calls system-wide, use the following procedures.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

For each trunk group in the system:

- Enter **change trunk group n** (where *n* is the trunk group number) to display the Trunk Group screen.
- Enter **n** in the `Dial Access` field.

For DEFINITY G2 and System 85 R2V2:

- Enter **PROC100 WORD1 FIELD7** to deny DAC access to all trunks.

For System 85 R2V3:

- Enter **PROC100 WORD1** to deny DAC access to all trunks.

To allow individual stations to use DACs, but deny DAC access to others, use the following procedure.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, DEFINITY G3, and System 75:

- Place the trunk group in a separate COR.
- Use COR-to-COR restrictions to deny stations with specified CORs from directly accessing the trunk group.

For DEFINITY G2 and System 85:

- Use **PROC102 WORD1** to assign trunk groups with dial access allowed to a MTRG.
- Use **PROC010 WORD3 FIELD2-10** to deny access to the MTRG.
- If DACs are required by switch users, use **PROC275 WORD1 FIELD15** to disable tandem tie trunk calls.

Use attendant control of trunk group access

If direct access to trunk groups must be allowed, consider making them attendant-controlled trunk groups. The attendant can then screen the calls.

Up to 12 trunk groups can be controlled.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, DEFINITY G3, and System 75:

- Enter **change attendant** to display the Attendant screen. In the `Feature Button Assignment` field, enter **act-tr-grp** and **deact-tr-grp** to activate and deactivate attendant control of a trunk group.
- Enter the corresponding trunk access code in the `Direct Trunk Group Select Button Assignment` field.
- Press the *act-tr-grp* button to activate attendant control of the trunk group.

  NOTE:
  This affects all users, not just remote access users. If calls are dialed via AAR/ARS/WCR, these trunks will be skipped in the routing pattern.

For DEFINITY G2 and System 85:

- Enter **PROC350 WORD2 FIELD1 = 20** to assign a FAC (System 85) or a Dial Access Code (DAC) (G2) that activates the attendant control feature.
- On the attendant console, press the deactivate button to deactivate the code.
- Each controlled trunk group requires a console key with trunk status indicators.

  NOTE:
  ARS/WCR skips over a trunk group under attendant control. Only when no other route is available will ARS/WCR select an attendant-controlled trunk group.

Disable facility test calls

The Facility Test Call feature provides the ability to make test calls to four types of facilities to ensure the facility is operating properly. The following types of calls are available to both local voice terminal users and Initialization and Administration System (INADS) terminal users:

- Trunk test call — Accesses specific tie or CO trunks, but not DID trunks.
- Touch-tone receiver test call — Accesses and tests the four touch-tone receivers located on a Tone Detector circuit pack or the eight receivers if a TN744 Call Classifier circuit pack is used.

- Time slot test call — Connects the voice terminal user to a specific time slot located on the Time Division Multiplex buses or out-of-service time slots.
- System tone test call — Connects the voice terminal user to specific system tones.

To activate the feature, the Facility Test Calls access code must be assigned. It is recommended that the access code be left **blank** except when actually testing trunks. (Do not use the default of 197.) The COR of the station user needs to have the Facility Access Trunk Test activated on the COR screen.

When properly administered by the customer, the feature enables users to minimize the ability of unauthorized persons to gain access to the network. However, it is the customer's responsibility to take the appropriate steps to properly implement the features, evaluate and administer the various restriction levels, and protect access codes.

CAUTION:

In rare instances, unauthorized individuals may connect to the telecommunications network through the use of test call features. In such cases, applicable tariffs require that the customer pay all network charges for traffic.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, when the user's COR allows it, test calls can be made to access specific trunks. Do not administer this feature unless you need it, and remove it after the test is completed. To remove the Facility Test Calls Access Code, use the following procedures.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Enter **change feature-access-codes** to display the FAC screen.
- Leave the Facility Test Calls Access Code field **blank**.

For DEFINITY G2 and System 85, calls over a dial-repeating tie line or designated maintenance extension can make trunk verification calls. Use the following procedure to disable this feature system-wide.

For DEFINITY G2 and System 85:

- Use **PROC350 WORD2 FIELD1 = 44** to disable the Trunk Verification Feature Dial Access Code.
- Use **PROC103 WORD1 FIELD7** to disallow bridge-on for the trunk group.

To allow stations with a specified COR to perform the test, but deny the ability to others, use the procedure below:

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change cor** to display the Class of Restriction screen.
- Enter **y** in the `Facility Access Trunk Test` field.
- Use **change station** to assign the COR with the FAC test permission to the appropriate station.
- Assign all other stations to a COR with the `Facility Access Trunk Test` field set to **n**.
- Never use the default code of 197.
- To monitor its use, assign a trunk access alarm button to a voice terminal.

To help secure the Facility Test Call feature from unauthorized use, follow these steps:

- Remove the access code when not in use.
- Never use the default code.
- Change the code frequently.
- Protect records of the code.
- Use CORs to restrict which users can use the access code.
- Always administer a trunk access alarm button to alert you visually when the feature is enabled. Assign a **trk-ac-alm** button on the Change Station screen.

DEFINITY G3V4 allows the sign off feature to alert the administrator that the code is administered.

Suppress remote access dial tone

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, when an authorization code is required, you can eliminate the remote access dial tone that callers hear after they enter the required barrier code. After the barrier code is entered, callers will not be given a prompt for the authorization code.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change remote-access** to display the Remote Access screen.
- To suppress the remote access dial tone, enter **n** in the `Remote Access Dial Tone` field.

For DEFINITY G2.2 and System 85:

- You cannot eliminate the dial tone prompt for entry of the authorization or barrier code, nor can you eliminate switch dial tone. You *can* eliminate AAR/ARS dial tone.

For DEFINITY G2.2:

- Use **PROC103 WORD1 FIELD15** to suppress WCR dial tone for that trunk group.
- Use **PROC312 WORD1 FIELD2** to suppress a specific network's dial tone for all users.

For DEFINITY G2.1 and System 85:

- Use **PROC103 WORD1 FIELD3=2** to set the `Network Trunk` field to a value of 2 to suppress AAR/AAS dial tone for that trunk group.
- Use **PROC285 WORD1 FIELD12** to suppress AAR dial tone for all users.

Disallow trunk-to-trunk transfer

Trunk-to-trunk transfer is a feature that allows an incoming trunk call to be transferred to an outgoing trunk call. If set to **yes**, the station can hang up and leave the two trunks still connected. If set to **no**, then the trunks are disconnected as soon as the station hangs up.

For DEFINITY G1, G3V1, G3V2, and System 75:

- Use **change system-parameters feature** to display the Features-Related System Parameters screen.
- Enter **n** in the `Trunk-to-Trunk Transfer` field.

For DEFINITY G2 and System 85:

- Set **PROC275 WORD4 FIELD3** to `0` to disable trunk-to-trunk transfer.

For DEFINITY G3V3 and later releases:

- Use **change system-parameters** to display the Features-Related System Parameters screen.
- Enter the following in the `Trunk-to-Trunk Transfer` field, as appropriate:
  - Enter **a** (all) to allow all trunk-to-trunk transfers.
  - Enter **r** to restrict all public trunks (CO, WATS, FX, DID, and CPE).
  - Enter **n** (none) to restrict all trunks from being transferred except DCS and CAS.

NOTE:
Even if trunk-to-trunk transfer is disallowed, the START 9 RELEASE sequence will supply a dial-tone to the caller, enabling trunk-to-trunk transfer to proceed.

Disable transfer outgoing trunk to outgoing trunk

The outgoing trunk to outgoing trunk transfer (OTTOTT) (G3r and G3V2 and later) feature allows a controlling party, such as a station user or attendant, to initiate two or more outgoing trunk calls and then transfer the trunks together. The transfer removes the controlling party from the connection and conferences the outgoing trunks. Alternatively, the controlling party can establish a conference call with the outgoing trunks and then drop out of the conference, leaving only the outgoing trunks on the conference connection.

Since OTTOTT allows calls to be established in which the only parties involved are external to the switch and are on outgoing trunks, it is a perilous enhancement of trunk-to-trunk transfer. To mitigate problems associated with its accidental use, this feature is only administrable on trunk groups on the Trunk Group screen and is enabled using the `Disconnect Supervision Out` field. This feature is not a system-wide option.

Also, OTTOTT is not intended for use in Distributed Communication System (DCS) networks, since DCS Trunk Turnaround provides comparable capabilities in a much safer way. However, use of OTTOTT with DCS is not prohibited, and may be helpful when one or more of the trunks go off the DCS network.

CAUTION:
This feature can be used to transfer an outside party to a trunk over which toll calls might be made.

To minimize the risk of toll fraud with this feature, follow these steps:

- Since trunks have to be specifically administered for OTTOTT, examine the COR and FRL of the trunk group to determine if they are appropriate.
- If the feature is not relevant to your business, do not enable it. If a temporary need for the feature arises, enable it and then turn it off.

Disallow outgoing calls from tie trunks

If your tie trunks are used solely for office-to-office calling, you can deny access from tie trunks to outgoing AAR/ARS/WCR trunks. This does not affect calls using TACs. For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change cor** to create a new Class of Restriction for the incoming tie line trunk group.
- Assign the lowest possible FRL that provides private network calls to tandem tie trunks.
- Assign COR-to-COR restrictions that give incoming tie lines no direct access calling permissions to CORs of trunk groups that are not dial-access restricted.
- Use **change trunk-group** to assign the COR to the tie line trunk group.

For G2 and System 85:

- Use **PROC103 WORD1 FIELD5=0** to deny access to AAR/ARS/WCR trunks from tie trunks [other than Electronic Tandem Network (ETN) trunks]. However, the calls coming in on an access tie line will not be able to access AAR to dial other network numbers, including extensions that terminate in this PBX. A recommended alternative is to assign a low FRL on the access tie line group in **PROC103 WORD1 FIELD2**.

Limit access to tie trunks

If you need to make AAR/ARS/WCR calls using tie trunks, you can limit access to the trunks using the following procedures.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change cor** to display the Class of Restriction screen.
- Assign a higher FRL to provide the calling range required.
- Use **change station** or **change trunk-group** to assign the COR to the originating stations or trunks.
- Assign COR-to-COR restrictions that give no calling permissions to other trunk group CORs.

For DEFINITY G2 and System 85:

- When DACs are available to users, enter **PROC110** to provide Trunk-to-Trunk restrictions.
- Force the entry of an authorization code with **PROC103 WORD1 FIELD6**.

  NOTE:
  The caller is not prompted for an authorization code on incoming tie trunk calls with a TCM.

- Set the default FRL to a low value with **PROC103 WORD1 FIELD2**.

  NOTE:
  ETN trunks pass along the originating station's FRL as a TCM. Other station permissions are not passed along.

Monitor trunks

The **monitor** command displays internal software state information for diagnosis.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, the **monitor** command can be used by the **cust**, **rcust**, **bcms** and **browse** customer logins. For G3V3 and later, the **monitor** command can be used by any super user or non-super user with permission to display administration and maintenance data.

The **monitor** command also helps locate facilities to which the trunk is communicating, and thus allows you to track hacking activity as it occurs. The **monitor** command provides 30 second updates on trunk activity.

Use terminal translation initialization

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, the Terminal Translation Initialization (TTI) feature allows a user to associate a terminal-administered-without-hardware translation to a valid port address by dialing a special digit sequence (feature access code, 1-to-7-digit TTI security code, and extension) from a terminal connected to the port. It also allows a user to disassociate a terminal from its port location by dialing a similar "disassociate" digit sequence.

The feature also includes the administration necessary to change unadministered ports in the switch to TTI ports (ports from which the TTI association sequence can occur).

CAUTION:
This feature may be subject to unauthorized use. Because a person could disassociate voice or data terminals, he or she might also be able to associate with another extension and obtain the other extension's permissions to dial out.

Require account codes

You can use the Forced Entry of Account Code (FEAC) feature to require callers to enter an account code (up to 15 digits) before calls to toll numbers are completed. This option can be specified for an originating station COS (G2 only), for an outgoing trunk group, or for access to ARS/WCR trunks. If an account code is not dialed when required, the call is denied. Although there is no verification of the digits, the digits entered must match the specified length (1 to 15 digits).

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75 R1V3:

- Use **change system-parameters feature** to display the Features-Related System Parameters screen.
- Enter **15** in the `SMDR/CDR Account Code Length` field.
- To activate the measure system-wide, enter **y** in the `Force Entry of Account Codes` field.
- To activate the feature on an individual basis, use **change cor** to display the Class of Restriction screen.
- Enter **y** in the `Force Entry of Account Code` field.
- Use **change station** to assign the COR to the appropriate stations.

  NOTE:
  Station Message Detail Recording (SMDR) and account codes are only required for toll calls.

- For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, use **change toll** to display the Toll Analysis screen.
- Enter dialed strings that require FEAC, and enter **x** in the `Toll` and `SMDR/CDR FEAC` fields. For G3, any dialed string, including 7-digit local numbers, can be identified as “toll.”

For DEFINITY G2 and System 85:

- Use **PROC010 WORD2 FIELD5** to force account code entry for an originating station.
- Use **PROC101 WORD1 FIELD8** to force account code entry for an outgoing trunk group.
- Use **PROC312 WORD1 FIELD3** to force account code entry for access to WCR (G2.2).
- Use **PROC275 WORD1 FIELD12** to force account code entry for access to ARS (G2.1 and System 85).
- Use **PROC275 WORD1 FIELD13** to set the length of account codes (**1** to **15**).

Assign COR restrictions to adjuncts when using expert agents

In an Expert Agent (EAS) environment, an auto-available split assigned to any adjunct equipment (for example, ICD, CONVERSANT Voice Information System, Voice Mail, or VRU) should have the COR restrictions assigned to the agent login ID. Both the login ID and the extension CORs should have the needed restrictions, but the COR of the login ID takes precedence.

Disable distinctive audible alert

The Distinctive Audible Alert feature on a 2500 set has the potential of returning stutter dial tone when used in conjunction with VRUs — modems, FAX machines, voice mail ports, and CONVERSANT Voice Information System ports. The stutter dial tone, in turn, converts to steady dial tone and allows a call to be made.

Analog ports assigned to adjunct equipment should have the Distinctive Audible Alert feature (a field on the 2500 screen) set to **no** (the default is **yes**).

For System 75, Communication Manager, MultiVantage™ Software, DEFINITY ECS, and DEFINITY G1, and G3, use **change station** to display the Station screen. Enter **n** in the `Distinctive Audible Alert` field.

Remove data origination code

The Data Origination feature is used in conjunction with modem pooling. It allows users to bypass many system restrictions and gives them access to outside facilities. It has the potential to be used by hackers to compromise a system.

The default data origination default code is 134. When a voice mail system is set to **digits** (instead of **subscriber**), the COR restrictions on the voice ports are not valid when the data origination code is used. If a voice mail system is set to **digits** and 134 is dialed from any phone, the switch returns outside dial tone and allows a call to be processed.

It is recommended that the data origination code be removed. If this feature is used, then the code should be changed.

Use world class routing restrictions

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G2.2 and G3, use the following steps to restrict WCR from unauthorized use.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3:

- Miscellaneous restrictions (COR-to-COR restrictions) are not observed during AAR/ARS call processing. The FRL value is used instead.
- Use **change COR** to display the Class of Restriction screen.
- Assign the lowest possible FRL to the barrier code, authorization code, VDN, station, or inbound trunk group. Use **change trunk-group** to assign the COR to all incoming trunks.
- Use tandem tie trunks for routing private network calls.
- Use **change toll** to display the Toll screen. Identify what calls are allowed or disallowed.
- Use **change ars analysis** to display the ARS Toll Analysis screen. Limit long distance and international calls permitted by ARS trunks.
- Use **change route-pattern** to assign the appropriate FRL for public network trunks in the routing pattern.
- Use **change ars analysis** to administer ARS Analysis Tables with at least 3- or 4-digit strings.
- Use **change ars analysis** to distinguish between 7- and 10-digit calls. Use the prefix digit instead of the `Min/Max` fields for long distance calls.
- Use wildcard characters with care.
- Prevent calls by not administering their numbers on the ARS Toll Analysis screen. If the originating endpoint is assigned a toll-restricted COR, this prevents TAC toll calls.

  NOTE:
  Whenever possible, TAC calls should be disallowed. See "Disable direct access to trunks" on page 5-39.

For DEFINITY G2.2:

- Do not turn on overlapped sending (default is **off** in G2.2, **on** in earlier releases). To turn off overlapped sending, enter **PROC103 WORD1 FIELD14.** Overlapped sending bypasses digit checking.
- To force waiting for a TCM, the trunk group must be an intermachine trunk group (**PROC103 WORD1 FIELD3=1 or 2**) and ETN software must be activated. A TCM will not be sent over an access tie trunk group no matter how low the FRL is in **F2**. However, a low FRL may be used to limit the calling from the tie line, or to force a prompt for an authorization code.

- Mark each string and route with an FRL permission value using **PROC314 WORD1 FIELD8**, and **PROC318 WORD1 FIELD4**.
- Use toll checking capabilities as shown:
  - For WCR, use **PROC010 WORD3 FIELD22**.
  - For toll-free tables, use **PROC319** and **PROC318 WORD1 FIELD6**.
- If needed, define more detail in the numbering plan by using **PROC314**. Use wildcard digits and variable string lengths with care.
- Send a # after troublesome call types (0 +, 011 +, etc.). Use **PROC321 WORD1 FIELD16.**

NOTE:
Use **PROC314** to route 0 and 00 calls to an attendant.

Change override restrictions on 3-way COR check

For G3V2 and later releases, the Restriction Override feature is used with the 3-way COR check on transfer and/or conference calls. The default is **none.**

Detecting toll fraud

After you have taken the appropriate security measures, use the monitoring techniques described in this section to routinely review system activity. Here are some signals of possible hacker activity:

- Employees cannot get outside trunks
- Customers have difficulty getting through to your 800 number
- Usage is higher than normal
- Nights and weekends have heavy call volume
- Attendants report frequent “no one there” or “sorry, wrong number” calls
- Bill shows calls were made to strange places

NOTE:
If you should suspect toll fraud in your system, you should call the Avaya Toll Fraud Intervention Hotline, 1-800-643-2353.

Table 5-4 shows the reports and monitoring techniques that track system activity and help detect unauthorized use:

Table 5-4. Reports and monitoring techniques

Monitoring Technique	Switch	Page #
Administration security	All	5-51
Call detail recording (CDR) / station message detail recording (SMDR)	All	5-53
Traffic measurements/performance	All	5-55
Automatic circuit assurance	All	5-56
BCMS measurements	G1 and G3	5-58
CMS measurements	All	5-58
Security Violations Measurement report	All	5-62
Security Violation Notification feature	Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3	5-59
Recent Change History report	Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1 and G3	5-68
Service observing	All	5-69
Malicious call trace	System 85 R2V4, DEFINITY G2, G3r, G3V2 and later	5-68
list call-forwarding command	DEFINITY G3V4 and later	5-70

Administration security

Logins for INADS port

For DEFINITY G3V4 and later, only Avaya logins can access the INADS port. If the customer wants INADS access, Avaya must administer customer login permission.

This permission is administered on a login basis. Avaya is responsible for performing the necessary administration for one customer superuser login. If additional customer logins require access to the system via the INADS port, the customer superuser login may perform the necessary administration to grant those permissions.

Forced password aging and administrable logins

DEFINITY G3V3 and later releases provide two features for enhanced login/password security.

- The first, Forced Password Aging, is a feature that the superuser administering the logins may activate. The password for each login can be aged starting with the date the password was created or changed, and continuing for a specified number of days, from 1 to 99. A user is notified at login, seven days before the password expiration date, that his or her password is about to expire. When the password expires, the user is required to enter a new password into the system to complete the login process. Once a non-superuser has changed his/her password, the user must wait 24 hours to change the password again.

  When a login is added or removed, the Security Measurement reports will not be updated until the next hourly poll, or until a **clear measurements security-violations** command has been entered.

- The second feature, Administrable Logins, allows users to define their own logins/passwords and allows superusers to specify a set of commands for each login. The system will allow up to 11 customer logins, each of which can be customized. Each login must be 3 to 6 alphabetic/numeric characters, or a combination of both. A password must be 4 to 11 characters and contain at least one alphabetic and one numeric symbol. Passwords can also contain any of the following symbols: ! & * ? ; ' ^ ( ) , . : - @ # $ %

NOTE:
The Monitor Security Violation Login tool is used to show the invalid login used and the date, time, and port that was used.

New shipments of the DEFINITY G3V3 and later are shipped from the factory with no customer logins and/or passwords defined. One customer superuser password is administered during installation. The customer must administer additional logins/passwords as needed. The superuser login has full customer permissions and can customize any login he or she creates.

On upgrades to the DEFINITY G3V3 or later, customer logins and passwords are carried forward. Password aging is set to one day, and customers must customize their logins/passwords following upgrades.

Login permissions for a specified login can be set by the superuser to block any object that can affect the health of the switch. Up to 40 administration or maintenance objects (commands) can be blocked for a specified login. When an object (administrative or maintenance command) is entered in the blocked object list on the Command Permissions Categories Restricted Object List screen, the associated administrative or maintenance actions cannot be performed by the specified login.

Commands for the DEFINITY G3V3 or later are grouped into three categories: common, administration, and maintenance. Each category has a group of subcategories, and each subcategory has a list of command objects that the commands act on. A superuser can set a user's permissions to restrict or block access to any command in these categories.

NOTE:
DEFINITY G3V3 and later releases allow for unique logins to be assigned (for example, MARY83, B3V3RLY, etc.). This eliminates the need to use **cust**, **rcust**, **browser**, and **bcms**. The **list login** command shows the assigned logins, and the state of the login (for example, **VOID**, **disabled**, etc.).

For information on administering Forced Password Aging and Administrable Logins for DEFINITY G3V3 and later, see Chapter 14.

Call detail recording/station message detail recording

This feature creates records of calls that should be checked regularly. A series of short holding times may indicate repeated attempts to decode remote access barrier codes or authorization codes. Call records can be generated for Remote Access when CDR/SMDR is activated for the remote access trunk group.

Authorization codes, if required, are recorded by CDR/SMDR; barrier codes are not. When you set the `Suppress CDR for Ineffective Call Attempts` field to **no**, calls that fail because the caller does not have adequate calling privileges print a condition code in the report to reflect the failed attempt. (See the CDR description in the *Administrator's Guide for* Avaya™ Communication Manager.) Review the report for these condition codes, which might indicate hacker activity.

Two optional products, Avaya Cost Allocator and Call Accounting System (CAS) Plus, enhance CDR/SMDR by allowing you to create customized reports. These reports can be used to isolate calls that may be suspicious.

NOTE:
Only the last extension on the call is reported. Unauthorized users who are aware of this procedure originate calls on one extension, then transfer to another extension before terminating the call. Internal toll abusers may transfer unauthorized calls to another extension before they disconnect so that CDR does not track the originating station. If the transfer is to your voice mail system, it could give a false indication that your voice mail system is the source of the toll fraud.

Review CDR/SMDR records for the following symptoms of abuse:

- Short holding times on one trunk group
- Patterns of authorization code usage (same code used simultaneously or high activity)
- Calls to international locations not normal for your business
- Calls to suspicious destinations
- High numbers of “ineffective call attempts” indicating attempts at entering invalid barrier codes or authorization codes
- Numerous calls to the same number
- Undefined account codes

For System 75, DEFINITY G1, and DEFINITY G3 and later:

- To display the Features-Related System Parameters screen, use the **change system-parameters** feature (G1 and System 75 only) or the **change-system parameters cdr** feature (G3 and later).
- Administer the appropriate format to collect the most information. The format depends on the capabilities of your CDR analyzing/recording device.
- Use **change trunk-group** to display the Trunk Group screen.
- Enter **y** in the `SMDR/CDR Reports` field.

For DEFINITY G2:

- Use **PROC275 WORD1 FIELD14** to turn on CDR for incoming calls.
- Use **PROC101 WORD1 FIELD8** to specify the trunk groups. Account code entry can be required for CDR (see “Require account codes” on page 5-47 for details).

Traffic measurements and performance

By tracking traffic measurements on the trunk groups, you can watch for unexplained increases in call volume, particularly during off-peak hours. Review the traffic measurements for the following symptoms of abuse:

- Unusually high peg counts (number of times accessed) on trunk groups
- A series of short or long holding times that may indicate repeated attempts to enter the system and/or success in doing so
- High volume on WCR patterns used for 0 + and 011 + calls
- Busiest hour for trunk group being inconsistent with business hours
- Drastic changes in switch occupancy profile compared to a typical 24-hour period

Monitor I

For DEFINITY G2 and System 85, the optional Monitor I tracks call volume and alerts you when the number of calls exceeds a predetermined threshold. Monitor I is a UNIX software package that collects measurements data from G2 and System 85 switches, stores the results, and produces various types of analysis reports.

With Monitor I, you can set up thresholds for expected normal traffic flow on each of your trunk groups. The application will alert you when the traffic flow exceeds the expected values. The data collected includes quantity and duration of incoming and outgoing calls, processor utilization, and security violation measurements for remote access and administration port access.

Use the **PROC400** series to turn on this report for the trunk groups.

SAT, Manager I, and G3-MT reporting

Traffic reporting capabilities are built-in and are obtained through the System Access Terminal (SAT), Manager I, and G3-MT terminals. These programs track and record the usage of hardware and software features. The measurements include peg counts (number of times accessed) and call seconds of usage. Traffic measurements are maintained constantly and are available on demand. However, reports are not archived and should therefore be printed to monitor a history of traffic patterns.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75 R1V3 and later:

- To record traffic measurements:
  - Enter **change trunk-group** to display the Trunk Group screen.
  - In the `Measured` field, enter **both** if you have BCMS and CMS, **internal** if you have only BCMS, or **external** if you have only CMS.

- To review the traffic measurements, enter **list measurements** followed by one of the measurement types (**trunk-groups, call-rate, call-summary, outage-trunk**, or **security-violations**) and the timeframe (**yesterday-peak**, **today-peak**, or **last-hour**).
- To review performance, enter **list performance** followed by one of the performance types (**summary** or **trunk-group**) and the timeframe (**yesterday** or **today**).

ARS measurement selection

The ARS Measurement Selection feature can monitor up to 20 routing patterns (25 for Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3) for traffic flow and usage.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Enter **change ars meas-selection** to choose the routing patterns you want to track.
- Enter **list measurements route-pattern** followed by the timeframe (**yesterday**, **today**, or **last-hour**) to review the measurements.

Automatic circuit assurance

This monitoring technique detects a pattern of short holding time calls or a single long holding time call which may indicate hacker activity. Long holding times on trunk-to-trunk calls can be a warning sign. The Automatic Circuit Assurance (ACA) feature allows you to establish time limit thresholds defining what is considered a short holding time and a long holding time. When a violation occurs, a designated station is notified. A display message accompanies the referral call. If the switch is equipped with a speech synthesis board, an audible message accompanies the call.

When a notification occurs, determine if the call is still active. If toll fraud is suspected (for example, **aca-short** or **aca-long** is displayed on the designated phone), use the busy verification feature (see “Busy verification” on page 5-70) to monitor the call in progress.

When hacker activity is present and remote access is enabled, there is usually a burst of short holding times as the hacker attempts to break the barrier code or authorization code protection, or long holding time calls after the hacker is successful. An ACA alarm on a remote access trunk should be considered a potential threat and investigated immediately. If the call is answered by an automated attendant, a hacker may be attempting to gain access to the system facilities using TACs.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Enter **change system-parameters feature** to display the Features-Related System Parameters screen.
- Enter **y** in the `Automatic Circuit Assurance (ACA) Enabled` field.
- Enter **local**, **primary**, or **remote** in the `ACA Referral Calls` field. If **primary** is selected, calls can be received from other switches. **Remote** applies if the PBX being administered is a DCS node, perhaps unattended, that wants ACA referral calls to go to an extension or console at another DCS node.
- Complete the following fields as well: `ACA Referral Destination`, `ACA Short Holding Time Originating Extension`, `ACA Long Holding Time Originating Extension`, and `ACA Remote PBX Identification`.
- To review and verify the entries, enter **list aca-parameters**.
- Enter **change trunk group** to display the Trunk Group screen.
- Enter **y** in the `ACA Assignment` field.
- Establish short and long holding times. The defaults are 10 seconds (short holding time) and one hour (long holding time).
- To review an audit trail of the ACA referral call activity, enter **list measurements aca**.

For DEFINITY G2 and System 85:

- Use **PROC285 WORD1 FIELD5** and **PROC286 WORD1 FIELD1** to enable ACA system-wide.
- Use **P120 W1** to set ACA call limits and number of calls thresholds.
- Choose the appropriate option:
  - To send the alarms and/or reports to an attendant, use **PROC286 WORD1 FIELD3**.

BCMS measurements (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G1 and G3)

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1 and G3, BCMS Measurements report traffic patterns for measured trunk groups.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1 and G3:

- Use **change trunk-group** to display the Trunk Group screen.
- In the `Measured` field, enter **internal** if you have only BCMS or **both** if you have BCMS and CMS.
- Use **change system-parameters feature** to display the Features-Related System Parameters screen.
- Enter **half-hour** in the `BCMS Measurement Interval` field.
- To review the measurements, use **list bcms trunk**.

CMS measurements

This monitoring technique measures traffic patterns and times on calls and compares them to traffic counts and time limit thresholds. An exceptions log is maintained whenever the traffic counts or time limits exceed the preset thresholds.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1 and G3:

- Use **change trunk-group** to display the Trunk Group screen.
- In the `Measured` field, enter **external** if you have only CMS or **both** if you have BCMS and CMS.
- To generate reports, use **cms reports**.

For DEFINITY G2:

- Use **PROC115 WORD1 FIELD5** to specify incoming or two-way measurements by CMS.
- Set up time limits and count thresholds on CMS (Trunk Group Exceptions). Exceptions are reported to designated CMS terminals (User Permissions: Trunk Group Access). CMS keeps a log of exceptions (Real-Time Exception Log, Historical Report: Trunk Group Exceptions).

Security violation notification (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3)

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, the Security Violation Notification feature (SVN) provides the capability to immediately detect a possible breach of the System Management, Remote Access, or Authorization Code features; and to notify a designated destination upon detection. It is intended to detect Generic 3 Management Terminal (G3-MT) or Generic 3 Management Application (G3-MA) login failures through the INADS port, based on customer-administrable thresholds. Once an SVN threshold is reached, (for a system management login, a remote access barrier code, and, for DEFINITY G3V3 and later, an authorization code), the system initiates a referral call to an assigned referral destination.

For systems earlier than DEFINITY G3V3, the referral destination must be an attendant console or station equipped with a display module. For DEFINITY G3V3 and later, the referral destination can be any station, if an announcement has been administered and recorded. Also for G3V3 and later releases, the SVN Referral Call with Announcement option provides a recorded message identifying the type of violation accompanying the SVN referral call, such as login violation, remote access violation, or authorization code violation. Using call forwarding, call coverage, or call vector Time of Day routing, SVN calls with announcements can terminate to any point on or off the switch. The SVN feature also provides an audit trail about each attempt to access the switch using an invalid login, remote access or (G3V3 and later) authorization code.

The SVN time interval selected, in conjunction with the threshold, specifies when a referral call occurs. For example, if the barrier code threshold is set to 10 with a time interval of two minutes, a referral call occurs whenever 10 or more invalid barrier codes are entered within two minutes.

The advantage of the SVN feature is that it notifies the user of the problem as it occurs so that there is an opportunity to interrupt unauthorized calls before charges are incurred, as well as a chance to apprehend the violator during the attempted violation. The **monitor security-violations** command displays the login activity in real-time on either remote access or system management ports.

Information about invalid system management login attempts and remote access attempts (and, for G3V3 or later), invalid authorization code attempts) is collected at two levels:

- On an immediate basis, when an invalid login attempt is made, for systems earlier than DEFINITY G3V3, the SVN feature can send a priority call to either an attendant console or a station equipped with a display module. For DEFINITY G3V3 and later, the SVN feature can send to any station if an announcement has been administered and recorded. When notified, the security administrator can request the Security Violations Status report, which shows details of the last 16 security violations of each type for Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3.

- On a historical basis, the number of security violations of each type is collected and reported in the Security Violations Summary Measurement report. This report shows summary information since the last time the counters were reset. (See "Security Violations Measurement reports" on page 5-62.)

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3:

- Enter **change system-parameters feature** to display the Feature-Related System Parameters screen. (For DEFINITY G3V3 and later, enter **change system-parameters security** to display the System-Parameters Security screen.)
- To monitor remote access, enter **y** in the `SVN Remote Access Violation Notification Enabled?` field.
- To monitor administration ports, on the same screen, enter **y** in the `SVN Login Violation Notification Enabled` field.
- To monitor authorization codes (G3V3 and later), enter **y** in the `SVN Authorization Code Violation Notification Enabled` field.
- Enter any valid unassigned extension number in the `Originating Extension` field(s).
- Enter the extension number of the person who will monitor violations in the `Referral Destination` field(s). For releases before DEFINITY G3V3, this destination must be a station equipped with a display module or an attendant console. In DEFINITY G3V3 and later, if an announcement extension is administered, the referral destination does not require a display module. In G3V3 and later, a violation occurs based on the number of invalid attempts and is not dependent on a forced disconnect.

  NOTE:
  If an announcement extension is administered, but no announcement is recorded, the referral call will not be made.

- For remote access, enter the number of attempts allowed before a violation occurs in the `Barrier Code Threshold` field, and enter the time interval in hours or minutes for tracking the number of attempts.
- For logins, enter the number of login attempts before a violation occurs in the `Login Threshold` field and the time interval in hours or minutes for tracking the number of attempts. To register as a violation, there must be three invalid login attempts (resulting in a forced disconnect) within the assigned time interval.

  NOTE:
  If you set the `Barrier Code Threshold` to **1**, any unsuccessful first attempt by authorized users to enter the barrier code will cause a violation. A suggestion is to set the threshold to allow three attempts within five minutes to allow for mistakes made by authorized users.

- In the `Feature Button Assignment` field, enter **rsvn-call** for the Remote Access Security Violation Notification button and **lsvn-call** for the Login Security Violation Notification button. The feature activation buttons do not have to reside on the referral destination station. They can be administered on any station. However, they must be activated before referral calls are sent to the referral destination.

NOTE:
For DEFINITY G3V3 and later releases, these buttons are called **lsvn-halt** and **rsvn-halt**. A new button, **asvn-halt**, lights the associated status lamp for the assigned station. The buttons operate the opposite way from DEFINITY G1 and G3 pre-V3 buttons; if activated, the calls are not placed.

In addition to those SVN features already discussed (SVN Authorization Code Violation Notification, SVN Referral Call With Announcement, and the new/renamed Referral Call Buttons), DEFINITY G3V3 and later releases offer the following SVN features:

- SVN Remote Access Violation Notification with Remote Access Kill After "n" Attempts

  This feature disables the Remote Access feature following a remote access security violation. Any attempt to use the Remote Access feature once it has been disabled will fail even if a correct barrier code or barrier code/authorization code combination is supplied until the feature is re-enabled.

- SVN Login Violation Notification with Login Kill After "n" Attempts

  This feature "locks" a valid login ID following a login security violation involving that login ID. Any attempt to use a login ID disabled following a login security violation will fail even if the correct login ID/password combination is supplied until the disabled login ID is re-enabled.

DEFINITY G3V4 offers an additional feature:

- The **status remote-access** command provides information on the state of the Remote Access feature. Valid states are **enabled**, **disabled**, **svn-disabled**, or **not-administered**. Valid barrier code states include **active** and **expired**.

For information on administering these parts of the Security Violation Notification feature, see Chapter 5.

Security Violations Measurement reports

This report identifies invalid login attempts and the entry of invalid barrier codes. It monitors the administration, maintenance, and remote access ports. A login violation is reported when a forced disconnect occurs (after three invalid attempts). Review the report daily to track invalid attempts to log in or to enter barrier codes, both of which may indicate hacker activity.

See *Reports for* Avaya™ Communication Manager for complete details on these reports.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1, G3, and System 75:

- Use **list measurements security-violations** to obtain this report, which is updated hourly.

  For DEFINITY G1 and System 75, only counts for invalid login attempts and invalid remote access attempts are provided.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, the report is divided into two sub-reports, a Summary report and a Detail report. The Security Violations Summary report has the following fields:

NOTE:
The report header lists the switch name, date and time the report was requested.

— Counted Since: The time at which the counts on the report were last cleared and started accumulating again, or when the system was initialized.

— Barrier Codes: The total number of times a user entered a valid or invalid remote access barrier code, and the number of resulting security violations. Barrier Codes are used with remote access trunks.

— Station Security Code Origination/Total: The number of calls originating from either stations or trunks that generated valid or invalid station security codes, the total number of such calls, and the number of resulting security violations.

— Authorization Codes: The number of calls that generated valid or invalid authorization codes, the total number of such call, and the number of resulting security violations. Calls are monitored based on the following origination types.

- Station
- Trunk (other than remote access)
- Remote access
- Attendant

- Port Type: The type of port used by the measured login process. If break-ins are occurring at this level, the offender may have access to your system administration. With DEFINITY Release 5r, port types can be:
  - SYSAM-LCL (SYSAM local port)
  - SYSAM-RMT (SYSAM remote port)
  - MAINT
  - SYS-PORT (system ports)
- Total: Measurements totaled for all the above port types.
- Successful Logins: The total number of successful logins into SM (that is, the login ID and the password submitted were valid) for the given port type.
- Invalid Login Attempts: The total number of login attempts where the attempting party submitted an invalid login ID or password while accessing the given port type.
- Invalid Login IDs: The total number of unsuccessful login attempts where the attempting party submitted an invalid login while accessing the given port type.
- Login Forced Disconnects: The total number of login processes that were disconnected automatically by the switch because the threshold for consecutive invalid login attempts had been exceeded for the given port type. The threshold is three attempts.
- Login Security Violations: The total number of login security violations for the given port type. As with barrier code attempts, the user can define the meaning of a security violation by setting two parameters administratively:
  - The number of unsuccessful logins
  - The time interval
- Login Trivial Attempts: The total number of times a user connected to the system and gave no input to the login sequence.

The Security Violations Detail report provides system management login data per login identification. It relates only to system administration. This report has the following fields:

- Login ID: The login identification submitted by the person attempting to login. Login IDs include the valid system login IDs.
- Port Type: The type of port where login attempts were made. DEFINITY Release 5r has the following ports:
  - YSAM-LCL (SYSAM local port)
  - SYSAM-RMT (SYSAM remote port)
  - MAIN
  - SYS-PORT (system ports)
  - MGR1

- INADS (The Initialization and Administration System port)
- EPN (The EPN maintenance EIA port)
- NET

— Successful Logins: The total number of times a login was used successfully to log into the system for the given port type.

— Invalid Passwords: The total number of login attempts where the attempting person submitted an invalid password for the given port type and login ID.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3:

- Use **monitor security-violations** for a real-time report of invalid attempts to log in, either through system administration or through remote access using invalid barrier codes. For G3V3 and later, the **monitor security-violations** command has been split into three separate commands:

  monitor security-violations

  — <login>

  — <remote-access>

  — <authorization-code>

  The four resulting Security Violations Measurement reports provide current status information for invalid Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY Generic 3 Management Applications (G3-MA) login attempts, remote access (barrier code) attempts, and authorization code attempts.

  The report titles are as follows:

  - Login Violations Status report
  - Remote Access (barrier code) Violations Status report
  - Authorization Code Violations Status report
  - Station Security Code Violations report

  NOTE:
  The data displayed by these reports is updated every 30 seconds. Sixteen entries are maintained for each type of violation in the security status reports. The oldest information is overwritten by the new entries at each 30 second update.

The Login Violations Status report has the following fields:

- Date: The day that the invalid attempt occurred
- Time: The time the invalid attempt occurred
- Login: The invalid login that was entered as part of the login violation attempt. An invalid password may cause a security violation. If a valid login causes a security violation by entering an incorrect password, the Security Violation Status report lists the login.
- Port: The port on which the failed login session was attempted

  The following abbreviations are used for DEFINITY G3i:

  - MGR1: The dedicated management terminal connection (the EIA connection to the maintenance board)
  - NET-N: The network controller dialup ports
  - EPN: The EPN maintenance EIA port
  - INADS: The INADS (Initialization and Administration System) port
  - EIA: Other EIA ports

  The following abbreviations are used for DEFINITY G3r:

  - SYSAM-LCL: Local administration to Manager 1
  - SYSAM-RMT: Dial up port on SYSAM board, typically used by services for remote maintenance, and used by the switch to call out with alarm information.
  - SYS-PORT: System ports accessed through TDM bus.
  - MAINT: Ports on expansion port networks maintenance boards, used as a local connection for on-site maintenance.
  - EXT: The extension assigned to the network controller board on which the failed login session was attempted. This is present only if the invalid login attempt occurred when accessing the system via a network controller channel.

The Remote Access Violations Status report has the following fields:

- Date: The day that the invalid attempt occurred
- Time: The time the invalid attempt occurred
- TG No: The trunk group number associated with the trunk where the authorization code attempt terminated
- Mbr: The trunk group member number associated with the trunk where the authorization code attempt terminated
- Ext: The extension used to interface with the Remote Access feature
- Barrier Code: The incorrect barrier code that resulted in the invalid access attempt (G3V3 and later)

In DEFINITY G3V3 and later, the Authorization Code Violations Status report has the following fields:

- Date: The day that the violation occurred
- Time: The time the violation occurred
- Originator: The type of resource originating the call that generated the invalid authorization code access attempt. Originator types include:
  - Station
  - Trunk (other than a trunk assigned to a remote access trunk group)
  - Remote access (when the invalid authorization code is associated with an attempt to invoke the Remote Access feature)
  - Attendant
- Auth Code: The invalid authorization code entered
- TG No: The trunk group number associated with the trunk where the remote access attempt terminated. It appears only when an authorization code is used to access a trunk.
- Mbr: The trunk group member number associated with the trunk where the remote access attempt terminated. It appears only when an authorization code is used to access a trunk.
- Barrier Code: The incorrect barrier code that resulted in the invalid access attempt. It appears only when an authorization code is entered to invoke remote access.
- Ext: The extension associated with the station or attendant originating the call. It appears only when an authorization code is entered from a station or attendant console.

The Station Security Code Violations report has the following fields:

- Date: The date that the attempt occurred
- Time: The time that the attempt occurred
- TG No: The trunk group number associated with the trunk where the attempt originated
- Mbr: The trunk group member number associated with the trunk where the attempt originated
- Port/Ext: The port or extension associated with the station or attendant originating the call.
- FAC: The feature access code dialed that required a station security code.
- Dialed Digits: The digits that the caller dialed when making this invalid attempt. This may help you to judge whether the caller was actually trying to break in to the system, or a legitimate user that made a mistake in the feature code entry.

Remote access barrier code aging/access limits (DEFINITY G3V3 and Later)

For DEFINITY G3V3 and later, Remote Access Barrier Code Aging allows the system administrator to specify both the time interval a barrier code is valid, and/or the number of times a barrier code can be used to access the Remote Access feature.

A barrier code will automatically expire if an expiration date or number of access attempts has exceeded the limits set by the switch administrator. If both a time interval and access limits are administered for an access code, the barrier code expires when one of the conditions is satisfied. If an expiration date is assigned, a warning message will be displayed on the system copyright screen seven days prior to the expiration date, indicating that the barrier code is due to expire. The system administer may modify the expiration date to extend the time interval if needed. Once the administered expiration date is reached or the number of accesses is exceeded, the barrier code no longer provides access to the Remote Access feature, and intercept treatment is applied to the call.

Expiration dates and access limits are assigned on a per barrier code basis. There are 10 possible barrier codes, 4 to 7 digits long. If there are more than 10 users of the Remote Access feature, the codes must be shared.

NOTE:
For upgrades, default expiration dates are automatically assigned to barrier codes (one day from the current date and one access). It is strongly recommended that customers modify these parameters. If they do not, when the barrier codes expire, the Remote Access feature will no longer function.

When a barrier code is no longer needed it should be removed from the system. Barrier codes should be safeguarded by the user and stored in a secure place by the switch administrator. See Chapter 13 for information on administering Barrier Code Aging.

Recent Change History report (Communication Manager, MultiVantage Software, DEFINITY ECS, and DEFINITY G1 and G3)

The latest administration changes are automatically tracked for Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1 and G3. For each administration change that occurs, the system records the date, time, port, login, and type of change that was made.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1 and G3:

- To review the report, enter **list history**. Check for unauthorized changes to security-related features discussed in this handbook.

NOTE:
Since the amount of space available for storing this information is limited, you should print the entire output of the **list history** command immediately upon suspicion of toll fraud.

For DEFINITY G3V4 with the Intel® processor, the history log has doubled in size to 500 entries, and provides login and logoff entries. This log includes the date, time, port, and login ID associated with the login or logoff.

Malicious call trace

For DEFINITY G2, G3r, System 85 R2V4, and DEFINITY G3V2 and later releases, malicious call trace (MCT) provides a way for terminal users to notify a predefined set of users that they may be party to a malicious call. These users may then retrieve certain information related to the call and may track the source of the call. The feature also provides a method of generating an audio recording of the call.

While MCT is especially helpful to those businesses that are prime targets of malicious calls, such as bomb threats, this feature can aid any business in tracing hackers. For this reason, it may be considered as a security tool for businesses that do not normally experience malicious calls.

Depending on whether the call originates within the system or outside it, the following information is collected and displayed:

- If the call originates within the system:
  - — If the call is on the same node or DCS subnetwork, the calling number is displayed on the controlling terminal.
  - — If an ISDN calling number identification is available on the incoming trunk, then the calling number is displayed.

- If the call originates outside the system, the incoming trunk equipment location is displayed. In this case, the customer must call the appropriate connecting switch.
- The following is displayed for all calls: called number, activating number, whether the call is active or not, and identification of any additional parties on the call.

There are several ways to activate the MCT feature. See the *Hardware Guide for* Avaya™ Communication Manager for more information.

Service observing

When toll fraud is suspected, this feature allows an authorized person, such as a security supervisor, to monitor actual calls in progress to establish whether or not an authorized user is on the call. The service observer has the option to listen only or to listen and talk.

An optional warning tone can be administered (on a per-system basis) to let the calling party and the user whose call is being observed know that a supervisor is observing the call. The warning tone is a 440-Hz tone. A two-second burst of this tone is heard before the supervisor is connected to the call. A half-second burst of this tone is heard every 12 seconds while a call is being observed. The warning tone is heard by all parties on the observed call.

NOTE:
The use of service observing may be subject to federal, state, or local laws, rules, or regulations and may be prohibited pursuant to the laws, rules, or regulations or require the consent of one or both of the parties to the conversation. Customers should familiarize themselves with and comply with all applicable laws, rules, and regulations before using this feature.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Enter **change system-parameters features** to display the Features-Related System Parameters screen.
- Enter **y** in the Service Observing Warning Tone field.
- Enter **change station** to display the Station screen.
- Enter **serv-obsrv** in the `Feature Button Assignment` field.
- Use **change cor** to display the Class of Restriction screen.
- Enter **y** in the `Service Observing` field.
- Enter **change station** to assign the COR to the station.

For DEFINITY G2 and System 85:

NOTE:
This feature is available only with an ACD split.

- Use **PROC054 WORD2 FIELD8** to assign the Service Observing Custom Calling Button to a multi-appearance terminal.

For DEFINITY G3V3 and later, the Observe Remotely (remote service observing) feature allows monitoring of physical, logical, or VDN extensions from external locations. If the Remote Access feature is used for remote service observing, then use barrier codes to protect remote service observing.

Busy verification

When toll fraud is suspected, you can interrupt the call on a specified trunk group or extension number and monitor the call in progress. Callers will hear a long tone to indicate the call is being monitored.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Enter **change station** to display the Station screen for the station that will be assigned the Busy Verification button.
- In the `Feature Button Assignment` field, enter **verify**.
- To activate the feature, press the **Verify** button and then enter the trunk access code and member number to be monitored.

For DEFINITY G2 and System 85:

- Administer a Busy Verification button on the attendant console.
- To activate the feature, press the button and enter the trunk access code and the member number.

List call-forwarding command

For DEFINITY G3V4 and later, this command provides the status of stations that have initiated Call Forwarding On Net and Off Net and Call Forwarding Busy/Don't Answer. The display includes the station initiating the Call Forwarding and the call forwarding destination

Small business communications systems

6

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

This chapter provides information on protecting the following communications systems:

- MERLIN II Communications System (page 6-5)
- MERLIN LEGEND Communications System (page 6-7)
- MERLIN Plus Communications System (page 6-59)
- PARTNER II Communications System (page 6-61)
- PARTNER Plus Communications System (page 6-61)
- System 25 (page 6-62)

Other chapters detail additional security measures to protect your equipment:

- Chapter 7 contains security measures to protect the attached voice messaging system. For general security measures, refer to ‘‘Protecting voice messaging systems’’ on page 7-2. For product-specific security measures, refer to:
  - ‘‘MERLIN II Communications System’’ on page 7-35
  - ‘‘MERLIN LEGEND Communications System’’ on page 7-38
  - ‘‘PARTNER II Communications System’’ on page 7-55
  - ‘‘PARTNER Plus Communications System’’ on page 7-57
  - ‘‘System 25’’ on page 7-60
- Chapter 8 contains security measures to protect the Automated Attendant feature of your communications system. For product-specific security measures, refer to:
  - ‘‘MERLIN II Communications System R3’’ on page 8-19
  - ‘‘MERLIN LEGEND Communications System’’ on page 8-20

— ‘‘PARTNER II Communications System’’ on page 8-21

— ‘‘PARTNER Plus Communications System’’ on page 8-22

— ‘‘System 25’’ on page 8-22

Features for the MERLIN systems

The following table identifies MERLIN II and MERLIN LEGEND security features by release number.

Table 6-1. MERLIN II and MERLIN LEGEND security features

Features	MII R3	ML R1.0/ 1.1	ML R2.0/ 2.1	ML R3.0/ 3.1	ML R4.0/ 4.1/ 4.2	ML R5.0	Comments
Automatic route selection (ARS)	x	x	x	x	x	x	
Administration security		x	x	x	x	x	5-character password on SPM program
Allowed list	x	x	x	x	x	x	2- to 11-digit code
Barrier code	x	x	x	x	x	x	MII: one code, four digits ML R1/R2: 16 codes, four digits each, default is 16 codes ML R3/R4/R5: 16 codes, digits increased to 4 through 11, default is 7 digits
Dial access to pools	x	x	x	x	x	x	Factory setting specifies no users are able to use any pool dial-out codes
Direct inward system access (DISA) NOTE: For MERLIN Legend systems, see “Remote Access.”		N/A	N/A	N/A	N/A	N/A	Users limited to dialing inside users or pool/line codes; ARS cannot be used by DISA callers; feature can be set for inward access only or full access

Continued on next page

Table 6-1. MERLIN II and MERLIN LEGEND security features — *Continued*

Features	MII R3	ML R1.0/ 1.1	ML R2.0/ 2.1	ML R3.0/ 3.1	ML R4.0/ 4.1/ 4.2	ML R5.0	Comments
Disallowed list	x	x	x	x	x	x	Default is List 7
Facility restriction levels (FRLs)		x	x	x	x	x	Levels 0 through 6; ARS related
Forced entry of account codes	x	x	x	x	x	x	Affects only outgoing calls
Night service		x	x	x	x	x	Whenever Night Service is on and Shared Remote Access is administered, calls normally routed to internal stations are provided remote access treatment.
Reliable/ unreliable disconnect	x	x	x	x	x	x	“Un-reliable” setting allows the user to dial without system screening if the far end disconnects.
Remote access		x	x	x	x	x	Access controlled by restrictions associated with the barrier codes.
Remote access kill after “n” attempts	x	x	x	x	x	x	N=3
Remote call forwarding		x	x	x	x	x	
Restrict incoming tie lines	*	x	x	x	x	x	MII (*) allows access to stations only on ML; default prohibits access to outgoing facilities via tie lines; access is allowed if the tie line is set for Remote Access, but access is controlled by an assigned barrier code.

Continued on next page

Table 6-1. MERLIN II and MERLIN LEGEND security features — *Continued*

Features	MII R3	ML R1.0/ 1.1	ML R2.0/ 2.1	ML R3.0/ 3.1	ML R4.0/ 4.1/ 4.2	ML R5.0	Comments
Station message detail recording (SMDR)	x	x	x	x	x	x	For ML R3 w/ Call ID, remote access number is recorded if received. For ML R4.2 and later releases, the optional ML Reporter Talk Time feature is disabled.
Station restrictions	x	x	x	x	x	x	Outward, toll, and unrestricted
Transfer to subscriber only		x	x	x	x	x	Related to mail system in use
Trunk-to-trunk transfer		x	x	x	x	x	Cannot be deactivated. For ML R3.1 and later releases, trunk-to-trunk transfer can be blocked for an extension.

MERLIN II Communications System

This section provides information on protecting the MERLIN II Communications System.

Additional security measures are required to protect adjunct equipment.

- Chapter 7 contains security measures to protect the attached voice messaging system. For general security measures, refer to "Protecting voice messaging systems" on page 7-2. For product-specific security measures, refer to "MERLIN II Communications System" on page 7-35.
- Chapter 8 contains security measures to protect the Automated Attendant feature of your communications system. See "MERLIN II Communications System R3" on page 8-19.

Protecting direct inward system access

The Direct Inward System Access (DISA) feature allows users to call into the MERLIN II Communications System from a remote location (for example, a satellite office, or while traveling) and use the system to make calls. However, unauthorized persons might learn the DISA telephone number and password, call into the system, and make long distance calls.

The following security measures assist you in managing the DISA feature to help prevent unauthorized use.

Security tips

- To reduce the system's vulnerability to toll fraud, outward restrict the port to which the remote maintenance device is connected.
- Evaluate the necessity for DISA. If this feature is not vital to your organization, consider not using it or limiting its use.

  To restrict DISA lines, do the following:

  — With a BIS-34D console:

  1. Move the TP switch to **P**.
  2. Press the conference button twice.
  3. Press the message button.
  4. Dial **#325**.
  5. Dial **0** for outward restriction.
  6. Press the message button again.

— With a MERLIN II Communications System display console:

1. From the administration menu, press these buttons: **Lines DISA.**
2. If callers must dial a password to make DISA calls, dial a 4-digit password.
3. Press **Enter**.
4. Press **NoRestr** for no restriction, or **InwdOnly** for inward restriction.
5. Press the line buttons until the lights next to them show the appropriate code:

   Green light on = line or line pool can be used for DISA

   Green light off = line or line pool cannot be used for DISA
6. Press **Conference** to return to the administration menu or leave administration mode.

If you need the feature, use as many of the security measures presented in this section as you can.

- Program DISA to require the caller to enter a system password before the system will allow the caller access. See ‘‘Administration / maintenance access’’ on page 4-4 and ‘‘General security measures’’ on page 4-8 for secure password guidelines.
- Use the system’s toll restriction capabilities to restrict the long distance calling ability of DISA users as much as possible, consistent with the needs of your business.
- Block out-of-hours calling by turning off Remote Access features at an intercom 10 administration telephone whenever possible.
- Protect your DISA telephone number and password. Only give them to people who need them, and impress upon these people the need to keep the telephone number and password secret.
- Monitor your SMDR records and/or your Call Accounting System reports regularly for signs of irregular calls. Review these records and reports for the following symptoms of abuse:
  - — Short holding times on one trunk group
  - — Calls to international locations not normal for your business
  - — Calls to suspicious destinations
  - — High numbers of “ineffective call attempts” indicating attempts at entering invalid barrier codes
  - — Numerous calls to the same number
  - — Undefined account codes

MERLIN LEGEND Communications System

This section provides information on protecting the MERLIN LEGEND Communications System.

Unauthorized persons concentrate their activities in the following two areas with the MERLIN LEGEND Communications System:

- Transfer out of the MERLIN LEGEND Communications System to gain access to an outgoing trunk and make long distance calls.
- Locate unused or unprotected mailboxes and use them as drop-off points for their own messages.

Additional security measures are required to protect adjunct equipment.

- Chapter 7 contains security measures to protect the attached voice messaging system. For general security measures, refer to ''Protecting voice messaging systems'' on page 7-2. For product-specific security measures, refer to ''MERLIN LEGEND Communications System'' on page 7-38.
- Chapter 8 contains security measures to protect the Automated Attendant feature of your communications system. See ''MERLIN LEGEND Communications System'' on page 8-20.

The MERLIN LEGEND Communications System permits trunk-to-trunk transfers from Voice Mail Integrated (VMI) ports starting with Release 2.1. Starting with Release 3.1, the following are in effect:

- VMI ports are assigned outward restrictions by default
- Trunk-to-trunk transfer can be allowed or disallowed on a per-station basis, and the default setting for all stations is restricted. Trunk-to-trunk transfer is the transferring of an outside call to another outside number. Whenever trunk-to-trunk transfer is disabled, users cannot transfer an outside call to an outside line.

  NOTE:
  The ability to transfer internal calls to outside numbers cannot be blocked for an individual extension. However, calling restrictions or disallowed lists can be assigned to individual extensions to prevent outward or toll calls. Also, a call transfer to an outside destination is disconnected if the original call is on a trunk that does not have reliable disconnect, or if another user joined the call, and the call is now a conference call (which cannot be transferred).

- Pool dial-out codes are restricted for all extensions by default. No extension or remote access user with a barrier code has access to pools until the restriction is removed by the system manager.

Unlike the MERLIN II Communications System R3, the MERLIN LEGEND Communications System does not allocate touch-tone receivers for incoming calls, and thus will not interpret touch tones from a caller as an attempt to circumvent toll restriction, and will not disconnect the call. This could leave the MERLIN LEGEND Communications System vulnerable to toll fraud if the ports are not outward restricted.

Preventive measures

- Provide good physical security for the room containing your telecommunications equipment and the room with administrative tools, records, and system programming information. These areas should be locked when not attended.
- Provide a secure trash disposal for all sensitive information, including telephone directories, call accounting records, or anything that may supply information about your communications system. This trash should be shredded.
- Educate employees that hackers may try to trick them into providing them with dial tone or dialing a number for them. All reports of trouble, requests for moving extensions, or any other administrative details associated with the MERLIN LEGEND Communications System should be handled by one person (the system manager) or within a specified department. Anyone claiming to be a telephone company representative should be referred to this person or department.
- No one outside of Avaya needs to use the MERLIN LEGEND Communications System to test facilities (lines/trunks). If a caller identifies himself or herself as an Avaya employee, the system manager should ask for a telephone number where the caller can be reached. The system manager should be able to recognize the number as an Avaya telephone number. *Before connecting the caller to the administrative port of the MERLIN LEGEND Communications system, the system manager should feel comfortable that a good reason to do so exists*. In any event, it is not advisable to give anyone access to network facilities or operators, or to dial a number at the request of the caller.
- Any time a call appears to be suspicious, call the Avaya Fraud Intervention Center at 1 800 628-2888 (fraud intervention for System 25, PARTNER and MERLIN systems).
- Customers should also take advantage of Avaya monitoring services and devices, such as the NetPROTECT℠ family of fraud-detection services, CAS with HackerTracker® and CAT Terminal with Watchdog. Call 1 800 638-7233 to get more information on these Avaya fraud detection services and products.

Protection via star codes and allowed/disallowed lists

Starting with MERLIN LEGEND Release 3.1, star codes can be added to Allowed and Disallowed Lists to help prevent toll fraud. These codes are dialed usually before an outgoing call, and they allow telephone users to obtain special services provided by the central office (CO). For example, in many areas, a telephone user can dial *67 before a telephone number to disable CO-supplied caller identification at the receiving party's telephone.

Whenever a user dials a star code, the system checks the allowed and disallowed lists to determine whether the star code is allowed. If the star code is allowed, the star code is passed to the CO, the calling restrictions are reset, and the digits following the star code are checked by the allowed lists, disallowed lists, and calling restrictions.

The system recognizes star codes containing two digits ranging from either 00 through 19 or 40 through 99 (for example, *14). It also recognizes star codes containing three digits ranging from 200 through 399 (for example, *234).

Therefore, for example, if a caller dials *67280, the system checks *67 against the allowed and disallowed lists. If this code is allowed, the system then checks 280 against the allowed and disallowed lists.

Multiple leading star codes (such as *67*70) are also handled by the system: the dialed number is checked against the allowed and disallowed lists after each star code is detected.

The following table gives examples of how to allow and disallow calls via star codes and disallowed lists.

Table 6-2. Allowing and disallowing calls via star codes and disallowed lists

Objective	Solution
Disallow calls preceded by *67, but allow all other calls.	Enter *67 as a Disallowed List entry.
Disallow calls preceded by all star codes, but allow all other calls.	Enter * as a Disallowed List entry.
Disallow calls preceded by either *67 or *69, but allow all other calls.	Enter *67 as a Disallowed List entry, and enter *69 as a separate Disallowed List entry.
Disallow calls preceded by *67, calls to 900 numbers, and calls to directory assistance (411), but allow all other calls.	Enter *67, 900, and 411 as separate Disallowed List entries.

Default disallowed list

By default, Disallowed List #7 contains the following entries, which are frequently associated with toll fraud:

- 0
- 10
- 11
- 976
- 1809
- 1700
- 1900
- 1*ppp*976 (where each *p* represents any digit)
- *

This list is automatically assigned to any port that is programmed as a VMI port.

The system manager should assign Disallowed List #7 to any extension that does not require access to the numbers in the list.

Assigning a second dial tone timer

A second dial tone timer can be assigned to lines and trunks to help prevent toll fraud.

NOTE:
This timer can be used with star codes, which are discussed earlier in this chapter.

If the timer is assigned, and if the user dials a certain set of digits, the CO provides a second dial tone to prompt the user to enter more digits. This ensures that digits are dialed only when the CO is ready to receive more digits from the caller. Therefore, the risk of toll fraud or of the call being routed incorrectly is reduced.

Setting facility restriction levels

Facility restriction levels (FRLs) can help prevent toll fraud. Some FRLs are already set to a default value before the product is shipped to the customer. Other FRLs can be set by the customer.

Security defaults and tips

The following list identifies features and components that can be restricted by FRLs, identifies the corresponding FRL, and discusses how the FRLs affect these features and components.

- Voice Mail Integrated (VMI) ports

  The default FRL for VMI ports is now 0. This restricts all outcalling. (Refer to Form 7d, “Group Calling.”)

- Default local route table

  The default FRL for the default local route table is now 2. No adjustment to the route FRL is required. (Refer to Table 18 on Planning Form 3g, “ARS Default and Special Numbers Table.”)

- Automatic route selection (ARS)

  The customer receives the product with ARS activated and with all extensions set to FRL 3. This allows all international calling. To prevent toll fraud, set the ARS FRL to the appropriate value in the following list.

  — 0 (restriction to inside calls only)

  — 2 (restriction to local calls only)

  — 3 (restriction to domestic long distance)

  NOTE:
  This restriction does not include area code 809, which is part of the North American Numbering Plan (NANP).

  — 4 (international calling)

  NOTE:
  In Release 3.1 and later systems, default local and default toll tables are factory-assigned an FRL of 2. This simplifies the task of restricting extensions; the FRL for an extension merely needs to be changed from the default of 3.

Protecting the Remote Access feature

The Remote Access feature allows users to call into the MERLIN LEGEND Communications System from a remote location (for example, a satellite office, or while traveling) and use the system to make calls. However, unauthorized persons might learn the remote access telephone number and password, call into the system, and make long distance calls.

For MERLIN LEGEND R3.1 and later systems, system passwords, called barrier codes, are by default restricted from making outside calls. In MERLIN LEGEND releases prior to Release 3.0, if you do not program specific outward calling restrictions, the user is able to place any call normally dialed from a telephone associated with the system. Such an off-premises network call is originated at, and will be billed from, the system location.

The MERLIN LEGEND Communications System has 16 barrier codes for use with remote access. For systems prior to MERLIN LEGEND R3, barrier codes have a 5-digit maximum; for R3 systems and later, barrier codes have an 11-digit maximum. For greater security, always use the maximum available digits when assigning barrier codes.

Beginning with MERLIN LEGEND R3.0, the following rules on barrier codes have been included in order to prevent telephone toll fraud:

- The remote access default requires a barrier code
- The barrier code is a flexible-length code ranging from 4 to 11 digits (with a default of 7) and includes the * character. The length is set system-wide.
- The user is given three attempts to enter the correct barrier code

The following security measures assist you in managing the Remote Access feature to help prevent unauthorized use.

Security tips

- Evaluate the necessity for remote access. If this feature is not vital to your organization, consider not using it or limiting its use.
- To turn off the Remote Access feature:
  1. On the System Administration screen, select `Lines and Trunks` and then select `Remote Access`.
  2. Choose `Disable Remote Access`.

  If you need the feature, use as many of the security measures presented in this section as you can.

- Program the Remote Access feature to require the caller to enter a barrier code before the system will allow the caller access. Up to 16 different barrier codes can be programmed, and different restriction levels can be set for each barrier code.
- For MERLIN LEGEND R3.0, program the Remote Access feature to enter an authorization code of up to 11 digits. For greater security, always use the maximum available digits when assigning authorization codes.
- It is strongly recommended that customers invest in security adjuncts, which typically use one-time passcode algorithms. These security adjuncts discourage hackers. Since a secure use of the Remote Access feature generally offers savings over credit card calling, the break-even period can make the investment in security adjuncts worthwhile.
- If a customer chooses to use the Remote Access feature without a security adjunct, multiple barrier codes should be employed, with one per user if the system permits. The MERLIN LEGEND system permits a maximum of 16 barrier codes. The barrier code for each user should not be recorded in a place or manner that may be accessible for an unauthorized user. The code should also not indicate facts about or traits of the user that are easily researched (for example, the user's birthdate) or discernible (for example, the user's hobbies, interests, political inclinations, and the like).
- Use the system's toll restriction capabilities, to restrict the long distance calling ability of remote access users as much as possible, consistent with the needs of your business.
- Block out-of-hours calling by manually turning off the Remote Access feature at an administration telephone whenever appropriate (if the feature is dedicated on a port).
- Protect your remote access telephone number and password. Only give them to people who need them, and impress upon those people the need to keep the telephone number and password secret.
- Monitor your SMDR records and/or your Call Accounting System reports regularly for signs of irregular calls. Review these records and reports for the following symptoms of abuse:
  - — Short holding times on one trunk group
  - — Patterns of authorization code usage (same code used simultaneously or high activity)
  - — Calls to international locations not normal for your business
  - — Calls to suspicious destinations
  - — High numbers of "ineffective call attempts" indicating attempts at entering invalid barrier codes or authorization codes
  - — Numerous calls to the same number
  - — Undefined account codes

Protecting remote system programming

The Remote System Programming feature allows your system administrator to use system programming and maintenance (SPM) software to make changes to your MERLIN LEGEND Communications System programming from another location. The system can be accessed remotely either by dialing into it directly using remote access or by dialing the system operator and asking to be transferred to the system's built-in modem. The feature also may be used, at your request, by Avaya personnel to do troubleshooting or system maintenance.

However, unauthorized persons could disrupt your business by altering your system programming. In addition, they could activate features (such as Remote Access) that would permit them to make long distance calls, or they could change restriction levels to allow long distance calls that would otherwise have been blocked.

The following security measures assist you in managing the Remote System Programming feature to help prevent unauthorized use.

Security tips

- The system programming capability of the MERLIN LEGEND Communications System is protected by a password. Passwords can be up to five characters in length and can be alpha or numeric and special characters. See "Administration / maintenance access" on page 4-4 and "General security measures" on page 4-8 for secure password guidelines.
- If you use the Remote Access feature to do remote system programming on your MERLIN LEGEND Communications System, follow all of the security tips listed for protecting the Remote Access feature.
  - — Even if the Remote Access feature is used only for remote system programming, it should be protected by a barrier code.
  - — Do not write the remote access telephone number or barrier code on the MERLIN LEGEND Communications System, the connecting equipment, or anywhere else in the system room.
- Train all employees, especially your system operator, to transfer only authorized callers to the system's built-in modem for remote programming. Hackers have also been known to use "social engineering" to gain transfer to the built-in modem.

Protecting remote call forwarding

The Remote Call Forwarding feature allows a customer to forward an incoming call to another off-premises number. However, a caller could stay on the line and receive another dial tone. At this point, the caller could initiate another toll call.

The following security measures assist you in managing the Remote Call Forwarding feature to help prevent unauthorized use:

- Provide the Remote Call Forwarding capability only to those people who need it.
- Do not use this feature with loop-start lines. Due to unreliable disconnects from the carrier's central office, this feature may allow dial-tone to be re-established and additional calls to be made.

MERLIN LEGEND/MAGIX toll fraud

Why toll fraud happens[1]

99.9% of toll fraud is committed from the outside. Why? There is no programming in place to prevent it.

A small percentage of toll fraud is committed from the inside by those who are employed by the business which is serviced by the Legend/Magix. It is fairly easy to catch a person who is operating from the inside.

- Employee making calls from any extension.
- A forwarded phone to an international phone number. Calls from the outside will dial an extension number which is forwarding to the outside phone number. From there the hacker can reach any phone number.
- A customer's vendor (for example, a cleaning service) making toll calls.

Tool fraud warning signs

- Incoming calls to toll-free area codes (800,888,877, etc.) are always busy.
- Direct inward dialing lines are always busy.
- Heavy call volume – especially at night and weekends.
- Unexplained increase in long distance calls.
- Switchboard operator complaining of frequent hang ups, or touch tone sounds, when they answer.

1. Published 8/17/00

- Employees receive calls requesting the be transferred for outside “operator assistance” or outbound calls.
- Employees receive frequent calls from foreign speaking callers, requesting to be transferred, or hanging up.
- Employees having difficulty obtaining an outside line.
- The customer is unable to access voice mail, and the system is not down.
- The customer is unable to administer programming functions within either the Legend/Magix, or the voice mail system.
- Callers asking sensitive information about your system.
- Unexplained changes in system software parameters.
- Unexplained changes in your voice mail system.
- Any discrepancies in the telephone bills.
- All trunks/lines are lit up on the operator console.

Tips to prevent toll fraud

- Have the telephone and voice mail systems toll-fraud secured by Avaya.
- Educate the telephone and voice mail system users to recognized toll fraud.
- Protect voice mail system administration access.
- Restrict voice mail ports.
- Use barrier codes if remote line access is required. Change barrier codes often.
- Put restrictions on ARS (automatic route selection) table.
- Make ARS tables and disallow lists to restrict 011 (international) calls, and other “hot spots” (for example, 809 = Puerto Rico, 787 = Puerto Rico, 242 = Bahamas).
- Restrict dial “0” for local operator.
- Tracing SMDR information (or Monitor) may be required if ongoing toll fraud is suspected.
- Restrict remote call forwarding on extensions.
- Change passwords frequently.
- Be aware of hackers social engineering.
- Update system back up disks.
- Transfer callers to known extensions only.
- Outward restrict any unused extensions, including MFM extensions.

- Have only system administrator transfer calls to “*10.”
- The customer’s long distance carrier may:
  - Restrict 011 and other “hot spot” area codes.
  - Restrict access to your toll free area codes from areas you do not wish to receive calls from.
  - Put after hours restrictions to terminate calls in the network.
- Restrict third-party billing with your local carrier.

Responsibility

The customer is responsible for the security of the system. The system administrator should read all system administration documents provided with the system to fully understand the risk of toll fraud and the steps that can be taken to reduce that risk. Avaya will not be responsible for any charge that result from unauthorized use.

Programming tools to prevent fraud

Know the release of the Merlin Legend you are working with. Some earlier releases may be incapable of performing certain functions, will later releases are able to perform these functions.

Release 5.0 and earlier was unable to remote call forwarding using an authorization code. Release 6.0 and later can remote call forwarding using an authorization code.

Security of your systems: preventing toll fraud[2]

As a customer of a new telephone system, you should be aware that there is an increasing problem of telephone toll fraud. Telephone toll fraud can occur in many forms, despite the numerous efforts of telephone companies and telephone equipment manufacturers to control it. Some individuals use electronic devices to prevent or falsify records of these calls. Others charge calls to someone else’s number by illegally using lost or stolen calling cards, billing innocent parties, clipping on to someone else’s line, and breaking into someone else’s telephone equipment physically or electronically. In certain instances, unauthorized individuals make connections to the telephone network through the use of the Remote Access features of your system.

2. Published 8/31/00

The Remote Access features of your system, if you choose to use them, permit off-premises callers to access the system from a remote telephone by using a telephone number with or without a barrier code. The system returns an acknowledgment, signaling the user to key in his or her barrier code, which is selected and administered by the system manager. After the barrier code is accepted, the system returns dial tone to the user. Barrier codes are, by default, restricted from making outside calls. If no specific outward calling restrictions are programmed, the user is able to place any call normally dialed from a telephone associated with the system. Such an off-premises network call is originated at, and will be billed from, the system location.

The Remote Access feature, as designed, helps the customer, through proper administration, to minimize the ability of unauthorized persons to gain access to the network. Most commonly, telephone numbers and codes are compromised when overheard in a public location, through theft of a wallet or purse containing access information, or through carelessness (for example, writing codes on a piece of paper and improperly discarding it). Additionally, hackers may use a computer to dial an access code and then publish the information to other hackers. Enormous charges can be run up quickly. It is the customer's responsibility to take the appropriate steps to properly implement the features, evaluate and administer the various restriction levels, protect access codes, and distribute access codes only to individuals who have been fully advised of the sensitive nature of the access information.

Common carriers are required by law to collect their tariffed charges. While these charges are fraudulent charges made by persons with criminal intent, applicable tariffs state that the customer of record is responsible for payment of all long-distance or other network charges. Avaya cannot be responsible for such charges and will not make any allowance or give any credit for charges that result from unauthorized access.

To minimize the risk of unauthorized access to your system:

- Use an unpublished remote access number
- Assign access codes randomly to users on a need-to-have basis, keeping a log of all authorized users and assigning one code to each person
- Use random-sequence access codes, which are less likely to be broken
- Use the longest-length access codes the system will allow
- Deactivate all unassigned codes promptly
- Ensure that remote access users are aware of their responsibility to keep the telephone number and any access codes secure
- When possible, restrict the off-network capability of off-premises callers, using calling restrictions, facility restriction levels (Hybrid/PBX mode only), and disallowed list capabilities. A prepared Disallowed List (number 7) is provided and is designed to prevent the types of calls that toll fraud abusers often make.
- When possible, block out-of-hours calling.

- Frequently monitor system call detail reports for quicker detection of any unauthorized or abnormal calling patterns.
- Limit remote call forwarding to persons on a need-to-have basis
- Change access codes every 90 days
- Use the longest-length barrier codes possible, following the guidelines for passwords

Toll fraud prevention

Toll fraud is the unauthorized use of your telecommunications system by third parties to make long-distance telephone calls. Under the law, you, the customer, are responsible for paying part or all of those unauthorized calls. Thus, the following information is of critical importance. Unauthorized persons concentrate their activities in two areas with the MERLIN MAGIX Integrated System:

- They try to transfer out of the MERLIN MAGIX Integrated System to gain access to an outgoing trunk and make long-distance calls.
- They try to locate unused or unprotected mailboxes and use them as drop-off points for their own messages.

The following is a discussion of how toll fraud is often perpetrated and ways to prevent unauthorized access that can lead to toll fraud.

Physical security, social engineering, and general security measures

Criminals called hackers may attempt to gain unauthorized access to your system and voice messaging system in order to use the system features. Hackers often attempt to trick employees into providing them with access to a network facility (line/trunk) or a network operator. This is referred to as social engineering. Hackers may pose as telephone company employees or employees of Avaya or your authorized dealer. Hackers will go through a company's trash to find directories, dialing instructions, and other information that will enable them to break into the system. The more knowledgeable they appear to be about the employee names, departments, telephone numbers, and the internal procedures of your company, the more likely it is that they will be able to trick an employee into helping them.

Preventive measures

Take the following preventive measures to limit the risk of unauthorized access by hackers:

- Provide good physical security for the room containing your telecommunications equipment and the room with administrative tools, records, and system manager information. These areas should be locked when not attended.
- Provide a secure trash disposal for all sensitive information, including telephone directories, call accounting records, or anything that may supply information about your system. This trash should be shredded.
- Educate employees that hackers may try to trick them into providing them with dial tone or dialing a number for them. All reports of trouble, requests for moving extensions, or any other administrative details associated with the MERLIN MAGIX Integrated System should be handled by one person (the system manager) or within a specified department. Anyone claiming to be a telephone company representative should be referred to this person or department.
- No one outside of Avaya needs to use the MERLIN MAGIX Integrated System to test facilities (lines/trunks). If a caller claims to be a Avaya employee, the system manager should ask for a telephone number where the caller can be reached. The system manager should be able to recognize the number as an Avaya telephone number. Before connecting the caller to the administrative port of the MERLIN MAGIX Integrated System, the system manager should feel comfortable that a good reason to do so exists. In any event, it is not advisable to give anyone access to network facilities or operators, or to dial a number at the request of the caller.
- Any time a call appears to be suspicious, call the Avaya Fraud Intervention Center at 1 800 628-2888 (fraud intervention for System 25, PARTNER, MERLIN, and MERLIN MAGIX systems).
- Customers should also take advantage of Avaya monitoring services and devices, such as the NetPROTECT family of fraud-detection services, CAS with HackerTracker, and CAT Terminal with Watchdog. Call 1 800 638-7233 to get more information on these Avaya fraud detection services and products.

Security risks associated with transferring through voice messaging systems

Toll fraud hackers try to dial into a voice mailbox and then execute a transfer by dialing ***T**. The hacker then dials an access code (either **9** for ARS or a pooled facility code), followed by the appropriate digit string to either direct dial or access a network operator to complete the call.

All extensions are initially, and by default, restricted from dial access to pools. In order for an extension to use a pool to access an outside line/trunk, this restriction must be removed.

Preventive measures

Take the following preventive measures to limit the risk of unauthorized transfers by hackers:

- Confirm that all MERLIN MAGIX Integrated System voice mail port extension numbers are outward-restricted. This denies access to facilities (lines/trunks). Voice mail ports are, by default, outward restricted.
- As an additional security step, network dialing for all extensions, including voice mail port extensions, should be processed through ARS using dial access code 9.

******SECURITY ALERT******

The MERLIN MAGIX Integrated System ships with ARS activated with all extensions set to Facility Restriction Level 3, allowing all international calling. ***To prevent toll fraud****, ARS facility restriction levels (FRLs) should be established using:*

FRL 0 for restriction to internal dialing only.

FRL 2 for restriction to local network calling only.

FRL 3 for restriction to domestic long-distance (excluding area code 809 for the Dominican Republic as this is part of the North American Numbering Plan, unless 809 is required).

FRL 4 for international calling.

WARNING:
Default local and default toll tables are factory-assigned an FRL of 2. This simplifies the task of restricting extensions: the FRL for an extension merely needs to be changed from the default of 3.

WARNING:
Each extension should be assigned the appropriate FRL to match its calling requirements. All voice mail port extensions not used for outcalling should be assigned to FRL 0 (the factory setting).

- Deny access to pooled facility codes by removing pool dial-out codes 70, 890 899, or any others on your system.
- Create a Disallowed List or use the pre-prepared Disallowed List number 7 to disallow dialing 0, 11, 10, 1700, 1809, 1900, and 976 or 1 (wildcard) 976. Disallowed List number 7 does not include 800, 1800, 411, and 1411, but Avaya recommends that you add them. Assign all voice mail port extensions to this Disallowed List. Avaya recommends assigning Disallowed List number 7. This is an added layer of security, in case outward restriction is inadvertently removed. (Voice messaging ports are assigned, by default, to Disallowed List number 7.)

If outcalling is required by voice messaging system extensions:

- Program an ARS Facility Restriction Level (FRL) of 2 on voice mail port extensions used for outcalling.
- If 800 and 411 numbers are used, remove 1800, 800, 411, and 1411 from Disallowed List number 7.
- If outcalling is allowed to long-distance numbers, build an Allowed List for the voice mail port extensions used for outcalling. This list should contain the area code and the first three digits of the local exchange telephone numbers to be allowed.

Additional general security for voice messaging systems:

- Use a secure password for the general mailboxes.
- The default administration mailbox, 9997, must be reassigned to the system manager's mailbox/extension number and securely password protected.
- All voice messaging system users must use secure passwords known only to the user.

Security risks associated with the Automated Attendant feature of voice messaging systems

Two areas of toll fraud risk associated with the Automated Attendant feature of voice messaging systems are:

- Pooled facility (line/trunk) access codes are translated to a menu prompt to allow remote access. If a hacker finds this prompt, the hacker has immediate access. (Dial access to pools is initially factory-set to restrict all extensions: to allow pool access, this restriction must be removed by the system manager.)
- If the automated attendant prompts callers to use Remote Call Forwarding (RCF) to reach an outside telephone number, the system may be susceptible to toll fraud. An example of this application is a menu or submenu that says, "To reach our answering service, select prompt number 5," and transfers a caller to an external telephone number. Remote call forwarding can be used securely only when the central office provides

"reliable disconnect" (sometimes referred to as forward disconnect or disconnect supervision), which guarantees that the central office does not return a dial tone after the called party hangs up. In most cases, the central office facility is a loop-start line/trunk which does not provide reliable disconnect. When loop-start lines/trunks are used, if the calling party stays on the line, the central office does return a dial tone at the conclusion of the call, enabling the caller to place another call as if it were being placed from your company. Ground-start trunks provide reliable disconnect and should be used whenever possible.

Preventive measures

Take the following preventive measures to limit the risk of unauthorized use of the Automated Attendant feature by hackers:

- Do not use automated attendant prompts for automatic route selection (ARS) codes or pooled facility codes.
- Assign all unused automated attendant selector codes to zero, so that attempts to dial these are routed to the system attendant.
- If RCF is required, MERLIN MAGIX Integrated System owners should coordinate with their Avaya Account Team or authorized dealer to verify the type of central office facility used for RCF. If it is a ground-start line/trunk, or if it is a loop-start line/trunk and central office reliable disconnect can be ensured, then nothing else needs to be done. In most cases, these are loop-start lines/trunks without reliable disconnect. The local telephone company must be involved in order to change the facilities used for RCF to ground-start line/trunks. Usually, a charge applies for this change. Also, hardware and software changes may be necessary in the MERLIN MAGIX Integrated System. The MERLIN Messaging Automated Attendant feature merely accesses the RCF feature in the MERLIN MAGIX Integrated System. Without these changes being made, this feature is highly susceptible to toll fraud. These same preventive measures must be taken if the RCF feature is active for MERLIN MAGIX Integrated System extensions, whether or not it is accessed by an automated attendant menu.

Security risks associated with the Remote Access feature

Remote access allows the MERLIN MAGIX Integrated System owner to access the system from a remote telephone and make an outgoing call or perform system administration using the network facilities (lines/trunks) connected to the MERLIN MAGIX Integrated System. Hackers, scanning the public switched network by randomly dialing numbers with war dialers (a device that randomly dials telephone numbers, including 800 numbers, until a modem or dial tone is obtained), can find this feature, which will return a dial tone to them. They can even employ war dialers to attempt to discover barrier codes.

Preventive measures

Take the following preventive measures to limit the risk of unauthorized use of the MERLIN MAGIX Integrated System Remote Access feature:

- The Remote Access feature can be abused by criminal toll fraud hackers if it is not properly administered. Therefore, this feature should not be used unless there is a strong business need.
- It is strongly recommended that customers invest in security adjuncts, which typically use one-time passcode algorithms. These security adjuncts discourage hackers. Since a secure use of the Remote Access feature generally offers savings over credit-card calling, the break-even period can make the investment in security adjuncts worthwhile.
- If a customer chooses to use the Remote Access feature without a security adjunct, then multiple barrier codes should be employed, with one per user, if the system permits. The MERLIN MAGIX Integrated System permits a maximum of 16 barrier codes.
- The maximum length should be used for each barrier code, and should be changed periodically. Barrier codes, like passwords, should consist of a random, hard-to-guess sequence of digits. The MERLIN MAGIX Integrated System permits a barrier code of up to 11 digits.

Other security hints

Make sure that the automated attendant selector codes do not permit outside line selection.

Multiple layers of security are always recommended to keep your system secure.

A number of measures and guidelines that can help you ensure the security of your system and voice messaging system follow.

Educating users

Everyone in your company who uses the telephone system is responsible for system security. Users and attendants/operators need to be aware of how to recognize and react to potential hacker activity. Informed people are more likely to cooperate with security measures that often make the system less flexible and more difficult to use.

- Never program passwords or authorization codes onto auto dial buttons. Display telephones reveal the programmed numbers and internal abusers can use the auto dial buttons to originate unauthorized calls.
- Discourage the practice of writing down barrier codes or passwords. If a barrier code or password needs to be written down, keep it in a secure place and never discard it while it is active.
- Instruct operators and attendants to tell their system manager whenever they answer a series of calls where there is silence on the other end or the caller hangs up.
- Advise users who are assigned voice mailboxes to frequently change personal passwords and not to choose obvious passwords.
- Ensure that the system manager advises users with special telephone privileges (such as remote access, outcalling, and remote call forwarding) of the potential risks and responsibilities.
- Be suspicious of any caller who claims to be with the telephone company and wants to check an outside line. Ask for a callback number, hang up, and confirm the caller's identity.
- Never distribute the office telephone directory to anyone outside the company; be careful when discarding it (shred the directory).
- Never accept collect telephone calls.
- Never discuss your telephone system's numbering plan with anyone outside the company.

Educating operators

Operators or attendants need to be especially aware of how to recognize and react to potential hacker activity. To defend against toll fraud, operators should follow the guidelines below:

- Establish procedures to counter social engineering. Social engineering is a con game that hackers frequently use to obtain information that may help them gain access to your system or voice messaging system.
- When callers ask for assistance in placing outside or long-distance calls, ask for a callback extension.
- Verify the source. Ask callers claiming to be maintenance or service personnel for a callback number. Never transfer to `*10` without this verification. Never transfer to extension 900.
- Remove the headset and/or handset when the console is not in use.

Detecting toll fraud

To detect toll fraud, users and operators should look for the following:

- Lost voice mail messages, mailbox lockout, or altered greetings
- Inability to log into voice mail
- Inability to get an outside line
- Foreign language callers
- Frequent hang-ups
- Touch-tone sounds
- Caller or employee complaints that the lines are busy
- Increases in internal requests for assistance in making outbound calls (particularly international calls or requests for dial tone)
- Outsiders trying to obtain sensitive information
- Callers claiming to be the “telephone” company
- Sudden increase in wrong numbers

Establishing a policy

As a safeguard against toll fraud, follow these guidelines for your MERLIN MAGIX Integrated System and voice messaging system:

- Change passwords frequently (at least quarterly). Changing passwords routinely on a specific date (such as the first of the month) helps users to remember to do so.
- Always use the longest-length password allowed.
- Establish well-controlled procedures for resetting passwords.
- Limit the number of invalid attempts to access a voice mailbox to five or less.
- Monitor access to the MERLIN MAGIX Integrated System dial-up maintenance port. Change the access password regularly and issue it only to authorized personnel. Disconnect the maintenance port when not in use. (This however, eliminates Avaya’s 24-hour maintenance surveillance capability and may result in additional maintenance costs.)
- Create a system management policy concerning employee turnover and include these suggestions:
    - — Delete all unused voice mailboxes in the voice mail system.
    - — If a terminated employee had remote access calling privileges and a personal authorization code, remove the authorization code immediately.
    - — If barrier codes and/or authorization codes were shared by the terminated employee, these should be changed immediately.

- Regularly back up your MERLIN MAGIX Integrated System files to ensure a timely recovery should it be required. Schedule regular, off-site backups.
- Keep the remote maintenance device turned off when not in use by Avaya or your authorized dealer.
- Limit transfers to registered subscribers only.
- Use the security violations notification options (Mailbox Lock or Warning Message) to alert you of any mailbox break-in attempts. Investigate all incidents.
- Review security policies and procedures and keep them up to date.

Choosing passwords

Passwords should be the maximum length allowed by the system.

Passwords should be hard to guess and should not contain:

- All the same numbers (for example, 1111, 666666)
- Sequential characters (for example, 123456)
- Numbers that can be associated with you or your business, such as your name, birthday, business name, business address, telephone number, or social security number
- Words and commonly used names

Passwords should be changed regularly—at least on a quarterly basis. Recycling old passwords is not recommended. Never program passwords (or authorization codes or barrier codes) onto a speed dial button.

Physical security

You should always limit access to the system console (or attendant console) and supporting documentation. Following are some recommendations:

- Keep the system console and supporting documentation in an office that is secured with a changeable combination lock. Provide the combination only to those individuals having a real need to enter the office.
- Keep telephone wiring closets and equipment rooms locked.
- Keep telephone logs and printed reports in locations that only authorized personnel can enter.
- Design distributed reports so they do not reveal password or trunk access code information.
- Keep the voice messaging system remote maintenance device turned off.

Limiting outcalling

When outcalling is used to contact subscribers who are off-site, use the MERLIN MAGIX Integrated System allowed lists and disallowed lists or ARS features to minimize toll fraud.

If outcalling will not be used, outward restrict all voice messaging system ports. If outcalling will be used, for the MERLIN Messaging System, ports to be unrestricted are port 2 on a 2-port system, port 4 on a 4-port system, or port 6 on a 6-port system. All other ports should be restricted. Use outward restriction, toll restrictions, allowed lists, disallowed lists, and FRLs as appropriate to minimize the possibility of toll fraud.

Limited warranty and limitation of liability

Avaya warrants to you, the customer, that your MERLIN MAGIX Integrated System will be in good working order on the date Avaya or its authorized reseller delivers or installs the system, whichever is later (“Warranty Date”). If Avaya determines that your system cannot be repaired or replaced, Avaya will remove the system and, at your option, refund the purchase price of your system or apply the purchase price towards the purchase of another Avaya system.

If you purchased your system directly from Avaya, Avaya will perform warranty repair in accordance with the terms and conditions of the specific type of Avaya maintenance coverage you selected. If you purchased your system from a Avaya-authorized reseller, contact your reseller for the details of the maintenance plan applicable to your system.

Magix R1.5: allowed lists enhancements

Two enhancements for allowed lists are supported in Release 1.5 of the MERLIN MAGIX system:

- Number of digits has been increased.
- One-to-one wildcard character matching is supported.

14-digit allowed lists

The number of digits possible in the allowed lists has increased from 7 to 14 digits. Now you have more control when equal access codes are used, for example, 1010xxx-1-xxx-xxx-xxxx. You can allow outward or toll restricted users to dial equal access codes to specific area codes and/or exchanges.

Wildcard for allowed lists

Now you can use one-to-one wildcard character matching in allowed list entries. Press **Hold** to enter a wildcard character. The character appears as a “p” on telephone displays and in the printed report.

Consider the following when you use wildcard characters in allowed and disallowed lists:

- Disallowed list entries can be from 1 to 12 characters in length.
- Before a dialed number is compared to an entry in the allowed list, the leading “1” is dropped. Thus, an allowed list entry of “p67” (where “p” is the wildcard character) matches dialed numbers of “267,” “367,” etc., but not “167.”
- You cannot use a wildcard character to match a * or # in an allowed or disallowed list.
- A wildcard character in positions 2–13 in an allow list entry matches dialed numbers 0–9 when the dialed number is not part of a star code.

NOTE:
A star code is a central office code used to perform a specific function, such as *70 to disable call waiting.

- A wildcard character in position 1 in an allowed list entry matches dialed number 0 and 2–9.
- If a star code is an entry in an allowed or disallowed list, that entry should only have the star code because anything entered in the list after the star code is ignored by the system. The following entries are valid:
  - *67
  - *69
  - *70
  - *200

The following are examples of entries that should **not** be placed in the allowed or disallowed list:

- *67201
- *69914
- *702125551212
- *2004319255

- If a star code is an entry in an allowed or disallowed list and a dialed number matches the star code, the allowed/disallowed process is reset after the match is done. Any digits dialed after the star code are compared to entries in the allowed/disallowed lists for restriction processing.

For example: *67 and 420 are two entries in an allowed list. If someone at an outward restricted extension dials *67 420-1234, the call succeeds. If the person at the same outward restricted extension dial *67 431-1234, the call fails (431 is not in the allowed list). If the person at the same extension dials 420-1234, the call succeeds. This type of processing also applies to disallowed lists.

Legend through Magix R1 automatic route selection

******SECURITY ALERT******

Do not place remote ARS access codes in the non-local dial plan by specifying, for example, a non-local extension range such as 9000–9050 when the remote ARS access code is 9. Doing so allows DID callers to make outside calls through the remote switch and may allow transferring of outside callers to outside dial tone on a remote switch, possibly resulting in toll fraud.

Magix R1.5 automatic route selection enhancements

Because of the changes in facilities and dial plans across the USA and Canada, Release 1.5 of the MERLIN MAGIX Integrated System offers new enhancements to the Automatic Route Selection feature:

- 10- and 11-digit dialing
- 24 programmable tables
- Wildcard characters in 6-digit tables
- Enhanced 911 service
- 10- and 11-digit dialing

Some central offices allow users to dial a 10-digit telephone number (area code and telephone number without the leading “1”) to reach a telephone number that requires an area code. In Release 1.5 of MERLIN MAGIX, the MERLIN MAGIX system can route either a 10-digit (without the leading “1”) or an 11-digit (with the leading “1”) dialed call based on both the area code and the exchange code. This has been accomplished by modifying ARS to include a search of 6-digit tables whether or not the user dials a leading “1.” The ARS Absorb Digit parameter (the number of user-dialed digits that ARS absorbs, that is, does **not** dial out) for each route has been enhanced to accommodate the new 10-digit dialing.

Skip this section if 10-digit dialing is not allowed in your area.

If you program the route in the 6-Digit table to absorb N digits, the actual number of digits absorbed will be as follows:

- If the user dials an 11-digit number (including the leading “1”), ARS absorbs N digits. For example, you program the 6-Digit table to absorb 4 digits, and the user dials 1-732-555-1234. In this example, 4 digits are absorbed, and 555-1234 is the number that ARS sends as the dialed number to the central office.
- If the user dials a 10-digit number (not including the leading “1”), ARS absorbs N-1 digits. For example, you program the 6-Digit table to absorb 4 digits, and the user dials 732-555-1234. In this example, 3 digits are absorbed, and 555-1234 is the number that ARS sends as the dialed number to the central office.

To configure ARS to correctly route 10- and 11-digits numbers, do the following:

- Determine the area codes and exchanges that allow 10-digit dialing and for which you want ARS routing based on 10-digit dialing.
- Determine the routing you want for each area code and exchange in the list.
- Add the area codes and exchanges to the ARS tables:
    - If all the exchanges in an area code should be routed on the same trunk pools, add the area code to an exchange table and to an area code table.
    - If you want only certain exchanges in an area code routed based on 10-digit dialing, add the area code and the exchanges to a 6-digit table.
    - When you configure a system for 10-digit dialing and a user places an outside call preceded by the ARS dial-out code, the system searches the 6-digit tables for area code and exchange code dialed by the user. If a match is not found, the system does one of the following:
- If the user dialed a leading “1,” the system searches the area code tables. If a match is not found in the area code tables, the call is routed by the Default Toll table.
- If the user did not dial a leading “1,” the system searches the exchange tables. If a match is not found in the exchange tables, the call is routed by the Default Local table.

******SECURITY ALERT******

A user restricted from dialing a toll number (11-digit) may be able to dial that same number by using 10-digit dialing when a “leading 1” is not required. Correct this situation by programming the ARS facility restriction level, the extension restriction level, and/or the allowed/disallowed lists. In addition, because non-matching 10-digit calls go to the Default Local table with an FRL of 2, users with an FRL of 2 can make 10-digit long distance calls.

******SECURITY ALERT******

The MERLIN MAGIX Integrated System ships with ARS activated with all extensions set to Facility Restriction Level 3, allowing all international calling. To prevent toll fraud, ARS FRLs should be established using:

- FRL 0 for restriction to internal dialing only.
- FRL 2 for restriction to local network calling only.
- FRL 3 for restriction to domestic long-distance (excluding area code 809 for the Dominican Republic as this is part of the North American Numbering Plan, unless 809 is required).
- FRL 4 for international calling.

WARNING:

WARNING: Default local and default toll tables are factory-assigned an FRL of 2. This simplifies the task of restricting extensions: the FRL for an extension merely needs to be changed from the default of 3.

WARNING:

WARNING: Each extension should be assigned the appropriate FRL to match its calling requirements. All voice mail port extensions not used for outcalling should be assigned to FRL 0 (the factory setting).

- Deny access to pooled facility codes by removing pool dial-out codes 70, 890 899, or any others on your system.
- Create a disallowed list or use the pre-prepared Disallowed List number 7 to disallow dialing 0, 11, 10, 1700, 1809, 1900, and 976 or 1 (wildcard) 976. Disallowed List number 7 does not include 800, 1800, 411, and 1411, but Avaya recommends that you add them. Assign all voice mail port extensions to this disallowed list. Avaya recommends assigning Disallowed List number 7. This is an added layer of security, in case outward restriction is inadvertently removed. (Voice messaging ports are assigned, by default, to Disallowed List number 7.)

If outcalling is required by voice messaging system extensions:

- Program an ARS FRL of 2 on voice mail port extensions used for outcalling.
- If 800 and 411 numbers are used, remove 1800, 800, 411, and 1411 from Disallowed List number 7.
- If outcalling is allowed to long-distance numbers, build an allowed list for the voice mail port extensions used for outcalling. This list should contain the area code and the first three digits of the local exchange telephone numbers to be allowed.

Additional general security for voice messaging systems:

- Use a secure password for the general mailboxes.
- The default administration mailbox, 9997, must be reassigned to the system manager's mailbox/extension number and securely password protected.
- All voice messaging system users must use secure passwords known only to the user.

Magix R1.5: Wildcard characters in ARS 6-digit tables

Release 1.5 of the MERLIN MAGIX system allows one-to-one wildcard character matching in the area code entry (not the exchange code entry) of 6-digit tables. This allows ARS to program numbers such as directory assistance (xxx-555-1212) for multiple area codes with one entry.

******SECURITY ALERT******

Some regions charge for directory assistance. Also, many directory assistance calls ask you if you want to dial the number for an additional charge. Use FRLs to restrict the user from making directory assistance calls. Use the ***Hold*** *button to enter a wildcard character when you program a 6-digit table. The wildcard character appears as "p" on a telephone display and on the printed report.*

Disallowed lists

Use this procedure to establish disallowed lists. These lists are telephone numbers that cannot be dialed from specified extensions (including unrestricted extensions). A maximum of eight lists (numbered 0 through 7) with 10 entries each (numbered 0 through 9) is allowed. Each number can have a maximum of 11 digits, including wildcards. The Pause character (entered by pressing the **Hold** button) is used to designate a wildcard character—for example, to indicate that calls to a given exchange are restricted in every area code.

******SECURITY ALERT******

Create a disallowed list or use the pre-prepared Disallowed List number 7 to disallow dialing `0`*,* `11`*,* `10`*,* `1700`*,* `1809`*,* `1900`*, and* `976` *or* `1(wildcard)976`*. Disallowed List number 7 does not include* `800` *and* `1800` *and* `411` *and* `1411`*, but Avaya recommends that you add them. Assign all voice mail port extensions to this disallowed list. Avaya recommends assigning Disallowed List number 7. This is an added layer of security in case outward restriction is inadvertently removed. (Voice messaging ports are assigned, 3 by default, to Disallowed List number 7.)*

Magix R1.5: Disallowed lists enhancements

Consider the following when you use wildcard characters in disallowed lists:

- Disallowed list entries can be from 1 to 12 characters in length.
- Before a dialed number is compared to an entry in the allowed list, the leading “1” is dropped. Thus, an allowed list entry of “p67” (where “p” is the wildcard character) matches dialed numbers of “267,” “367,” etc., but not “167.”
- When a dialed number is compared to an entry in the disallowed list, the leading “1” is *not* dropped. Thus, a disallowed list entry of “p67” matches dialed numbers of “167” and “267,” “367,” etc.
- You cannot use a wildcard character to match a * or # in an allowed or disallowed list.
- A wildcard character in any position in a disallowed list entry matches dialed number 0–9 when the dialed number is not part of a star code.

NOTE:
A star code is a central office code used to perform a specific function, such as *70 to disable call waiting.

- If a star code is an entry in an allowed or disallowed list, that entry should only have the star code because anything entered in the list after the star code is ignored by the system. The following entries are valid:
  - *67
  - *69
  - *70
  - *200

The following are examples of entries that should **not** be placed in the allowed or disallowed list:

- *67201
- *69914
- *702125551212
- *2004319255

- If a star code is an entry in an allowed or disallowed list and a dialed number matches the star code, the allowed/disallowed process is reset after the match is done. Any digits dialed after the star code are compared to entries in the allowed/disallowed lists for restriction processing.

For example: *67 and 420 are two entries in an allowed list. If someone at an outward restricted extension dials *67 420-1234, the call succeeds. If the person at the same outward restricted extension dial *67 431-1234, the call fails (431 is not in the allowed list). If the person at the same extension dials 420-1234, the call succeeds. This type of processing also applies to disallowed lists.

- Disallowed List 7 has a new default entry. Entry 9 has a value of “ppp976” to support the 10-digit dialing available in Release 1.5. When you upgrade from a MERLIN MAGIX Release 1.0 system or from a MERLIN LEGEND system to a MERLIN MAGIX Release 1.5 system, you must add this new entry to Disallowed List 7 during conversion.

A star code is a central office code used to perform a specific function, such as *70 to disable call waiting.

Loop-start reliable disconnect

Disconnects signals on incoming calls on loop-start trunks are classified as one of the following:

- **Reliable**. A disconnect signal is sent to the system by the local telephone company shortly after a caller hangs up. Loop-start trunks must be reliable for remote call forwarding and trunk-to-trunk transfer. Also, reliable disconnect is strongly recommended for remote call transfers, and VMSs such as MERLIN LEGEND Mail.

NOTE:
If the local telephone company uses a short disconnect interval, do not specify a reliable disconnect signal. Also, to ensure proper voice messaging operation, and for private network systems, the system must have ground-start or loop-start trunks with reliable disconnect.

- **Unreliable**. A disconnect signal is not sent by the local telephone company on every call.

****** SECURITY ALERT ******

Toll fraud can occur when loop-start lines/trunks are used with unreliable disconnect. If the Legend user stays on the line after the called party hangs up, the central office will return a dial tone at the conclusion of the call enabling the user to place another call as if it were being placed from your company. This call will not show up on SMDR. This overrides restrictions of the phone.

Since the disconnect signal on most loop-start trunks is unreliable, the factory setting for the disconnect signal is **unreliable**.

If you select **reliable** disconnect, you can set the interval after which the line/trunk is released.

Trunk-to-trunk transfer is programmed on a per-extension basis and should remain disabled even if the loop-start trunk has reliable disconnect.

Disconnect signaling reliability

Use this procedure to classify the disconnect signal sent by the central office on loop-start trunks as one of the following:

- **Reliable**. Signal sent within a short time.
- **Unreliable**. Signal may not be provided.

****** SECURITY ALERT ******

Toll fraud can occur if you have loop-start trunks with unreliable disconnect. In this situation, if someone calls you and they hang up, the central office could send dial tone before the Legend user hangs up, allowing the user to place another call as if it originated at your company.

The setting selected applies to all trunks in the system because trunks cannot be programmed individually. The reliable/unreliable setting does not apply to loop-start trunks emulated on a T1 facility. If you specify a reliable disconnect for trunks programmed with a short hold disconnect interval, active calls, as well as trunks on hold, may be disconnected. For more information about reliable and unreliable disconnect and its implications, see the *Hardware Guide for* Avaya™ Communication Manager.

Marked system speed dial

For numbers that include confidential information, such as passwords or account billing numbers, the listing can be specifically designated in system programming to suppress the number dialed so that users with display telephones see only the code that is dialed (600–729) and not the number dialed. This is called a *marked* system speed dial code. When a number is dialed using a marked system speed dial code, any calling restrictions (such as toll or outward restrictions) assigned to the extension are overridden. In addition, the system speed dial code is printed on Station Message Detail Recording (SMDR) reports instead of the number.

Night service group assignment

Each night service group is associated with either an individual QCC (in Hybrid/PBX mode) or an individual DLC through system programming.

A night service group can include the following types of members:

- Any type of extension
- One calling group for each night service group
- Calling group with one non-local member

- Outside lines can be assigned to night service groups in order for calls received on these lines to receive night service treatment. The system manager can assign the following types of outside lines to night service groups:
  - Loop-start lines
  - Ground-start lines
  - NI-BRI B-channels
  - PRI B-channels that are routed by line appearance
  - Automatic incoming tie trunks
- The following types of outside lines cannot be assigned to night service groups:
  - DID (Direct Inward Dial) trunks
  - Dial-in tie trunks
  - PRI B-channels that are routed by dial plan
  - Line/trunk jacks programmed for alarm, music-on-hold, or paging
  - Unequipped line/trunk jacks
- Night service group members and operators must all be local system users. Private trunks should not be assigned to night service groups.

During night service operation, calls received on lines assigned to a night service group ring at the night service destination for the group (an extension or calling group). A line need not be assigned to an operator position in order to receive night service coverage to a calling group.

Lines that are not assigned to a night service group, whether or not they appear at operator consoles, do not receive night service treatment.

****** SECURITY ALERT ******

If night service is used to activate remote administration you should not use a line with a published telephone number. Professional toll fraud criminals scan telephone directories for published local and 800 telephone numbers. Using these numbers, they attempt to gain access to the system, then may use such features as remote access to reach outside facilities from within the system.

Remote Access feature

The Remote Access feature allows people to use the system by dialing the number of a line/trunk designated for remote access. The remote user should be required to dial a barrier code (password) after reaching the system. Beginning with Release 3.0, the system-wide barrier code length is programmed for a minimum of 4 digits and a maximum of 11. After gaining access to the system, a remote user can do any of the following:

- Dial extension numbers directly without going through a system operator. Remote callers can call inside extensions, data workstations, or calling groups just as if they were calling from an extension within the system.
- Select a regular or special-purpose outside line (for example, a WATS line) or a pool or ARS line to make outgoing calls. If the pool is busy, the system can be programmed to allow the remote user to use Callback to queue a call for the busy pool.
- Arrange to have calls forwarded, change the forwarding destination, or cancel forwarding to a telephone inside or outside the system.

****** SECURITY ALERT ******

Security of your system. *As a customer of a new communications system, you should be aware that telephone toll fraud is an increasing problem. Telephone toll fraud can occur in many forms, despite the numerous efforts of telephone companies and telephone equipment manufacturers to control it. Some individuals use electronic devices to prevent or falsify records of these calls. Others charge calls to someone else's number by illegally using lost or stolen calling cards, billing innocent parties, clipping on to someone else's line, and breaking into someone else's telephone equipment physically or electronically. In certain instances, unauthorized individuals make connections to the telephone network through the use of remote access features.*

The Remote Access feature of your system, if you choose to use it, permits off-premises callers to access the system from a remote telephone by using an 800 number or a 7- or 10-digit telephone number. The system returns an acknowledgment signaling you to key in your barrier code, which is selected and programmed by the system manager. After the barrier code is accepted, the system returns a dial tone to you. If restrictions are not in place, you can place any call normally dialed from a telephone within the system. Such an off-premises network call is originated at, and will be billed from, the system location.

The Remote Access feature, as designed, helps the customer, through proper programming, to minimize the ability of unauthorized persons to gain access to the network. Most commonly, telephone numbers and codes are compromised when overheard in a public location, through theft of a wallet or purse containing access information, or through carelessness (writing codes on a piece of paper and improperly discarding it). Additionally, hackers may use a computer to dial an access code and then publish the information to other hackers. Enormous charges can be run up quickly. It is the customer's responsibility to take the

appropriate steps to properly implement the features, evaluate and program the various restriction levels, protect access codes, and distribute access codes only to individuals who have been fully advised of the sensitive nature of the access information.

Common carriers are required by law to collect their tariffed charges. If these charges are fraudulent charges made by persons with criminal intent, applicable tariffs state that the customer of record is responsible for payment of all long-distance or other network charges. Avaya cannot be responsible for such charges and will not make any allowance or give any credit for charges that result from unauthorized access.

To minimize the risk of unauthorized access to your communications system:

- Program the maximum length (11) for systemwide barrier code length (Release 3.0 and later).
- Use an unpublished remote access number.
- Assign barrier codes randomly to users on a need-to-have basis, keeping a log of all authorized users and assigning one code to one person.
- Use random-sequence barrier codes, which are less likely to be easily broken.
- Deactivate all unassigned codes promptly.
- Ensure that remote access users are aware of their responsibility to keep the telephone number and any barrier codes secure.
- When possible, restrict the off-network capability of off-premises callers, through use of calling restrictions and disallowed list features.
- When possible, block out-of-hours calling.
- Frequently monitor system call detail reports for quicker detection of any unauthorized or abnormal calling patterns.
- Limit remote call forwarding to persons on a need-to-have basis.
- Change barrier codes periodically.
- Beginning with Release 3.0, additional security to prevent telephone toll fraud is included:
- The remote access default requires a barrier code.
- The barrier code is a flexible-length code ranging from 4 to 11 digits (with a default of 7) and includes the * character. The length is set system-wide.
- The user is given three attempts to enter the correct barrier code.

- Whether or not the dialed digits are correct, an inter-digit time-out occurs during the first attempt. The system processes only the valid number of digits. So if a hacker enters four digits and the length is four digits, he or she hears dial tone. If a hacker enters four digits and keeps entering more, the system uses the time-out to hide the correct number of digits from the hacker. The time-out recurs until the caller has dialed the eleventh digit—giving the impression that additional digits are required—even if the barrier code length is shorter.
- SMDR registers 16 zeros for any remote access calls in which three failed attempts have occurred.

Trunk-to-trunk transfer

This section contains instructions to allow or disallow trunk-to-trunk transfer at each extension.

If trunk-to-trunk transfer is disallowed on an extension in a private network, the extension cannot transfer an outside call to a local system trunk connected to the PSTN. See Administration for *Network Connectivity for* Avaya™ Communication Manager for more information.

Trunk-to-trunk transfer may only be performed on ground-start trunks and loop-start trunks with reliable disconnect. As of Release 4.0, trunk-to-trunk transfer may be performed on BRI, tie lines, PRI, ground-start trunks, and loop-start trunks that have reliable disconnect.

Trunk-to-trunk transfer is factory set to disabled and may be enabled for a specific extension. Single-line telephones are restricted from completing a trunk-to-trunk transfer.

Toll fraud investigation: disallow list information[3]

General information

Hierarchy of ways to restrict an extension:

- FRL takes precedence over everything, except marked system speed dials.
- Marked system speed dial takes precedence over anything.
- Allow list takes precedence over call restrictions (outward, toll, unrestricted).
- Disallow list takes precedence over an allow list.

3. Published 8/8/00; Reviewed for accuracy by Sue Fulmer, Tier III Senior Engineer.

“Pauses” (p =wildcard): Have always been available on Legend disallow lists.

“ * “ : Up to R3.1, was not permitted in the disallow lists. (it has always been permitted in an allowed list, if it is not the first character.)

R3.1 < releases has a default disallow list which is assigned to all voice mail ports. This list includes: 0, 10, 11, 1809, 1700, 1900, 976, 1ppp976, *.

If the international country code is known, which the customer wants to restrict access to, make the disallow list entry as follows:

Ex: 011582Venezuela

Standard disallow list entries

0	Operator assistance.
010	Long distance with operator assistance.
10	Long distance with operator assistance.
11	Use with rotary dial phones and * codes (1+ dialing)
011	United States long distance dialing code.
555	Pay per minute “information” toll call.
1555	Pay per minute “information” toll call.
1ppp555	Pay per minute “information” toll call with wildcards. Access to “information” in any area code.
700	Pay per minute toll call.
1700	Pay per minute toll call.
1ppp700	Pay per minute toll call.
888	Toll free call.
877	Toll free call.
866	Toll free call.
855	Toll free call.
800	Toll free call.
900	Pay per minute toll call.

1900	Pay per minute toll call.
1ppp900	Pay per minute toll call with wildcards.
976	Pay per minute toll call.
1976	Pay per minute toll call.
1ppp976	Pay per minute toll call with wildcards.
ppp1976	Pay per minute toll call where wildcards are used to access 976.
*	Programming code for use with rotary phones.

Other area codes to include on the disallow lists.

Caribbean Islands

242	Bahamas
246	Barbados
268	Antigua
340	Virgin Islands
441	Bermuda
473	Granada
758	St. Lucia
787	Puerto Rico
345	Cayman Islands

Questions to ask the customer

- Voice mail ports:
  - Do any mailboxes use outcalling to a pager/cell phone?
  - Do any mailboxes use outcalling to an internal extension?
- Does any extension have remote call forwarding permission?
  - YES = Notify customer to program an allow list and disallow list for that extension.
  - NO = Remove all remote call forwarding permission from all extensions.

- Can the remote access password be changed?
  - From “craftr4” to something else.
- Does any extension need to be able to dial 0?
- Can all unused and MFM extensions be restricted?
  - Outward restricted.
  - FRL = 0.

LEGEND/MAGIX toll fraud at a glance[4]

Release and Version of the Legend/Magix.

- Different releases have different capabilities.

Operating Mode.

Operator Extension(s).

System Set Up. **(Print)**

- Password.
- Type of cards. Do they have a T1?

Trunk Information. **(Print)**

- Check remote access of trunks.

Trunk to Trunk Transfer

- Extensions > Trk Transfer > (page down) (inspect): Will list the extensions which have this permission.

Trunk Tie **(Print) ****Only if the customer has a T1.

- Check for wink/wink.
- If T1 is PRI, there is no information listed in this print.

PRI. **(Print) **** If the customer has a T1 which is PRI.

- Check for remote access: check for dial plan routing table.

Remote Access. **(Print)**

- Check if barrier code is required.
- Check for restrictions.

4. Published 8/30/00

System Directory. **(Print)**

- Check for marked system speed dials.

Calling Groups. **(Print)**

- Identify voice mail extension ports.
- Identify lines on the IntegratedVMI group. (automated attendant vs live body answering)

Extension Directory **(Print)**

- Check for voice mail extension ports.
  - FRL level.
  - Restriction level.
  - Remote call forwarding.
- Check for remote call forwarding of all extensions.
  - Unused extensions including MFMs should be outward restricted, with FRL=0.

Disallow List **(Print)**

- Check for the basic list.
- Add list(s) if necessary.

Disallow To List **(Print)**

- Check to be sure **ALL** extensions (including unused) are referencing the general list(s).
- Check that voice mail extension ports are referencing the toll free list.

Individual Voice Mail Extension Ports **(Print)**

- Check for dial out code(s), and remove if present.

ARS Table **(Print)**

- FRL levels of all tables.
- Dial 0.
- Pattern A/B: Delineates time of day pool(s) are to be used. Can be used to restrict use of specific pools (ex: T1=70, etc.)

Access Log.

- If the customer sees programming changes which they feel they did not make.

Allow Lists

- When outcalling is used.

Night Service

- Exclusion list: Are voice mail ports listed?

MERLIN Mail/MERLIN LEGEND Mail/MERLIN messaging toll fraud at a glance[5]

Auto Attendant

- Program all unused selector codes to go to the general mailbox or operator.
- Do not program selector codes to ARS pool codes.

System administrator extension number.

- Change the default from 9997 to something else.

Delete **ALL** unused mailboxes.

- May need to remote access via RMD using Hyperterminal.

All mailboxes should use the maximum digit length for passwords.

LEGEND/MAGIX toll fraud check list[6]

Check lines with remote access (shared or dedicated.)

- Remove if not needed.
- If needed:
  - Use barrier code.
  - ARS restrict.
  - Toll or outward restrict.
  - Assign disallow list.
  - Assign allowed list if needed.
  - If lines are loop start and reliable disconnect is set to “no”, then system will NOT allow access to outside trunk.

5. Published 8/30/00
6. Published 8/30/00

Check lines for remote call forwarding.

- Remove if not needed.
- If needed: instruct customer of possible toll fraud.

Check voice mail ports for Merlin Mail, Merlin Legend Mail, Merlin Messaging, Audix, automated attendant (stand alone), or CPE (customer provided equipment.)

- If outcalling is **not** required:
  - Outward restrict voice mail ports.
  - Change ARS restriction to 0.
  - Remove pool dial-out codes (all of them. Ex: 70, 890-899, etc.)
  - Make sure no ARS table has FRL of 0.
  - Be sure the voice mail ports are NOT assigned to any allowed list, except outcalling phone numbers used.
- If outcalling is required for local phone numbers:
  - Outward restrict voice mail ports.
  - Change ARS restrictions from 3 to 2 on:
    - Merlin Mail, Merlin Legend Mail, Merlin Messaging: if a 2 or 4 port system: last port only, the others should be changed to 0.
    - If a 6 port system, the last 2 ports should be changed to FRL=0.
    - Audix – all ports.
    - Automated attendant – not applicable.
  - Remove pool-dial-out codes.
  - Make sure no other ARS tables have FRL of 2 or less.
  - Make allowed list for outcalling numbers ONLY.
  - Make allowed to list and add voice ports on.
- If outcalling is needed for long distance numbers.
  - Outward restrict voice mail ports.
  - Change ARS restrictions from 3 to 2 on:
    - Merlin Mail, Merlin Legend Mail, Merlin Messaging: if a 2 or 4 port system: last port only, the others should be changed to 0. If a 6 port system, the last 2 ports should be changed to FRL=0.
    - Audix – all ports.
    - Automated attendant – not applicable.
  - Remove pool dial out codes (all, 70, 890-899).

- Make allowed list for outcalling numbers.
- Make sure no other ARS tables have FRL of 2 or less.
- Make allowed list and add to voice ports on:
  - Merlin Mail, Merlin Legend Mail, Merlin Messaging: if a 2 or 4 port system: last port only, the others should be changed to 0. If a 6 port system, the last 2 ports should be changed to FRL=0.
  - Audix – all ports.
  - Automated attendant – not applicable.

Make disallowed lists for voice ports.

- Make disallowed lists.
  - See “Toll Fraud Disallow List Information” for specifics on entries.
  - If customer is using 800 numbers or skypager numbers do not add 800 numbers.
- Assign all voice mail ports to disallowed lists.

Restrict ARS Table 19: Dial 0 Output.

- Remove pool from table if dial 0 for local operator is not needed.
- Customer can always dial 9-1010288 for AT&T access code, or they may dial the Sprint, MCI, etc. access code if they prefer.
- Change FRL from 3 to 4 or greater, and change FRL on extension that need access to operator from 3 or 4 to greater number (match FRL of table 19).

Check night service exclusion list. Remove voice ports from list if they are in the list.

Audix. Check with toll fraud specialists in integrated solutions for securing Audix.

Merlin Mail, Merlin Legend Mail, Merlin Messaging.

- Change password for mailboxes to the maximum digit length and change frequently.
- Change password for general mailbox to the maximum digit length and change frequently.
- Change the system administrator extension number from 9997 to something else.
- Change password for system administrator extension number (9997) to the maximum digit length and change frequently.
- Remove ALL mailboxes not used.

- Assign all unused automated attendant selector codes to go to either the operator or the general mailbox.
- See “Check voice mail ports for Merlin Mail, Merlin Legend Mail, Merlin Messaging, Audix, automated attendant (stand alone), or CPE (customer provided equipment),” page 6-46 and “Make disallowed lists for voice ports,” for other restrictions”, page 6-46.

Automated attendant – stand-alone.

- Make ports outward restricted.
- Restrict transfer to available extensions only (set for lowest and highest extension digits.)
- Set the maximum number of digits to match the dial plan.
- Change the default system password.

CPE (customer premise equipment – PBX [non Lucent/Avaya])

- Make ports outward restricted.
- Check with vendor for toll fraud security.

Lines/Trunks.

- Remote access: see step A. above.
- Loop start.
  - Reliable disconnect = YES: signal sent by local company.
  - Reliable disconnect = NO: no signal sent by local company.
  - Remote Call Forward can not be used with reliable disconnect = NO.
  - Trunk to trunk transfer can have problem with reliable disconnect = NO.
  - T1 does not respond to reliable disconnect.
  - IS3 defaults to reliable disconnect = YES.
  - Toll fraud security can not be assured.

DID (Direct Inward Dial). Should not end with the same number as the pool dial out codes (70, 890 – 899)

TIE (400 EM and/or 100D DS1)

- Outward or toll restrict if possible.
- ARS restrict.
- Use barrier codes if possible.
- Assign disallowed list.
- Assign allowed list.

DS1 – T1 and/or PRI.

- WATTS: Customers may restrict 011 and 809 (the Dominican Republic) dialing if they have no need to call overseas or the 809 area code. See Disallow List Information.
- ISDN – PRI: The way toll restrictions can be bypassed are limited on lines/trunks.

011 Restrictions (International).

- Make ARS table for 011.
  - If 011 is not needed, make the FRL on 011 table 4 or greater and change FRL on extensions which need access to 011 the same.
  - If 011 is needed, make the FRL on 011 table 4 or greater and change FRL on extensions requiring access to 011 the same.
- Make disallow list for 011.
  - Make disallow list.
  - Assign all ports not needing access to 011 (including MFM's and default locations, etc) to disallow list.
- See "Toll Fraud Investigation: Disallow List Information," page 6-40 if specific countries or areas need to be restricted.

Caribbean Islands restrictions (or any other "hot spot" geographic area) See www.nanpa.com (North American Numbering Plan Administration) or www.att.com/traveler/tools/codes.html (international country codes) for area code and geographic break downs.

Ex: 809 = Dominican Republic 441 = Bermuda 473 = Granada

787 = Puerto Rico. 268 = Antigua 345= Caiman Islands

242 = Bahamas 758 = St. Lucia

246 = Barbados 340 = Virgin Islands

- Make a table for an affected area code (ex: 809, 787, etc.) and make FRL on extensions requiring access to these area codes, the same.
- Make disallow list for affected area codes (ex: 011809, 011787, etc.) Assign **ALL** extensions not requiring access to affected area code (ex: 011809, 011787, etc.) to disallow list (include MFM's, unused extensions, and default extensions etc.)
- FRL should be set to secure toll fraud through ARS.

Extension restrictions.

- Outward restrict MFM extensions not used for calling outside.
- Outward restrict ALL unused extensions not used for calling outside.
- Outward or toll restrict extension ports not in use, not used for calling outside, and not used for calling long distance.

Passwords. Change all passwords frequently, and use the maximum digits allowed.

Remote programming access. It is recommended for customer with a PC and SPM (system programming and maintenance) software to change the password for the “*10” transfer.

CAUTION:
If the customer “forgets” the new password, requiring us to dispatch a technician to find it out, they will be billed TIV (trouble investigation).

LEGEND TOLL FRAUD INTERVENTION FORM[7]

DATE: _____ TIME: _____ IL#: _____

BUSINESS NAME: _____

ADDRESS: _____

PHONE: _____ FAX: _____

CONTACT: _____ CBR: _____

MBO: _____ INSTALLED: _____

RELEASE/VERSION: _____ MODE: PBX _____ KEY: ____ OP(S): _____

DETAILS: TF OCCURRED: _____ SUSPECTED: _____ OTHER: _____

VOICE MAIL TYPE: _____ MAIL RMD PORTS: _____

VOICE MAIL OUTCALLING: Y ____ N: ___ ALLOW LIST #: _____ AUDIX LTR: _____

VMI CALLING GRP #: _____

TYPE: _____ HUNT: _____ CVR GRP(S): _____ LINES: _____

7. Published 8/9/00

Port												
FRL												
Rstrn												
D.O.C												

REMOTE CALL FORWARDING EXTS:_____

DISALLOW LIST INT'L : _____CARIBBEAN: _____ VOICE PORTS: _____

REMOTE ACCESS LINES: _____

TIE/T1 SETTING: TIE-TOLL _____ TIE-PBX _____ DISALLOW LIST: Y_____ N _____

TIE LINE RESTRICTION: UNRESTRICTED ____ TOLL ___ OUTWARD ___

DIAL 0 TABLE: REMOVE DIAL 0 OPTION: YES ___ NO ___

MARKED SYSTEM SPEED DIALS: YES ___ NO ___ IF YES, LIST _____

TOLL FRAUD ABUSE COVERED? YES ___ NO ___

MODIFICATIONS/REMARKS:

REFERRED BY:_____ TF SPECIALIST: _____

EXHIBIT 1 8/16/00

Toll Fraud Incident Report

Business Name:

Business Address:

Contact Name:

Main Number:

System Type:

Date Work Started:

Work Performed by:

Customer Approved Changes:

- **Assigned all voice mail extensions to overseas Disallowed Lists.**
- Created Disallowed List 6, which includes most commonly dialed numbers used by hackers, and assigned to voice mail ports.
- Blocked calls to 011 (International) from all voice mail ports through Disallowed List 5.
- **Blocked calls to 809 (Caribbean Area) from all voice mail ports through Disallowed List 6.**

Recommendations:

- Update Legend/Magix's back-up.
- Transfer calls to known extension numbers only.
- Never transfer anyone to 90, 900, 500, 700, or to an outside operator.
- Outward restrict any unused extensions, including MFM's (7300) A copy of the extension directory is attached.
- Change all passwords frequently (including 9997 and 9999 and 9991, etc.)
- Delete all unused mailboxes.
- Have only the System Administrator transfer call to *10.
- CAUTION: Hackers may abuse your system through voice mail, remote line access, remote call forwarding, Table 19 (Dial 0 for local operator), TIE lines, T1, access to 500 service and social engineering. To keep your system as secure as possible, it is advised not to unrestrict any toll fraud security put into place!
- You may contact your long distance carrier and restrict 011 and 809 access, if applicable.

- You may contact your 800 carrier and restrict access to your 800#'s from locations you do not wish to receive 800 calls from, if applicable.
- You may call your local carrier and restrict 3rd party billing.
- It is recommended to restrict access to 500 service through Disallowed List 3 and Table 13.
- Using marked System Speed Dial numbers may leave an opening for toll fraud.
- Using Remote Line Access may leave an opening for toll fraud.
- Using Remote Call Forwarding may leave an opening for toll fraud.
- It is necessary to restrict the voice ports.
- It is recommended to create Disallowed List 7, and include the most commonly dialed numbers used by hackers and assign the list to the voice ports.
- It is recommended in Legend R3.0 and less, to restrict all extensions from dialing "0" for the local operator. You may dial 9-1010288 or 800-CALL-ATT instead. Not restricting may leave an opening for toll fraud. Legend R3.1 and greater, and all Magix automatically have Disallow List 7.
- Merlin Legend Mail R1. Restrict transfer to registered subscribers only.
- It is recommended to outward restrict the ports for any Auto Attendant.

EXHIBIT 2 8/16/00

Toll Fraud Incident Report

Business Name:

Business Address:

Contact Name:

Main Number:

System Type:

Date Work Started:

Work Performed by:

Customer Approved Changes:

Created Disallowed List 3 & 4: International country codes:

011582	Venezuela
011581	Venezuela
011603	South America (customer not sure where)
011595	Paraguay
011525	Mexico
011573	Columbia
011571	Columbia
011809	Dominican Republic
011372	Estonia
011528	Mexico
011506	Costa Rica
011526	Mexico
011345	CMNDS (customer not sure where this is)
011902	Nova Scotia
011813	Japan
011529	Mexico

ALL live (no phantoms) extensions listed on the extension directory, including the voice mail ports are accessing these two lists.

2: Created Disallow list 5 when encompasses the Caribbean countries:

Puerto Rico

Puerto Rico

Bahamas

Barbados

Burmuda

Antigua

St. Lucia

Virgin Islands

Granada

Camen Islands

All voice mail ports, extensions 563, 564, 565, 566, 567, 568, are accessing this list.

3. Created Disallow list 7 which includes operator, international, and pay per minute area codes, in addition to wildcard calls, were included.

operator

long distance operator assistance

long distance international

Pay per minute calls

Pay per minute calls

Pay per minute calls

1ppp976 Pay per minute calls with wildcard

* Telephone provider programming code

Directory assistance

All voice mail ports, extensions 563, 564, 565, 566, 567, 568, are accessing this list.

- Change SPM (system programming and maintenance) password from default to “june6.”
- Change T1 toll type from Tie-PBX to Toll.
- Remove remote call forwarding capabilities from extensions 7100, 7116.
- Remove dial out codes from voice mail port extensions 563 – 568.

Recommendations:

- Update Legend/Magix’s back-up.
- Transfer calls to known extension numbers only.
- Never transfer anyone to 90, 900, 500, 700, or to an outside operator.
- Outward restrict any unused extensions, including MFM’s (7300) A copy of the extension directory is attached.
- Change all passwords frequently (including 9997 and 9999 and 9991, etc.)
- Delete all unused mailboxes.
- Have only the System Administrator transfer call to *10.
- CAUTION: Hackers may abuse your system through Voice Mail, Remote Line Access, Remote Call Forwarding, Table 19 (Dial 0 for local operator), TIE Lines, T1, access to 500 service and social engineering. To keep your system as secure as possible, it is advised not to unrestrict any toll fraud security put into place!
- You may contact your Long Distance carrier and restrict 011 and 809 access, if applicable.
- You may contact your 800 carrier and restrict access to your 800#’s from locations you do not wish to receive 800 calls from, if applicable.
- You may call your local carrier and restrict 3rd party billing.
- It is recommended to restrict access to 500 service through Disallowed List 3 and Table 13.
- Using marked System Speed Dial numbers may leave an opening for toll fraud.
- Using Remote Line Access may leave an opening for toll fraud.
- Using Remote Call Forwarding may leave an opening for toll fraud.
- It is necessary to restrict the voice ports.
- It is recommended to create Disallowed List 7, and include the most commonly dialed numbers used by hackers and assign the list to the voice ports.
- It is recommended in Legend R3.0 and less, to restrict all extensions from dialing “0” for the local operator. You may dial 9-1010288 or 800-CALL-ATT instead. Not restricting may leave an opening for toll fraud. Legend R3.1 and greater, and all Magix automatically have Disallow List 7.
- Merlin Legend Mail R1. Restrict transfer to registered subscribers only.
- **It is recommended to outward restrict the ports for any Auto Attendant.**

Revised 8/17/00

EXHIBIT 3: Letter from Avaya

Dear _____,

At your request, Avaya has conducted a toll fraud investigation. Toll fraud was suspected to have occurred. The system is located at the above address. Your main listed telephone number is 775-353-4255.

Avaya has now completed its work. The attached Toll Fraud Incident Report documents all changes you approved Avaya to make to your telecommunications systems and additional security recommendations if applicable.

> *Please be advised that by performing this work, Avaya is not assuming any responsibility or liability for this, or any future toll fraud activity. Also, you should be aware that the purpose of the work performed was to promptly stop the toll fraud your company was incurring; it was not to audit or to ensure your telecommunications systems are secure.*

Avaya urges you to take every appropriate step to secure your telecommunications systems from toll fraud.

You may be interested in a copy of the Avaya Product Security Handbook (order #555-025-600). To order call 1-800-457-1235.

For questions concerning claims, liability, etc., you may call:

> Avaya Inc. Fraud Resolution Group (908-953-6988)

For questions concerning this intervention incident or for technical support, you may call:

> Avaya Inc. Technical Service Organization (800-628-2888)

Respectfully,

Alison S. Elefante
System Support Specialist
Toll Fraud Intervention Specialist
Avaya, Inc.

MERLIN Plus Communications System

This section provides information on protecting the MERLIN Plus Communications System.

Protecting remote line access (R2 only)

The Remote Line Access feature allows users to call into the MERLIN Plus Communications System from a remote location (for example, a satellite office, or while traveling) and use the system to make calls. However, unauthorized persons might learn the remote line access telephone number and password, call into the system, and make long distance calls.

The following security measures assist you in managing the Remote Line Access feature to help prevent unauthorized use.

Security tips

- Evaluate the necessity for remote line access. If this feature is not vital to your organization, consider not using it or limiting its use. If you need the feature, use as many of the security measures presented in this section as you can.
- Disallow all or selected international calls on remote line access ports.
- Administer trunk pools for originated line screening to avoid operator-assisted calls from toll-restricted stations.
- Program the Remote Line Access feature to require the caller to enter a 5-digit password before the system will allow the caller access. The password is comprised of the user's extension number (first 2 digits) plus 3 unique digits.
- Use the system's toll restriction capabilities to restrict the long distance calling ability of remote line access users as much as possible, consistent with the needs of your business.
- Block out-of-hours calling by turning off DXD and Remote Line Access features at an extension 10 telephone whenever possible.
- Protect your remote line access telephone number and password. Only give them to people who need them, and impress upon these people the need to keep the telephone number and password secret.

- Monitor your SMDR records and/or your Call Accounting System reports regularly for signs of irregular calls. Review these records and reports for the following symptoms of abuse:
  - Patterns of authorization code usage (same code used simultaneously or high activity)
  - Calls to international locations not normal for your business
  - Calls to suspicious destinations
  - High numbers of “ineffective call attempts” indicating attempts at entering invalid barrier codes or authorization codes
  - Numerous calls to the same number
  - Undefined account codes
- Activate “Automatic Call Restriction Reset” (R2 only)

Protecting remote call forwarding (R2 only)

For Release 2, the MERLIN Plus Communications System allows a customer to forward an incoming call to another (remotely located) telephone number. However, a caller could stay on the line and receive another dial tone. At this point, the caller could initiate a toll call without any outward call restrictions at all.

The following security measures assist you in managing the Remote Call Forwarding feature to help prevent unauthorized use.

- Implement the “Automatic Timeout” feature of the MERLIN Plus Communications System R2 “B” (Remote Call Forwarding feature). Contact the Avaya National Service Assistance Center (NSAC) at 800 628-2888 to determine if your system has the Automatic Timeout feature as part of the 533B memory module.
- Provide the remote call forwarding capability only to those who need it.

PARTNER II Communications System

This section provides information on protecting the PARTNER II Communications System.

Additional security measures are required to protect adjunct equipment.

- Chapter 7 contains security measures to protect the attached voice messaging system. For general security measures, refer to ''Protecting voice messaging systems'' on page 7-2. For product-specific security measures, refer to ''PARTNER II Communications System'' on page 7-55.
- Chapter 8 contains security measures to protect the Automated Attendant feature of your communications system. See ''PARTNER II Communications System'' on page 8-21.

The PARTNER II Communications System does not permit trunk-to-trunk transfers, thus reducing the risk of toll fraud. In addition, it allows individual stations to be administered for outward restriction.

An optional remote administration unit provides remote administration for all releases of the PARTNER II Communications System. Protect the remote administration unit by making sure to assign a password for unattended mode, and once remote administration is not necessary, remove it from unattended mode. Otherwise, a hacker could change the programming remotely.

PARTNER Plus Communications System

This section provides information on protecting the PARTNER Plus Communications System.

Additional security measures are required to protect adjunct equipment.

- Chapter 7 contains security measures to protect the attached voice messaging system. For general security measures, refer to ''Protecting voice messaging systems'' on page 7-2. For product-specific security measures, refer to ''PARTNER II Communications System'' on page 7-55.
- Chapter 8 contains security measures to protect the Automated Attendant feature of your communications system. See ''PARTNER Plus Communications System'' on page 8-22.

The PARTNER Plus Communications System does not permit trunk-to-trunk transfers, thus reducing the risk of toll fraud. In addition, it allows individual stations to be administered for outward restriction.

An optional remote administration unit provides remote administration for all releases of the PARTNER Plus Communications System. Protect the remote administration unit by making sure to assign a password for unattended mode, and once remote administration is not necessary, remove it from unattended mode. Otherwise, a hacker could change the programming remotely.

System 25

This section provides information on protecting the System 25.

Additional security measures are required to protect adjunct equipment.

- Chapter 7 contains security measures to protect the attached voice messaging system. For general security measures, refer to “Protecting voice messaging systems” on page 7-2. For product-specific security measures, refer to “System 25” on page 7-60.
- Chapter 8 contains security measures to protect the Automated Attendant feature of your communications system. See “System 25” on page 8-22.

System 25 allows trunk-to-trunk transfer capability, increasing the opportunities for toll fraud. However, trunk-to-trunk transfers on loop-start trunks are not allowed unless the switch is administered to allow it. A fast busy signal indicates that the transfer is not allowed. Do not allow trunk-to-trunk transfers on loop start trunks unless there is a business need for it. This may be administered from the system administration menu.

For R3V3, international calls (or international calls to selected countries) can be disallowed from a toll restricted station, and toll restricted stations can be blocked from using Interexchange Carrier Codes (IXCs) to make domestic or international direct dialed calls. Also, unless a trunk pool is administered for “Originating Line Screening,” toll restricted stations cannot make operator-assisted calls.

To further reduce the system’s vulnerability to toll fraud, outward restrict the tip/ring port to which the remote maintenance device is connected.

Protecting remote access

The Remote Access feature allows users to call into System 25 from a remote location (for example, a satellite office, or while traveling) and use the system to make calls. However, unauthorized persons might learn the remote access telephone number and password (barrier access code), call into the system, and make long distance calls.

System 25 allows up to 16 different barrier access codes and one remote maintenance barrier access code for use with the Remote Access feature. Except for R3V3, barrier access codes have a 5-digit maximum. R3V3 allows up to 15 characters, including the digits 0 to 9, #, and *. Also for R3V3, an alarm is generated at the attendant console if an invalid barrier access code is entered. For greater security, always use the maximum available digits when assigning barrier access codes.

The following security measures assist you in managing the Remote Access feature to help prevent unauthorized use.

Security tips

- Evaluate the necessity for remote access. If this feature is not vital to your organization, consider not using it or limiting its use. If you need the feature, use as many of the security measures presented in this section as you can.
- Program the Remote Access feature to require the caller to enter a password (barrier access code) before the system will allow the caller access.
- Use the system's toll restriction capabilities to restrict the long distance calling ability of remote access users as much as possible, consistent with the needs of your business. For example, allow users to make calls only to certain area codes, or do not allow international calls.
- Protect your remote access telephone number and password (barrier access code). Only give them to people who need them, and impress upon these people the need to keep the telephone number and password (barrier access code) secret.
- Monitor your SMDR records and/or your Call Accounting System reports regularly for signs of irregular calls. Review these records and reports for the following symptoms of abuse:
  - — Short holding times on one trunk group
  - — Calls to international locations not normal for your business
  - — Calls to suspicious destinations
  - — High numbers of "ineffective call attempts" indicating attempts at entering invalid barrier codes or authorization codes
  - — Numerous calls to the same number
  - — Undefined account codes

Protecting remote system administration

The Remote System Administration feature allows your telephone system administrator to make changes to your System 25 system programming from another location by dialing into the system. The feature also may be used, at your request, by Avaya personnel to do troubleshooting or system maintenance.

However, unauthorized persons could disrupt your business by altering your system programming. In addition, they could activate features (such as Remote Access) that would permit them to make long distance calls through your system.

The following security measures assist you in managing the Remote System Administration feature to help prevent unauthorized use.

Security tips

- The system administration capability of the system is protected by a password. Passwords can be up to eight characters in length and can be alpha or numeric and include the pound sign (#). See "Administration / maintenance access" on page 4-4 and "General security measures" on page 4-8 for secure password procedures. See Chapter 14 for information on how to change passwords.
- If you have a special telephone line connected to your system for remote system administration, do one of the following:
  - — Unplug the line when it is not being used.
  - — Install a switch in the line to turn it off when it is not being used.
  - — Install a security device, such as Avaya's remote port security device. (See Chapter 16 for more information.)
- Protect your remote system administration telephone number and password. Only give them to people who need to know them, and impress upon these people the need to keep the telephone number and password secret.
- If your Remote System Administration feature requires that someone in your office transfer the caller to the remote system administration extension, impress upon your employees the importance of transferring only authorized individuals to that extension.

Voice messaging systems

7

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

The information in this chapter helps prevent unauthorized users from finding pathways through the voice messaging system and out of the switch. This chapter presents each communications system, and the voice mail systems it may host.

- Communication Manager (page 7-4)
- MultiVantage™ Software (page 7-4)
- DEFINITY ECS (page 7-4)
- DEFINITY communications systems (page 7-4)
- MERLIN II Communications System (page 7-35)
- MERLIN LEGEND Communications System (page 7-38)
- PARTNER II Communications System (page 7-55)
- PARTNER Plus Communications System (page 7-57)
- System 25 (page 7-60)
- System 75 (page 7-4)
- System 85 (page 7-4)

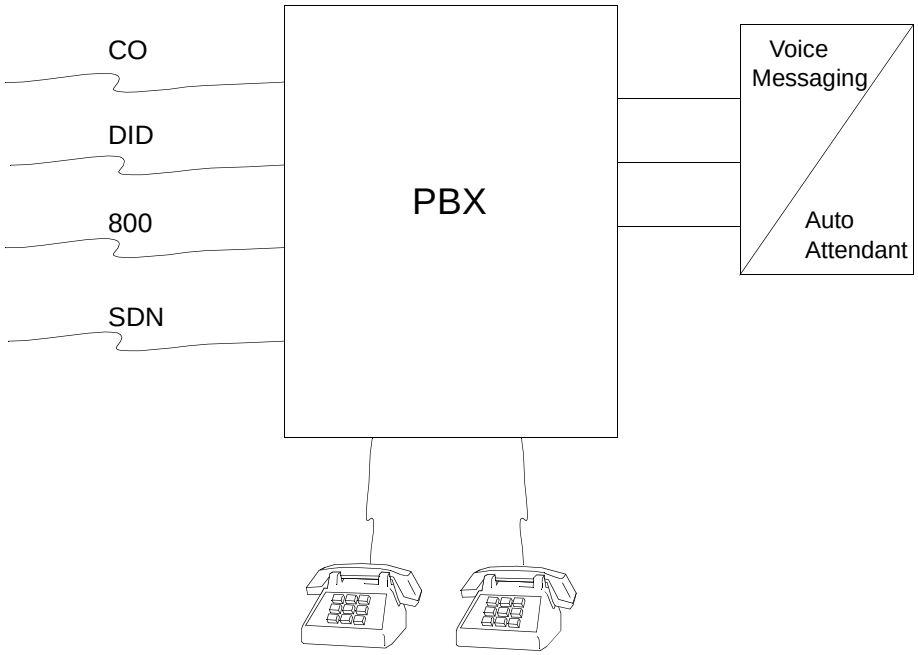
NOTE:
The tools and measures in this chapter fall into two categories; those that are implemented in the switch, and those that are implemented in the voice messaging adjunct. It is recommended that security measures related to voice adjuncts be implemented in both the switch and the voice adjunct. If you are using a non-Avaya adjunct with a Avaya switch, the switch security measures described here should be implemented as well as adjunct security measures described in the adjunct documentation supplied by the non-Avaya vendor.

Protecting voice messaging systems

Voice messaging toll fraud has risen dramatically in recent years. Now more than ever, it is imperative that you take steps to secure your communications systems. Callers into the voice messaging/automated attendant system may transfer to an outgoing trunk if adequate security measures are not implemented (see Figure 7-1).

In addition, mailboxes associated with voice messaging systems can facilitate toll fraud or industrial espionage if they are accessible to unauthorized users.

Figure 7-1. Call transfer through the PBX



Criminals attempt to transfer to the following codes:

- ARS dial access codes (most likely the digit “9”)
- Trunk access codes (TACs)
- Trunk verification codes, facility test call access codes, or data origination codes

All security restrictions that prevent transfer to these codes should be implemented. The only tool a criminal needs to breach an inadequately secured system is a touch-tone telephone. With the advent of cellular phones, hackers have yet another means of accessing voice mailboxes. If a user calls the voice mail system from a cell phone and inputs his or her password, the voice mailbox becomes vulnerable to toll fraud. Since cell phones can be monitored, a hacker can obtain the password and access the voice mailbox. Tell users not to enter passwords on a cell phone.

Security tips

- Restrict transfers back to the host PBX by not allowing transfers, by using enhanced call transfer, or by allowing transfer to subscriber only.
- When password protection into voice mailboxes is offered, it is recommended that you use the maximum length password where feasible.
- Deactivate unassigned voice mailboxes. When an employee leaves the company, remove the voice mailbox.
- Do not create voice mailboxes before they are needed.
- Establish your password as soon as your voice mail system extension is assigned. This ensures that only you will have access to your mailbox - not anyone who enters your extension number and #. (The use of only the “#” indicates the lack of a password. This fact is well-known by telephone hackers.)
- Never have your greeting state that you will accept third party billed calls. A greeting like this allows unauthorized individuals to charge calls to your company. If you call someone at your company and get a greeting like this, point out the vulnerability to the person and recommend that they change the greeting immediately.
- Never use obvious or trivial passwords, such as your phone extension, room number, employee identification number, social security number, or easily guessed numeric combinations (for example, 999999). See ‘‘Administration / maintenance access’’ on page 4-4 and “General security measures” on page 4-8 for secure password guidelines.
- Change adjunct default passwords immediately; never skip the password entry. Hackers find out defaults.
- Lock out consecutive unsuccessful attempts to enter a voice mailbox.
- Discourage the practice of writing down passwords, storing them, or sharing them with others. If a password needs to be written down, keep it in a secure place and never discard it while it is active.
- Never program passwords onto auto dial buttons.

- If you receive any strange messages on the voice mail system, if your greeting has been changed, or if for any reason you suspect that your voice mail system facilities are being used by someone else, contact the Avaya Toll Fraud Intervention Hotline.
- Contact your central office to verify that your carrier provides “reliable disconnect” for your host PBX or switch. “Reliable disconnect” is sometimes referred to as a forward disconnect or disconnect supervision. It guarantees that the central office will not return a dial tone after the called party hangs up. If the central office does not provide reliable disconnect and a calling party stays on the line, the central office will return a dial tone at the conclusion of the call. This permits the caller to place another call as if it were being placed from your company.
- Contact your voice messaging system supplier. There may be additional measures you can take to prevent unauthorized users from transferring through voice mail to outgoing trunks.

Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY communications systems, System 75,and System 85

The voice messaging products that work with these systems are listed below:

- AUDIX Voice Mail System — The AUDIX Voice Mail System is a system that is external to the Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY communications systems and connected to the switch by station lines and data links. (See ‘‘Protecting the AUDIX, DEFINITY AUDIX, and Avaya INTUITY voice mail systems’’ on page 7-16.)
- AUDIX Voice Power System — The AUDIX Voice Power System includes AUDIX Voice Power (VP), AUDIX VP Lodging, and AUDIX VP Auto Attendant. (See ‘‘Protecting the AUDIX Voice Power System’’ on page 7-30.)
- CONVERSANT Voice Information System. (See ‘‘Protecting the CONVERSANT Voice Information System’’ on page 7-33.)
- DEFINITY AUDIX System — The DEFINITY AUDIX System is a system comprised of circuit packs resident in the switch. (See ‘‘Protecting the AUDIX, DEFINITY AUDIX, and Avaya INTUITY voice mail systems’’ on page 7-16.)
- Avaya INTUITY AUDIX System — The Avaya INTUITY System includes both the INTUITY Voice Messaging System and the INTUITY Intro Voice Response System. (See ‘‘Protecting the AUDIX, DEFINITY AUDIX, and Avaya INTUITY voice mail systems’’ on page 7-16.)

Also see ‘‘Related documentation’’ in the ‘‘About this document’’ section for a list of manuals on these products.

Tools that prevent unauthorized calls

You can help prevent unauthorized callers who enter the voice messaging system from obtaining an outgoing facility by using the security tools shown in Table 7-1.

Table 7-1. Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY communications systems, System 75, and System 85 voice mail security tools

Security Tool	Switch	Page #
Enhanced call transfer (see ‘‘Protecting the AUDIX, DEFINITY AUDIX, and Avaya INTUITY Voice Mail Systems’’)	DEFINITY G1 (Issue 5.0), G2, G3, Communication Manager, MultiVantage™ Software, DEFINITY ECS, System 75 R1V3 (Issue 2.0), System 85 R2V4	7-16
Facility restriction levels*	All	7-5
Station-to-trunk restrictions*	All	7-6
Class of restriction	DEFINITY G1, G3, Communication Manager, MultiVantage™ Software, DEFINITY ECS, and System 75	7-7
Class of service	DEFINITY G2 and System 85	7-7
Toll analysis	DEFINITY G1, G2, G3, Communication Manager, MultiVantage™ Software, DEFINITY ECS, and System 85	7-7

Facility restriction levels

The switch treats all the PBX ports used by voice mail systems as stations. Therefore, each voice mail port can be assigned a COR/COS with an FRL associated with the COR/COS. FRLs provide eight different levels of restrictions for AAR/ARS/WCR calls. They are used in combination with calling permissions and routing patterns and/or preferences to determine where calls can be made. FRLs range from 0 to 7, with each number representing a different level of restriction (or no restrictions at all).

The FRL is used for the AAR/ARS/WCR feature to determine call access to an outgoing trunk group. Outgoing call routing is determined by a comparison of the FRLs in the AAR/ARS/WCR routing pattern to the FRL associated with the COR/COS of the call originator.

The higher the FRL number, the greater the calling privileges. For example, if a station is not permitted to make outside calls, assign it an FRL value of 0. Then ensure that the FRLs on the trunk group preferences in the routing patterns are 1 or higher.

For example, when voice mail ports are assigned to a COR with an FRL of 0, outside calls are disallowed. If this is too restrictive because the Outcalling feature is being used, the voice mail ports can be assigned to a COR with an FRL that is low enough to limit calls to the calling area needed.

NOTE:
Voice messaging ports that are outward restricted via COR cannot use AAR/ARS/WCR trunks. Therefore, the FRL level doesn't matter since FRLs are not checked.

Station-to-trunk restrictions

Station-to-trunk restrictions can be assigned to disallow stations from dialing specific outside trunks. By implementing these restrictions, callers cannot transfer out of voice mail to an outside facility using trunk access codes.

For G2 and System 85, if TACs are necessary for certain users to allow direct dial access to specific facilities, such as tie trunks, use the Miscellaneous Trunk Restriction feature to deny access to others. For those stations and all trunk-originated calls, always use ARS/AAR/WCR for outside calling.

NOTE:
Allowing TAC access to tie trunks on your switch may give the caller access to the Trunk Verification feature on the next switch, or the outgoing trunks through either ARS or TACs.

Class of restriction

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, each voice port on the voice mail adjunct is considered an extension to the switch and should be assigned its own unique COR. Up to 64 CORs can be defined in the system. For DEFINITY G3rV1, G3i-Global, and G3V2 and later, this has been increased to 96 CORs. The CORs are assigned to stations and trunks to provide or prevent the ability to make specific types of calls, or calls to other specified CORs. For example, a voice mail extension could be assigned to a COR that prohibits any outgoing calls.

Class of service

For DEFINITY G2 and System 85, a voice mail port must be assigned a COS. The following COS options relate to voice mail toll fraud prevention:

- Call Forward Off-Net: allows a user to call forward outside the switch to non-toll locations.
- Call Forward Follow Me: allows a user to forward calls outside the switch when other options are set.
- Miscellaneous Trunk Restrictions: restricts certain stations from calling certain trunk groups via dial access codes.
- Outward Restriction: restricts the user from placing calls over the CO, FX, or WATS trunks using dial access codes to trunks. Outward restriction also restricts the user from placing calls via ARS/WCR. Use ARS/WCR with WCR toll restrictions instead.
- Toll Restriction: prevents users from placing toll calls over CO, FX, or WATS trunks using dial access codes to trunks. Use ARS/WCR with WCR toll restrictions instead.
- WCR Toll Restriction: restricts users from dialing the ARS or WCR Network I Toll Access Code, or from completing a toll call over ARS/WCR.
- Terminal-to-Terminal Restrictions: restricts the user from placing or receiving any calls except from and to other stations on the switch.

Toll analysis

The Toll Analysis screen allows you to specify the toll calls you want to assign to a restricted call list (for example, 900 numbers) or to an unrestricted call list (for example, an outcalling number to a call pager). Call lists can be specified for CO/FX/WATS, TAC, and ARS calls, but not for tie TAC or AAR calls.

Security measures in the PBX

Security measures in the PBX are designed to prevent criminals from placing fraudulent calls once they have accessed the voice messaging system. However, these security measures do not restrict criminals from reaching the voice mail system, such as by dialing a DID station that is forwarded to the voice mail system. Incoming calls to the voice mail system may transfer to outgoing facilities if proper security measures are not implemented. Security steps can be implemented in the PBX and in the voice messaging/automated attendant system.

Limit voice mail to internal calling

If outcalling is not activated in the voice mail system, you can restrict voice mail callers from dialing an outside number by making the ports outward restricted.

For DEFINITY G1, G3, and System 75:

- Use **change cor** to display the Class of Restriction screen, then create an outward restricted COR by entering **outward** in the `Calling Party Restriction` field.
- Assign FRL 0.
- Use **change station** to assign the outward restricted COR to the voice mail ports.
- Use COR-to-COR restrictions to block voice mail ports from directly accessing the CORs of outgoing trunks. The trunk CORs should be unique.

For DEFINITY G2 and System 85:

- Use **PROC010 WORD3 FIELD19** to assign outward restriction to the voice mail ports' COS.
- Make the voice ports Toll Restricted and ARS Toll Restricted, and assign an FRL of 0. Enter **no** for all Miscellaneous Trunk Restriction Groups (MTRGs).

Restrict the outside calling area

When you assign the lowest possible FRL to the voice mail ports, you can limit the trunks that are available to callers. FRLs can be assigned to offer a range of calling regions. Choose the one that provides the most restricted calling range that is required. Table 7-2 provides suggested FRL values.

Table 7-2. Suggested values for FRLs

FRL	Suggested Value
0	No outgoing (off-switch) calls permitted.
1	Allow local calls only; deny 0+ and 1 800 calls.
2	Allow local calls, 0+, and 1 800 calls.
3	Allow local calls plus calls on FX and WATS trunks.
4	Allow calls within the home NPA.
5	Allow calls to certain destinations within the continental USA.
6	Allow calls throughout the continental USA.
7	Allow international calling. Assign attendant console FRL 7. Be aware, however, if Extension Number Portability is used, the originating endpoint is assigned FRL 7.

NOTE:
In Table 7-2, FRLs 1 through 7 include the capabilities of the lower FRLs. For example, FRL 3 allows private network trunk calls and local calls in addition to FX and WATS trunk calls. Verify the route pattern FRLs — no pattern should carry an FRL of 0.

For DEFINITY G1, G3, and System 75:

- Use **change cor** for the voice mail ports (versus subscribers) to display the Class of Restriction screen.
- Enter the FRL number (**0** through **7**) in the FRL field. Assign the lowest FRL that will meet the outcalling requirements, if the Outcalling feature is being utilized. The route patterns for restricted calling areas should have a higher FRL assigned to the trunk groups.
- Use **change route-pattern** to display the Route Pattern screen.
- Use a separate partition group for ARS on the ports used for outcalling, and limit the numbers that can be called.

NOTE:
For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, the Restricted Call List on the Toll Analysis table can also be used to restrict calls to specified areas.

For DEFINITY G2 and System 85:

- Use **PROC010 WORD3 FIELD23** to assign FRLs for use with AAR/ARS/WCR trunks. Assign higher FRLs to restricted patterns in **PROC309** than the FRL in the COS for the voice mail ports.
- For DEFINITY G2.2, do not use **PROC314** to mark disallowed destinations with a higher FRL value. **PROC314 WORD1** assigns a Virtual Nodepoint Identifier (VNI) to the restricted dial string. **PROC317 WORD2** maps the VNI to the pattern, and **PROC317 WORD2** shows the pattern preference, with the FRL in field 4.

  For earlier releases, use **PROC313** to enter disallowed destinations in the Unauthorized Call Control table.

Allow calling only to specified numbers

A reverse strategy to preventing calls is to allow outbound calls only to certain numbers. For G1 and System 75, you must specify both the area code and the office code of the allowable numbers. For G3, you can specify the area code or telephone number of calls you allow.

For DEFINITY G1 and System 75:

- Use **change ars fnpa xxx** to display the ARS FNPA Table, where **xxx** is the NPA that will have some unrestricted exchanges.
- Route the NPA to an RHNPA table (for example, **r1**).
- Use **change rnhpa r1: xxx** to route unrestricted exchanges to a pattern choice with an FRL equal to or lower than the originating FRL of the voice mail ports.
- If the unrestricted exchanges are in the Home NPA, and the Home NPA routes to **h** on the FNPA Table, use **change hnpa xxx** to route unrestricted exchanges to a pattern with a low FRL.

NOTE:
If assigning a low FRL to a pattern preference conflicts with requirements for other callers (it allows calls that should not be allowed), use ARS partitioning to establish separate FNPA/HNPA/RHNPA tables for the voice mail ports.

For DEFINITY G2 and System 85:

- Use **PROC311 WORD2** to establish 6-digit translation tables for foreign NPAs, and assign up to 10 different routing designators to each foreign NPA (area code).
- Use **PROC311 WORD3** to map restricted and unrestricted exchanges to different routing designators.
- If the unrestricted toll exchanges are in the Home NPA, use **PROC311 WORD1** to map them to a routing designator.

- If the Tenant Services feature is used, use **PROC314 WORD1** to map routing designators to patterns. If tenant services is not used, the pattern number will be the same as the routing designator number.
- Use **PROC309 WORD3** to define the restricted and unrestricted patterns.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3:

- Use **change ars analysis** to display the ARS Analysis screen.
- Enter the area codes or telephone numbers that you want to allow and assign an available routing pattern to each of them.
- Use **change routing pattern** to give the pattern preference an FRL that is equal to or lower than the FRL of the voice mail ports.

NOTE:
For DEFINITY G3, the Unrestricted Call List (UCL) on the Toll Analysis table can be used to allow calls to specified numbers through ARS/WCR. The COR for the voice mail ports should show “all-toll” restriction and access to at least one UCL.

For DEFINITY G2.2:

- Use **PROC314 WORD1** to assign a VNI to the unrestricted dial string. Map the VNI to a routing pattern in **PROC317 WORD2**, and assign a low FRL to the pattern in **PROC318 WORD1**. If you permit only certain numbers, consider using Network 3, which contains only those numbers.

Detecting voice mail fraud

Table 7-3 shows the reports that help determine if a voice mail system used with the Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY communications systems, System 75, or System 85 is being used for fraudulent purposes.

Table 7-3. Reports and monitoring techniques for voice mail

Monitoring Technique	Switch	Page #
Call detail recording (SMDR)	All	7-13
Traffic measurements and performance	All	7-14
Automatic circuit assurance	All	7-15
Busy verification	All	7-16
Call Traffic report	All	7-14
Trunk Group report	G1, G3, System 75	7-14
Traffic reports	Any with the AUDIX Voice Mail System	7-16
Call detail recording	Any with the AUDIX Voice Mail System R1V5 with Digital Networking	7-19

See ‘‘Security tips’’ on page 7-3 for additional ways to detect voice mail fraud.

NOTE:
The system administrator can also view a logfile to see if a mailbox is being hacked. For the AUDIX Voice Mail System R1, the administrator can view the logfile by typing **system:log:display**. For the DEFINITY AUDIX and Avaya INTUITY Voice Mail Systems, the administrator can view the logfile by typing **display administration-log**.

Call detail recording and / station message detail recording

With the Call Detail Recording (CDR) feature activated for the incoming trunk groups, you can check the calls into your voice mail ports. A series of short holding times may indicate repeated attempts to enter voice mailbox passwords. See also "Security violation notification (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3)" on page 5-59.

NOTE:
Most call accounting packages discard this valuable security information. If you are using a call accounting package, check to see if this information can be stored by making adjustments in the software. If it cannot be stored, be sure to check the raw data supplied by the CDR.

Review CDR for the following symptoms of voice mail abuse:

- Short holding times on any trunk group where voice mail is the originating endpoint or terminating endpoint
- Calls to international locations not normal for your business
- Calls to suspicious destinations
- Numerous calls to the same number
- Undefined account codes

NOTE:
For DEFINITY G2 and System 85, since CDR only records the last extension on the call, internal toll abusers transfer unauthorized calls to another extension before they disconnect so that the CDR does not track the originating station. If the transfer is to your voice mail system, it could give a false indication that your voice mail system is the source of the toll fraud.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- To display the Features-Related System Parameters screen, use the **change system-parameters** feature (G1 and System 75 only) or the **change system-parameters cdr** feature (G3, MultiVantage™ Software, and Communication Manager).

  NOTE:
  Also using direct TACs on some SMDRs/CDRs can result in the non-recording of fraudulent calls.

- Administer the appropriate format to collect the most information. The format depends on the capabilities of your CDR analyzing and recording device.
- Use **change trunk-group** to display the Trunk Group screen.
- Enter **y** in the `CDR Reports` field (`SMDR Reports` on older systems).

For DEFINITY G2:

- Use **PROC275 WORD1 FIELD14** to turn on the CDR for incoming calls.
- Use **PROC101 WORD1 FIELD8** to specify the trunk groups.

Call Traffic report

This report provides hourly port usage data and counts the number of calls originated by each port. By tracking normal traffic patterns, you can respond quickly if an unusually high volume of calls begins to appear, especially after business hours or during weekends, which might indicate hacker activity.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, traffic data reports are maintained for the last hour and the peak hour. For DEFINITY G2 and System 85, traffic data is available via Monitor I which can store the data and analyze it over specified periods.

Trunk Group report

This report tracks call traffic on trunk groups at hourly intervals. Since trunk traffic is fairly predictable, you can easily establish over time what is normal usage for each trunk group. Use this report to watch for abnormal traffic patterns, such as unusually high off-hour loading.

SAT, Manager I, and G3-MT reporting

Traffic reporting capabilities are built-in and are obtained through the System Access Terminal (SAT), Manager I, and G3-MT terminals. These programs track and record the usage of hardware and software features. The measurements include peg counts (number of times accessed) and call seconds of usage. Traffic measurements are maintained constantly and are available on demand. However, reports are not archived and should therefore be printed to monitor a history of traffic patterns.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- To record traffic measurements:
  - — Use **change trunk-group** to display the Trunk Group screen.
  - — In the `Measured` field, enter **both** if you have BCMS and CMS, **internal** if you have only BCMS, or **external** if you have only CMS.
- To review the traffic measurements, use **list measurements** followed by one of the measurement types (**trunk-groups**, **call-rate**, **call-summary**, or **outage-trunk**) and the timeframe (**yesterday-peak**, **today-peak**, or **last-hour**).

- To review performance, use **list performance** followed by one of the performance types (**summary** or **trunk-group**) and the timeframe (**yesterday** or **today**).

ARS measurement selection

The ARS Measurement Selection report can monitor up to 20 routing patterns (25 for G3) for traffic flow and usage.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change ars meas-selection** to choose the routing patterns you want to track.
- Use **list measurements route-pattern** followed by the timeframe (**yesterday**, **today**, or **last-hour**) to review the measurements.

For DEFINITY G2, use Monitor I to perform the same function.

Automatic circuit assurance

This monitoring technique detects a number of short holding time calls or a single long holding time call which may indicate hacker activity. Long holding times on trunk-to-trunk calls can be a warning sign. The ACA feature allows you to establish time limit thresholds defining what is considered a short holding time and a long holding time. When a violation occurs, a designated station is visually notified.

When notification occurs, determine if the call is still active. If toll fraud is suspected, use the busy verification feature (see "Busy verification" on page 7-16) to monitor the call in progress.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change system-parameters features** to display the Features-Related System Parameters screen.
- Enter **y** in the `Automatic Circuit Assurance (ACA) Enabled` field.
- Enter **local**, **primary**, or **remote** in the `ACA Referral Calls` field. If **primary** is selected, calls can be received from other switches. **Remote** applies if the PBX being administered is a DCS node, perhaps unattended, that wants ACA referral calls to go to an extension or console at another DCS node.
- Use **change trunk group *x*** (where ***x*** identifies the trunk group to be modified) to display the Trunk Group screen.
- Enter **y** in the `ACA Assignment` field.
- Establish short and long holding times. The defaults are 10 seconds (short holding time) and one hour (long holding time).

- To review, use **list measurements aca.**
- Administer an **aca** button on the console or display station to which the referral will be sent.

For DEFINITY G2 and System 85:

- Use **PROC285 WORD1 FIELD5** and **PROC286 WORD1 FIELD1** to enable ACA system-wide.
- Use **PROC120 WORD1** to set ACA call limits and number of calls thresholds.
- Use **PROC286 WORD1 FIELD3** to send the alarms and/or reports to an attendant.

Busy verification

When toll fraud is suspected, you can interrupt the call on a specified trunk group and monitor the call in progress. Callers will hear a long tone to indicate the call is being monitored.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change station** to display the Station screen for the station that will be assigned the Busy Verification button.
- In the `Feature Button Assignment` field, enter **verify**.
- To activate the feature, press the Verify button and then enter the trunk access code and member number to be monitored.

For DEFINITY G2 and System 85:

- Administer a Busy Verification button on the attendant console.
- To activate the feature, press the button and enter the trunk access code and the member number.

Protecting the AUDIX, DEFINITY AUDIX, and Avaya INTUITY voice mail systems

Toll fraud is possible when the application allows the incoming caller to make a network connection with another person. Thus, bridging to an outbound call, call transfer, and 3-way-conferencing are vulnerable areas and should be protected.

Unauthorized system use

You can minimize the risk of unauthorized people gaining access to your system by strictly following the compliance guidelines for, and using the aging feature of, your voice mail and AUDIX system administration (sa) passwords.

Additionally, the “trusted server” has direct access to AUDIX and its functionality. The same strict adherence to guidelines of trusted server passwords as with administration passwords is strongly recommended.

This section discusses security considerations for these topics.

Administration passwords

Your INTUITY AUDIX system comes equipped with administrative password features and options that you control to assist you in securing your system. These include:

- Change default administrator password
- Administrator password standards
- Administrator password aging

Changing the default administration password. When you first get your system, both the **sa** (system administrator) and **vm** (voice mail administrator) logins come with a default password. You are required to change this password immediately.

Administrator password standards. There are certain minimum standards passwords must follow to comply with the system’s standards.

Administration of password aging. You can administer several parameters of the password aging feature that will enhance the level of security the system maintains. Password aging ensures that administration passwords are changed at reasonable intervals. Use the Password Expiration feature for administrative logins to reduce the danger of unauthorized system access.

Some people tend to change a password when they must do so and then, shortly afterwards, to change back to an old familiar password. Administering the Minimum Age Before Changes feature makes it inconvenient to use this tactic.

Three additional items define the limits associated with password aging. They are listed below:

- Password Expiration
- Minimum Age Before Changes
- Expiration Warning

These items can be located by selecting `Customer/Services Administration` from the main menu.

Trusted server security

A trusted server is a computer or a software application in a domain outside of INTUITY AUDIX that uses its own login and password to launch a Avaya INTUITY Messaging Applications Programming Interface (IMAPI) LAN session and access AUDIX mailboxes. Two examples of trusted servers are:

- Synchronizer software running on an e-mail server
- Enhanced List Application (ELA) software running as a server on the Avaya INTUITY

Trusted servers can access and manipulate an AUDIX message just as the AUDIX application can do. (See *Avaya INTUITY Messaging Solutions Administration* for in-depth discussions and definitions of trusted servers, domains, and integration of e-mail and other trusted server software with AUDIX.)

Securing a system that allows access from another domain involves a two-pronged approach. You must consider security from both an internal and an external perspective. External security involves administration to prevent access from an unauthorized source, such as a trusted server or trusted server administrator. Internal security focuses on preventing, or recovering from, damage if a breach occurs (for example, a virus is transmitted in a message component, such as an attached software file).

External security for trusted servers. The trusted server is empowered to do everything to a user mailbox that an AUDIX user can do. You must administer a password that the trusted server application uses to request a connection to the AUDIX server. Additionally, to prevent unauthorized access through IMAPI into your system from an external source, such as a trusted server, you can administer an IMAPI password that the trusted server must also use when connecting to AUDIX. This IMAPI password prevents an unauthorized source from starting an IMAPI session and is used as a secondary layer of security in addition to the required trusted server password.

While administration of the IMAPI password is optional, it is *strongly recommended*. If you choose to administer this password, it is further recommended that you change it on a regular basis (for example, monthly). (If you have your administrator's password set to age automatically, you could use the system prompt telling you that your password must be changed as a reminder to change the IMAPI password, as well.)

The two new trusted server screens that have been added for Release 4 are Trusted-Server Profile and IMAPI-Password. Instructions for their administration are in the *Avaya INTUITY Messaging Solutions Administration* manual.

Internal security. INTUITY AUDIX F4 allows the transmission between domains of two new message components, including text (e-mail) and binary (software) file attachments. Within the AUDIX system, Message Manager supports these message components as well. With these new components come new security considerations, namely the inadvertent delivery of a “virus” that may be embedded in a file attachment. This can occur in *any* system that supports the delivery of binary files. While the AUDIX machine cannot be infected with viruses embedded in these software files, client machines may become infected when a user launches the application associated with the software file.

AUDIX does not perform any virus detection. Your company should carefully evaluate the security risks of file attachments and make provisions for virus detection software on PCs running an e-mail application or Message Manager. Your PC/LAN administrator(s) likely has considerable experience detecting and preventing the transmission of software viruses that you can use when planning for e-mail. Furthermore, your administrator has minimum requirements that the AUDIX server and e-mail server must meet to be allowed on the company network at all.

At a minimum, you should advise your users that file attachments should be detached (*not* launched) and scanned for viruses before use.

Traffic reports (AUDIX Voice Mail System only)

The AUDIX Voice Mail System provides tracking of traffic data over various timespans. Reviewing these reports on a regular basis helps to establish traffic trends. If increased activity or unusual usage patterns occur, such as heavy call volume on ports assigned to outcalling, they can be investigated immediately. Beginning with AUDIX Voice Mail System R1V2, the AUDIX Data Acquisition Package (ADAP) uses a PC to provide extended storage and analysis capabilities for the traffic data.

Call detail recording (AUDIX Voice Mail System only)

For the AUDIX Voice Mail System R1V5 and later, this optional feature provides a detailed view of the activity associated with each voice mail session, outgoing calls, and system-wide activity.

Voice session record (AUDIX Voice Mail System only)

The activity for each individual voice mailbox is recorded in a voice session record. A voice session begins whenever a caller attempts to log into the AUDIX Voice Mail System, is redirected to the voice mail system for call answering, enters *R, or **R, transfers from one automated attendant to another (nested), or is transferred by the Enhanced Automated Attendant feature.

The record reveals the routing of the call, including the caller (if internal), recipient, port, community, mailbox IDs (corresponds to the voice mail system subscriber's extension number input during a login or as input by the calling party), the time and duration of the call, the type of session (voice mail, call answer, guest password, or automated attendant), the message activity, and number of login attempts.

Also reported is the session termination method. Each possible termination method is assigned a value as shown in Table 7-4. This information can be downloaded to a PC using ADAP to be available on demand or at scheduled intervals.

Table 7-4. AUDIX Voice Mail System session termination values

Value	Reason for Session Termination
01	Caller transferred out of the AUDIX Voice Mail System
02	Caller disconnected established call
03	Caller abandoned call before the AUDIX Voice Mail System answered
04	Caller entered **X
05	Caller entered *R from call answer
06	Caller entered **R from voice mail
07	The AUDIX Voice Mail System terminated the call due to a system problem
08	The AUDIX Voice Mail System terminated the call due to a caller problem (for example, full mailbox timeout)
09	The AUDIX Voice Mail System terminated call originated by another AUDIX Voice Mail System
10	Transfer from an automated attendant to another automated attendant mailbox
11	Transfer from an automated attendant to a call answer mailbox
12	Transfer from an automated attendant to a mailbox with guest greeting

Outgoing voice call detail record (AUDIX Voice Mail System only)

An outgoing call record is also created for every outbound call that is originated by the AUDIX Voice Mail System via a voice port. This includes call transfers, outcalling, and message waiting activation and/or deactivation via access codes. A record is also created for call attempts for the Message Delivery feature.

The outgoing voice call detail record supplies the date the call was placed, the time, the AUDIX Voice Mail System port number used for the call, the duration of the call, the voice mailbox id, the number dialed, and the call type as shown in Table 7-5.

Table 7-5. AUDIX Voice Mail System outgoing call type values

Value	Outgoing Call Type
10	Transfer from voice mail with *****T or *0
11	Transfer from voice mail via return call
12	Transfer from call answer with *T, *0 or **0**
13	Transfer from automated attendant via menu selection
14	Transfer from automated attendant via extension specification
15	Transfer from automated attendant via time out
16	Transfer from automated attendant via *T
17	Transfer from bulletin board via *****T, *****0 or 0
20	Outcalling for any message
21	Outcalling for priority message
30	Message waiting activation/deactivation
40	Message delivery

Unsuccessful call transfer attempts can result in multiple records being created for a single session. Review these records regularly for the following signs of hacker activity:

- Failed login attempts
- Multiple call transfers for a single session
- Numerous outbound calls from the same voice mailbox
- Calls to strange places
- Heavy volume of Transfer Out of AUDIX Voice Mail System calls

Protecting passwords

The AUDIX, DEFINITY AUDIX, and Avaya INTUITY Voice Mail Systems offers passwords and password time-out mechanisms that can help restrict unauthorized users.

Voice mail systems R1V4 and later allow you to specify the minimum length required. Use a minimum of six digits, and always specify a minimum password length that is greater than the extension length. For example, if the extensions are five digits, require six or more digits for the password. A longer password is more difficult for a hacker to break, and offers greater system security.

For the Avaya INTUITY System, administrator passwords follow standard UNIX conventions, but have a 6-character minimum, one of which must be non-alpha. Subscriber passwords can be up to 15 digits.

For Communication Manager, MultiVantage™ Software, and DEFINITY ECS, administrator passwords are 3 to 10 characters, alpha and numeric. Subscriber passwords can be up to seven digits.

Voice mail subscribers are given three attempts in one call to correctly enter their mailbox before they are automatically disconnected. You also can specify how many consecutive invalid attempts are allowed before a voice mailbox is locked.

- The AUDIX, DEFINITY AUDIX, and Avaya INTUITY Voice Mail Systems provide three logins, each with individual password protection. For the AUDIX and DEFINITY AUDIX Voice Mail Systems, only one of these, “cust,” is customer-controlled. For the Avaya INTUITY Voice Mail System, “cust,” “sa,” and “vm” are customer-controlled. For administrative access to a voice mail system, the customer must log in and enter a password.

  You should routinely change the “cust,” “sa,” and “vm” login passwords, using the maximum digits allowed (10). Avaya will routinely change the passwords for the two voice mail system support logins.

- Change the administration password from the default.

- Use the “Minimum Password” feature, when available, to specify a minimum password length of at least 6 characters. Never set the minimum password to 0.

- Make sure subscribers change the default password the first time they log into the voice mail system. To insure this, make the default password fewer digits than the minimum password length.

See ‘‘Administration / maintenance access’’ on page 4-4 and ‘‘General security measures’’ on page 4-8 for secure password guidelines. See Chapter 14 for information on how to change passwords.

Security features

Before implementing any security measures to protect the voice mail system, it is important to understand how they work. You need to be aware of the possible trade-offs associated with each security measure listed below.

Basic call transfer

With the Basic Call Transfer feature, after a voice mail system caller enters *0, the system performs the following steps:

1. The voice mail system verifies that the digits entered contain the same number of digits administered for extension lengths.

   If call transfer is restricted to subscribers (for the DEFINITY AUDIX System and the Avaya INTUITY System only), the voice mail system also verifies that the digits entered match the extension number of an administered subscriber.

2. If Step 1 is successful, the voice mail system performs a switch-hook flash, putting the caller on hold.

   NOTE:
   If step 1 is unsuccessful, the voice mail system plays an error message and prompts the caller for another try.

3. The voice mail system sends the digits to the switch.
4. The voice mail system completes the transfer.

With basic call transfer, a caller can dial any number, provided the number of digits matches the length of a valid extension. So, if an unauthorized caller dials a transfer code followed by the first digits of a long-distance telephone number, such as 91809, the voice mail system passes the numbers on to the switch. (This is an example showing a 5-digit plan.) The switch interprets the first digit (9) as an access code, and the following digits as the prefix digit and area code. At this point, the caller enters the remaining digits of the phone number to complete the call.

If call transfer is restricted to subscribers (for the DEFINITY AUDIX System and the Avaya INTUITY System only), the caller cannot initiate a transfer to an off-premises destination unless the digits entered match an administered subscriber's mailbox identifier; for example, 91809. To ensure the integrity of the subscriber restriction, do not administer mailboxes that start with the same digit(s) as a valid switch trunk access node. It is strongly recommended that all transfers be restricted to subscribers when the Basic Call Transfer feature is used.

Enhanced call transfer

With the Enhanced Call Transfer feature, the voice mail system uses a digital control link message to initiate the transfer and the switch verifies that the requested destination is a valid station in the dial plan. With this feature, when voice mail system callers enter ***T** followed by digits (or ***A** for name addressing) and #, the following actions take place:

1. The voice mail system verifies that the digits entered contain the same number of digits as administered for extension lengths.

   If call transfer is restricted to subscribers (for the DEFINITY AUDIX System and the Avaya INTUITY System only), the voice mail system also verifies that the digits entered match the extension number of an administered subscriber.

   NOTE:
   When callers request a name addressing transfer, the name must match the name of an AUDIX, DEFINITY AUDIX, or Avaya INTUITY Voice Mail System subscriber (either local or remote) whose extension number is in the dial plan.

2. If Step 1 is successful, the voice mail system sends a transfer control link message containing the digits to the switch.

   If Step 1 is unsuccessful, the voice mail system plays an error message to the caller and prompts for another try.

3. The switch verifies that the digits entered match a valid station number in the dial plan.

   - If Step 3 is successful, the switch completes the transfer, disconnects the voice mail system voice port, and sends a “successful transfer” control link message to the voice mail system.
   - If Step 3 is unsuccessful, the switch leaves the voice mail system voice port connected to the call, sends a “fail” control link message to the voice mail system, and then the voice mail system plays an error message requesting another try.

With the Enhanced Call Transfer feature, the reason for a transfer is included in the control link message that the voice mail system sends to the switch. For call answer calls, such as calls that are redirected to the voice mail system when an extension is busy or does not answer, when a caller enters 0 to escape to attendant, the voice mail system normally reports the transfer to the switch as “redirected.”

The switch uses this reason to determine how to proceed with the call. If the reason for the transfer is “redirected,” the call will not follow the destination’s coverage path or its call forwarding path. This is because the switch will not redirect a previously redirected call.

This restriction may not be acceptable where it is desirable to have the call follow the coverage path of the “transferred-to” station. Enhanced call transfer can be administered to allow this type of transfer. This capability is available in AUDIX Voice Mail System R1V7, the DEFINITY AUDIX System 3.0, and the Avaya INTUITY System. Contact your Avaya Sales Representative for additional details and availability.

Transfer out of the system

The Transfer Out of AUDIX feature offers many conveniences for the AUDIX, DEFINITY AUDIX, or Avaya INTUITY Voice Mail System caller and subscriber. When this feature is enabled, the voice mail system performs the following services:

- Callers can enter ***T** or ***0** from a voice mail session to call another extension. (Callers can also enter ***T*A** for name addressing.)
- Subscribers can return calls from other subscribers.
- Callers can enter ***T** to call another extension either before or after leaving a call answer message.
- Callers can enter ***0** or **0** to escape to attendant either before or after leaving a call answer message.
- The voice mail system transfers calls from the automated attendant via a menu selection, extension request, or time out.
- The voice mail system transfers calls from the automated attendant or bulletin board sessions (some versions) when the caller enters ***T**.

NOTE:
For the DEFINITY AUDIX System Release 2.2, transfers are permitted only to numbers administered in the **transfer-dialplan** screen. Refer to your DEFINITY AUDIX System Release 2.2 documentation for additional procedures and information.

Outcalling

Outcalling automatically notifies authorized voice mail system subscribers whenever a message arrives in their voice mail. When outcalling is activated, after a caller leaves a message for a subscriber, the voice mail system calls the number designated by the subscriber and delivers a recorded message notification. Outcalling also can be used for message notification when a subscriber’s phone does not have a message indicator lamp.

Outcalling permission may be administered on a per-subscriber and a per-COS basis in the voice mail system. The maximum number of digits to be used for outcalling is administered on a per-system basis.

NOTE:
This feature is not affected by enhanced call transfer.

AMIS networking

AMIS networking (available on the DEFINITY AUDIX System, the AUDIX Voice Mail System R1V6 and later, and the Avaya INTUITY System) allows voice messages to be sent to and received from subscribers on other vendors' voice messaging systems. This service is based on the Audio Message Interchange Specification. This feature allows calls to be placed to off-premises voice messaging systems.

Message delivery

AMIS networking (available on the DEFINITY AUDIX System, the AUDIX Voice Mail System R1V6 and later, and the Avaya INTUITY System) offers a message delivery service that delivers voice messages to any designated telephone number. As in the case of outcalling, this feature allows calls to be placed to destinations that are off-premises.

Security measures

Where indicated, the security measures in this section apply to specific releases of both the AUDIX Voice Mail System and the switch.

Disallow outside calls

CAUTION:

If TAC calls are permitted, they may be accepted as a valid extension number. Even with Enhanced Call Transfer activated, toll hackers may be able to enter a TAC to get an outside line if 3-digit station numbers and 3-digit TACs are used.

The Enhanced Call Transfer feature is available on a voice mail system integrated with the System 85 R2V4, System 75 R1V3, Issue 2.0, and later software releases, DEFINITY Generic 1, Issue 5.0, and later software releases, DEFINITY Generic 2, DEFINITY Generic 3, DEFINITY ECS, MultiVantage™ Software, and Communication Manager. If you have an earlier release but want the added security offered by the Enhanced Call Transfer feature, consider upgrading to the required PBX software.

Use the following procedures to activate the Enhanced Call Transfer feature.

NOTE:

For System 75 R1V3, Issue 2.2 is required if you are using 3-digit extension numbers.

For ALL systems (Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 75, and System 85 R2V4):

1. On the AUDIX Voice Mail System R1 system:appearance screen, enter **y** in both the `Call Transfer Out of AUDIX` and `Enhanced Call Transfer` fields.

   Then press **Change/Run**.

   or

   For the DEFINITY AUDIX System and the Avaya INTUITY System, use the Feature-Related System Parameters screen and enter **enhanced** in the `Transfer Type` field. Then press **Enter**.

   NOTE:
   When the Enhanced Call Transfer feature is activated, there is a change in how the Escape to Attendant feature works. If a calling party enters 0 or *0 to transfer to the covering extension after being redirected to the voice mail system, the call does not follow the coverage path when the covering extension is busy or does not answer. The AUDIX Voice Mail System R1V7, DEFINITY AUDIX System 3.0, and Avaya INTUITY Voice Mail System allow calls to follow a coverage path.

2. On the AUDIX Voice Mail System R1 Maintenance:audits:fp screen, tab to the `Service Dispatcher` field and enter **x**.

   Tab to the `Start` field and enter **x**.

   Then press **Change/Run**.

   NOTE:
   For the DEFINITY AUDIX System and the Avaya INTUITY System, no audit is required.

3. For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

   On the switch, use **change listed-directory-numbers** to change the Listed Directory Numbers screen, and enter a 4-digit extension number that routes calls to an attendant.

4. For DEFINITY G2 and System 85:

   On the switch, use **PROC204 WORD1** to assign a Listed Directory Number and display characters for the attendant console.

   On the AUDIX Voice Mail System R1 System:appearance screen, or Feature-Related System Parameters screen for the DEFINITY AUDIX System and the Avaya INTUITY System; if “0000” appears in the System Covering Extension field, change the entry to the new 4-digit Listed Directory Number.

After you activate the Enhanced Call Transfer feature, test it by following the steps below:

1. Dial into your voice mail system.
2. Press ***T**.
3. Enter an invalid extension number followed by #.

   The failed announcement should play, followed by a prompt for another extension number.
4. Enter a valid extension number followed by #.

   You should notice that the call transfers much faster than with basic call transfer.

Disable transfer out of the system

When the Transfer Out of AUDIX feature is teamed with the Enhanced Call Transfer feature, the risk of toll fraud is minimized since the switch confirms that the number entered for the transfer is a valid PBX extension. However, if you do not need to transfer out, consider eliminating this feature (see "Transfer out of the system" on page 7-25 for details).

To do this, on the AUDIX Voice Mail System R1 System:appearance screen, enter **n** in the `Call Transfer Out of AUDIX` field. For the DEFINITY AUDIX and Avaya INTUITY Systems, use the Feature-Related System Parameters screen, entering **none** in the `Transfer Type` field.

NOTE:
If your automated attendant system uses transfer to an extension, you cannot use this security measure.

1. On the AUDIX Voice Mail System R1 Maintenance:audits:fp screen, tab to the `Service Dispatcher` field and enter **x**.
2. Tab to the `Start` field and enter **x**.
3. Then press **Change/Run**.

   NOTE:
   For the DEFINITY AUDIX System and the Avaya INTUITY System, no audit is required.

Limit outcalling

The measures you can take to minimize the security risk of outcalling depend on how it is used. When outcalling is used only to alert on-premises subscribers who do not have voice mail system message indicator lamps on their phones, you can assign an outward-restricted COR to the voice mail system voice ports.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change cor** to display the Class of Restriction screen, and then create an outward restricted COR by entering **outward** in the `Calling Party Restriction` field. The COR should carry an FRL of 0. Outward calling party restrictions and calling permissions should be blocked from all trunk CORs.
- Assign the outward restricted COR to the voice mail system voice ports.

For DEFINITY G2 and System 85:

- Use **PROC010 WORD3 FIELD19** to assign outward restriction to the voice mail system voice ports' COS. Assign an FRL of 0 to the COR, and enter **no** for all Miscellaneous Trunk Group Restrictions.

When outcalling is used for subscribers who are off-site (often the message notification is forwarded to a call pager number), three options exist to minimize toll fraud: 1) the voice mail system voice ports can be assigned to a toll-restricted COR that allows calling only within a local area, 2) the outcalling numbers can be entered into an unrestricted calling list for either ARS or toll analysis, or 3) outcalling numbers can be limited to 7 or 10 digits.

- On the voice mail system subscriber screen, turn off outcalling by entering **n** in the `Outcalling` field.
- On the voice mail system Outcalling screen, limit the number of digits that can be dialed for outcalling; allowing exactly the number of digits required to complete the call.

  NOTE:
  If outcalling is to a pager, additional digits may be required.

Protect AMIS networking

To increase security for AMIS analog networking, including the message delivery service, restrict the number ranges that may be used to address messages. Be sure to assign all the appropriate PBX outgoing call restrictions on the voice mail system voice ports.

Security tips

- Require callers to use passwords.
- Have the application verify that long distance numbers are not being requested, or verify that only permitted numbers are requested.
- Use appropriate switch translation restrictions.
- Administer all appropriate switch restrictions on the voice mail system voice ports.
- You may determine whether to allow transfer only to another system subscriber or to any extension of the correct extension length (that is, the number of digits for extensions administered through the switch). For example, your system may be configured to support the 4-digit plan, the 5-digit plan, and so on. The most secure approach, which is the default, is to only allow transfers to other system subscribers. If you decide to allow transfers to any extension, then you should check the switch COR on the voice ports for proper restrictions.
- Administer the voice mail system to use the Enhanced Call Transfer feature if the switch software allows.

  NOTE:
  When configured to operate in Digital Port Emulation mode, the DEFINITY AUDIX System does not support Enhanced Call Transfer.

Protecting the AUDIX Voice Power System

The AUDIX Voice Power System provides both automated attendant and voice mail functionality. The Automated Attendant feature answers incoming calls and routes them to the appropriate department, person, or mailbox. The voice mail feature provides call coverage to voice mailboxes along with a variety of voice messaging features.

Unauthorized persons concentrate their activities in two areas with the AUDIX Voice Power System:

- They try to transfer out of the AUDIX Voice Power System to gain access to an outgoing trunk and make long distance calls.
- They try to locate unused or unprotected mailboxes and use them as dropoff points for their own messages.

Traffic reports

The AUDIX Voice Power System tracks traffic data over various timespans. Reviewing these reports on a regular basis helps to establish traffic trends. If increased activity or unusual usage patterns occur, such as heavy call volume on ports assigned to outcalling, they can be investigated immediately.

Protecting passwords

The AUDIX Voice Power System offers password protection to help restrict unauthorized access. Subscribers should use a maximum length password and should change it routinely. Passwords can be up to 9 digits. See ''Administration / maintenance access'' on page 4-4 and ''General security measures'' on page 4-8 for secure password guidelines. See Chapter 14 for information on how to change passwords.

Security tips

The following security measures assist you in managing features of the AUDIX Voice Power System to help prevent unauthorized use.

- Set `Transfer to Subscribers Only` to **yes**. This limits transfers to only those switch extensions with a mailbox in the AUDIX Voice Power System.
- Require employees who have voice mailboxes to use passwords to protect their mailboxes. See ''Administration / maintenance access'' on page 4-4 and ''General security measures'' on page 4-8 for secure password guidelines.
- Make sure subscribers change the default password the first time they log in to the AUDIX Voice Power System.
- Have the AUDIX Voice Power System administrator delete unneeded voice mailboxes from the system immediately.
- On the System Parameters screen, use the maximum number of digits allowable for extension entry (six). This will make it more difficult for criminals to guess the login and password combinations of your users.
- Set up automated attendant selection codes so that they do not permit outside line selection.
- If you have Release 1.0 of the AUDIX Voice Power System, implement all appropriate security measures on the PBX side.
- If you do not need to use the Outcalling feature of the AUDIX Voice Power System, completely restrict the outward calling capability of the AUDIX Voice Power System ports through the COR assignments of the ports on the switch.
- If outcalling is used, restrict the calling area through the CORs of the voice ports on the switch.

WARNING:

Entering "#" transfers calls to the switch; that is, the transfer feature is always available and appropriate outgoing port restrictions must be in place to avoid toll fraud.

Security measures

The security measures described in this section do not apply if you are using Release 1.0 of the AUDIX Voice Power System. In this case, use PBX restrictions to safeguard your system.

Transfer only to system subscribers

The AUDIX Voice Power System has the ability to allow callers to transfer only to mailbox subscribers. When an AUDIX Voice Power System caller requests a transfer using ***T** followed by an extension number, the AUDIX Voice Power System can compare the extension number entered with the valid extension numbers administered in the subscriber database.

If the extension is invalid, the transfer is denied and an error message is played to the caller. However, it does not prevent transfers from pre-administered dial strings in the automated attendant from accessing the outgoing facilities. Refer to Chapter 8 for procedures to restrict the automated attendant ports.

- On the AUDIX Voice Power System, within the System Parameter Administration screen, enter **yes** in the `Transfer to Subscribers Only` field.

  NOTE:
  You cannot use this security measure if calls are transferred to people in your company who are not AUDIX Voice Power System subscribers (see "Limit transfers out of the system" on page 7-32).

Limit transfers out of the system

When you need to allow transfers to people who are not AUDIX Voice Power System subscribers, you can add their extension numbers to the AUDIX Voice Power System subscriber database, but restrict access to their voice mailboxes.

- On the System Parameter Administration screen, enter **yes** in the `Transfer to Subscriber Only` field.
- On the Subscriber Administration screen, add each extension number for non-AUDIX Voice Power System subscribers.
- Enter # in the `Subscriber Password` field to prevent access to the corresponding voice mail.
- Enter **yes** in the `Does the subscriber have switch call coverage` field. On the switch side, do not specify the AUDIX Voice Power System extension as a coverage point for any of these added extensions.

NOTE:
Although these restricted voice mailboxes cannot receive call answer messages, they do receive broadcast messages and even may receive a misdirected message from another subscriber. To save storage space, you should periodically clean out these mailboxes by accessing the restricted mailboxes and deleting all messages.

NOTE:
On AUDIX Voice Power System 2.1.1, mailboxes can be set individually to "1 minute," reducing the clean-up that these mailboxes require.

Protecting the CONVERSANT Voice Information System

This section addresses security issues for the CONVERSANT and INTUITY CONVERSANT Voice Information Systems. These systems provide a platform used to build and execute voice response applications that involve network connections. Poor application design could allow unauthorized calls to be placed through the VIS.

Two ways to prevent unauthorized use of the CONVERSANT Voice Information Systems are as follows:

- Block outbound access to the network at the switch (PBX or central office) that provides service to the VIS. Blocking outbound access includes blocking call origination, bridging, and transfer capabilities. This method does not rely on a secure VIS or robust VIS application design, and can be done by blocking all outgoing calls or transfer access (using one-way trunks for T1 or PRI), or by limiting the codes that can be dialed.
- Monitor the current VIS environment to determine if your application is at risk. This method should be used when blocking outbound access is inappropriate (for example, if the application requires outbound features, or if access to VIS administration is not well-controlled or only provides partial protection).

Protecting passwords

System administrator passwords follow standard UNIX password conventions. There are no end-user passwords. See ''Administration / maintenance access'' on page 4-4 and ''General security measures'' on page 4-8 for secure password guidelines. Also, do the following:

- Restrict the "root" login to a single individual or to as few individuals as possible.
- Do not document any passwords.
- Always change the "root" password from the default during installation and change it frequently after installation.

NOTE:
This information applies to remote maintenance board (RMB) access as well.

See Chapter 14 for information on how to change system administrator passwords.

Security measures

Design applications with toll fraud in mind.

- Make sure the application verifies that long distance numbers are not being requested, or that only permitted numbers are requested. The Transfer Call and Call Bridge capabilities of Script Builder, and the “tic” instruction at the transaction state machine (TSM) script level provide network access. If the ASAI package is loaded, additional TSM instructions and libraries provide access using the ASAI facility. In addition, a poorly designed prompt and collect action for transfer could let the caller enter any number for an outside access number.
- If numbers are contained in a database where anyone with database access can change them, or if they are entered by the caller, fraud is possible. Build the numbers into the application, or have the application control them to minimize the possibility of toll fraud.
- The VIS Feature Test (feature_tst) package contains application programs that can be assigned to channels to test system components that allow any 4-digit number to be dialed, such as transfer and call bridging. The application should not be assigned to a channel, or the package should not be loaded except when these tests are being used.
- Anyone with access to application code can hide logic in it that provides network access and is triggered under specific circumstances. Make sure that only trusted individuals can access application code.
- An application can be audited using Automatic Number Identification (ANI) capabilities through PRI and ASAI (or normal call data tools) to set up local database tables to collect numbers. If a significant number of repeat inbound calls are identified, an administrator can be notified using the Netview package, UNIX, or ARU, or an application can be spawned to call someone to alert the administrator about the calls.

Protect local and remote access.

- Restrict login access to trusted individuals with a need to maintain or administer the system.
- Restrict remote login access.
- Use the administrative interface and its security classes for logins. Certain capabilities are restricted for particular classes. For example, the Operations class cannot modify applications.
- Make sure when you use a modem that it is administered properly to prevent access by outside users. Make sure the phone is disconnected from the modem when the modem is not in use, or use the RPSD lock.
- Use standard UNIX tools to monitor login statistics.

Security tips

Toll fraud is possible when the application allows the incoming caller to make a network connection with another person. Thus, bridging to an outbound call, call transfer, and 3-way-conferencing should be protected.

- Require callers to use passwords.
- Have the application verify that long distance numbers are not being requested, or verify that only permitted numbers are requested.
- Use appropriate switch translation restrictions.
- Restrict the COR and have distinctive audible alert set to no for all analog ports assigned in the switch. If no calls are routed out of the system, assign outward restriction and an FRL of 0, and enter **no** for all trunk group CORs.

MERLIN II Communications System

The MERLIN II Communications System may be used with the MERLIN MAIL Voice Messaging System. For security measures to protect the voice messaging system, see ‘‘Protecting the MERLIN MAIL Voice Messaging System’’ on page 7-35.

Also see ‘‘Related documentation’’ in the ‘‘About this document’’ section for a list of manuals on this product.

The MERLIN II Communications System R3 offers the following features:

- It does not allow trunk-to-trunk transfer, thus reducing toll fraud exposure.

To reduce the system’s vulnerability to toll fraud, do the following:

- Program the MERLIN II Communications System to assign toll restriction level to the MERLIN MAIL Voice Messaging System ports.
- Monitor SMDR reports and/or Call Accounting System reports for outgoing calls that might be originated by internal and external abusers.

Protecting the MERLIN MAIL Voice Messaging System

Unauthorized persons concentrate their activities in two areas with the MERLIN MAIL Voice Messaging System:

- They try to use the MERLIN MAIL Voice Messaging System to gain access to an outgoing trunk in order to make long distance calls.
- They try to locate unused or unprotected mailboxes and use them as dropoff points for their own messages.

The MERLIN MAIL Voice Messaging System provides automated attendant, call answer, and voice mail functionality. The Automated Attendant feature answers incoming calls and routes them to the appropriate department, person, or mailbox. The Call Answer feature provides call coverage to voice mailboxes. The Voice Mail feature provides a variety of voice messaging features.

The area of toll fraud risk associated with the Automated Attendant feature is indicated below.

- Pooled facility (line/trunk) access codes are translated to a selector code to allow remote access. If a hacker chooses this selector code, the hacker has immediate access.

Take the following preventative measures to limit the risk of unauthorized use of the Automated Attendant feature by hackers:

- Do not program automated attendant selector codes for automatic route selection (ARS) codes or pooled facility codes.
- Assign all unused automated attendant selector codes to zero, so that attempts to dial these will be routed to the system operator or to the general mailbox.

Protecting passwords

Passwords can be up to 4 digits. See ''Administration / maintenance access'' on page 4-4 and ''General security measures'' on page 4-8 for secure password guidelines. See Chapter 14 for information on how to change passwords.

Security tips

The MERLIN MAIL Voice Messaging System can be administered to reduce the risk of unauthorized persons gaining access to the network. However, phone numbers and authorization codes can be compromised when overheard in a public location, lost through theft of a wallet or purse containing access information, or when treated carelessly (writing codes on a piece of paper and improperly discarding them).

Hackers may also use a computer to dial an access code and then publish the information for other hackers. Substantial charges can accumulate quickly. It is your responsibility to take appropriate steps to implement the features properly, to evaluate and administer the various restriction levels, and to protect and carefully distribute access codes.

To reduce the risk of unauthorized access through your voice messaging system, observe the following procedures:

- Monitor SMDR reports and/or Call Accounting System reports for outgoing calls that might be originated by internal and external abusers.
- Create a disallowed list to disallow dialing 0, 70, 011, 809, 1809, 0809, 10, 9999, 411, 1411, 800, 888, 700, 900, 976, 550, 1800, 1888,1700, 1500, 1900, 1976, 1550, 0800, 0888, 0700, 0500, 0900, 0976, and 0550. Assign all MERLIN MAIL Voice Messaging System ports to this list. Avaya recommends using List 7 — the last disallowed list. This is an added layer of security, in case other restrictions are inadvertently removed.
- Require employees who have voice mailboxes to use 4-digit passwords to protect their mailboxes.
- Require the system administrator and all voice mailbox owners to change their password from the default.
- Have employees use random sequence passwords.
- Impress upon employees the importance of keeping their passwords a secret.
- Encourage employees to change their passwords regularly.
- Use a secure password for the general mailbox.
- Reassign the system administrator's mailbox/extension number from the default of 9997. Be certain to password protect the new mailbox.
- Have the MERLIN MAIL Voice Messaging System administrator delete unneeded voice mailboxes from the system immediately.
- Set the maximum number of digits in an extension parameter appropriate to your dial plan. The MERLIN MAIL Voice Messaging System will not perform transfers to extensions greater than that number.
- When possible, restrict the off-network capability of callers by using calling restrictions and disallowed list features.
- When possible, block out-of-hours calling.
- Toll restrict all voice mail port extensions.
- Consider requiring network dialing to be allowed through ARS only.
- Deny access to pooled facility codes by removing pool dial-out codes 9, 890-899, or any others on your system.
- Instruct employees to contact their system administrator immediately if any of the following occur:
    - Strange voice mail messages are received
    - Their personal greeting has been changed
    - They suspect their MERLIN MAIL Voice Messaging System mailbox is being used by someone else

MERLIN LEGEND Communications System

The MERLIN LEGEND Communications System may be used with the following voice messaging systems:

- AUDIX Voice Power System — the AUDIX Voice Power System is a system that is external to the MERLIN LEGEND Communications System and connected to the switch by station lines and data links. (See "Protecting the AUDIX Voice Power System" on page 7-39.)
- INTUITY Voice Messaging System (See "Protecting the INTUITY Voice Messaging System" on page 7-41.)
- MERLIN MAIL Voice Messaging System. (See "Protecting the MERLIN MAIL, MERLIN MAIL-ML, MERLIN MAIL R3, and MERLIN LEGEND Mail voice messaging systems" on page 7-45.)
- MERLIN MAIL-ML Voice Message System. (See "Protecting the MERLIN MAIL, MERLIN MAIL-ML, MERLIN MAIL R3, and MERLIN LEGEND Mail voice messaging systems" on page 7-45.)
- MERLIN MAIL R3 Voice Message System. (See "Protecting the MERLIN MAIL, MERLIN MAIL-ML, MERLIN MAIL R3, and MERLIN LEGEND Mail voice messaging systems" on page 7-45.)
- MERLIN LEGEND Mail Voice Messaging System. (See "Protecting the MERLIN MAIL, MERLIN MAIL-ML, MERLIN MAIL R3, and MERLIN LEGEND Mail voice messaging systems" on page 7-45.)
- Messaging 2000 Voice Mail System (See "Maintaining Message 2000 system security" on page 7-50.)

Also see "Related documentation" in the "About this document" section for a list of manuals on these products.

The MERLIN LEGEND Communications System ships with ARS activated and all extensions set to FRL 3, allowing all international calling. To prevent toll fraud, ARS FRLs should be established using:

- FRL 0 for restriction to internal dialing only
- FRL 2 for restriction to local network calling only
- FRL 3 for restriction to domestic long distance (excluding area code 809 for the Dominican Republic, as this is part of the North American Numbering Plan, unless 809 is required)
- FRL 4 for international calling

Each extension should be assigned the appropriate FRL to match its calling requirement. All voice mail port extensions and barrier codes not used for outcalling should be assigned to FRL 0, which is the default setting for voice mail ports starting with Release 3.1. Prior to this release, the default setting is FRL 3.

Protecting the AUDIX Voice Power System

The AUDIX Voice Power System provides both automated attendant and voice mail functionality. The Automated Attendant feature answers incoming calls and routes them to the appropriate department, person, or mailbox. The voice mail feature provides call coverage to voice mailboxes along with a variety of voice messaging features.

Unauthorized persons concentrate their activities in two areas with the AUDIX Voice Power System:

- They try to transfer out of the AUDIX Voice Power System to gain access to an outgoing trunk and make long distance calls.
- They try to locate unused or unprotected mailboxes and use them as dropoff points for their own messages.

Protecting passwords

The AUDIX Voice Power System offers password protection to help restrict unauthorized access. Subscribers should use a maximum length password and should change it routinely. Passwords can be up to 9 digits. See "Administration / maintenance access" on page 4-4 and "General security measures" on page 4-8 for secure password guidelines. See Chapter 14 for information on how to change passwords.

Security tips

The following security measures assist you in managing features of the AUDIX Voice Power System to help prevent unauthorized use.

- Avaya recommends setting `Transfer to Subscribers Only` to **yes**. This limits transfers to only those valid switch extensions for which a mailbox is assigned.
- If you have Release 1.0 of the AUDIX Voice Power System, implement all appropriate security measures on the switch side.
- Require employees who have voice mailboxes to use passwords to protect their mailboxes. See "Administration / maintenance access" on page 4-4 and "General security measures" on page 4-8 for secure password guidelines.
- Make sure subscribers change the default password the first time they log in to the AUDIX Voice Power System.
- Have the AUDIX Voice Power System administrator delete unneeded voice mailboxes from the system immediately.
- On the System Parameters screen, use the maximum number of digits allowable for extension entry (six). This will make it more difficult for criminals to guess the login and password combinations of your users.

- Set up automated attendant selection codes so that they do not permit outside line selection.
- Assign toll restriction levels to the AUDIX Voice Power System ports.
- If you do not need to use the Outcalling feature of the AUDIX Voice Power System, completely restrict the outward calling capability of the AUDIX Voice Power System ports.

WARNING:
Entering "#" transfers calls to the switch; that is, the transfer feature is always available and appropriate outgoing port restrictions must be in place to avoid toll fraud.

Security measures

The security measures described in this section do not apply if you are using Release 1.0 of the AUDIX Voice Power System. In this case, use switch restrictions.

Transfer only to system subscribers

The AUDIX Voice Power System has the ability to allow callers to transfer only to mailbox subscribers. When an AUDIX Voice Power System caller requests a transfer using ***T** followed by an extension number, the AUDIX Voice Power System can compare the extension number entered with the valid extension numbers administered in the subscriber database.

If the extension is invalid, the transfer is denied and an error message is played to the caller. However, it does not prevent transfers from pre-administered dial strings in the automated attendant from accessing the outgoing facilities. Refer to Chapter 8 for procedures to restrict the automated attendant ports.

- On the AUDIX Voice Power System, within the System Parameter Administration screen, enter **yes** in the `Transfer to Subscribers Only` field.

  NOTE:
  You cannot use this security measure if calls are transferred to people in your company who are not AUDIX Voice Power System subscribers (see "Limit transfers out of the system" on page 7-32).

Limit transfers out of the system

When you need to allow transfers to people who are not AUDIX Voice Power System subscribers, you can add their extension numbers to the AUDIX Voice Power System subscriber database, but restrict access to their voice mailboxes.

- On the System Parameter Administration screen, enter **yes** in the `Transfer to Subscriber Only` field.
- On the Subscriber Administration screen, add each extension number for non-AUDIX Voice Power System subscribers.
- Enter # in the `Subscriber Password` field to prevent access to the corresponding voice mail.
- Enter **yes** in the `Does the subscriber have switch call coverage` field. On the switch side, do not specify the AUDIX Voice Power System extension as a coverage point for any of these added extensions.

NOTE:
Although these restricted voice mailboxes cannot receive call answer messages, they do receive broadcast messages and even may receive a misdirected message from another subscriber. To save storage space, you should periodically clean out these mailboxes by accessing the restricted mailboxes and deleting all messages.

NOTE:
On AUDIX Voice Power System 2.1.1, mailboxes can be set individually to “1 minute,” reducing the clean-up required to service these mailboxes.

Protecting the INTUITY Voice Messaging System

The INTUITY Voice Messaging System provides automated attendant, call answer, and voice mail functionality. The Automated Attendant feature answers incoming calls and routes them to the appropriate department, person, or mailbox. The Call Answer feature provides call coverage to voice mailboxes. The Voice Mail feature provides a variety of voice messaging features.

Voice messaging systems have two areas of weakness:

- Codes that transfer to inside or outside dial tone

  Once thieves transfer to inside dial tone, they have access to any unprotected switch features. Preventing this type of abuse requires security at both the switch and at the voice messaging system.

- Mailboxes that can be used as message drops

  Once thieves break into a mailbox, they can use it as a message drop for untraceable calls for illegal activities. if you have 800 lines that can connect to your voice messaging system, they can pass stolen information around at your expense using your 800 lines.

Protecting passwords

The INTUITY AUDIX System offers password protection to help restrict unauthorized access. Subscribers should use the longest feasible password length and should change it routinely. Passwords can be up t o 15 digits, and you can specify the minimum number of digits required. Use a minimum of five digits, and a length at least one digit longer than the extension number length. See "Administration / maintenance access" on page 4-4 and "General security measures" on page 4-8 for secure password guidelines. See Chapter 14 for information on how to change passwords.

Security tips

- At the switch or media server, assign toll restrictions to voice message system and automated attendant ports.
- If you do not use the outcalling features of the voice messaging system, restrict the outward calling capability of all voice ports.
- Use a dial plan that does not allow extensions beginning with the same digits as ARS, TAC, or verification and test codes.
- Inform all system operators that they are not to dial outside calls. Request that operators report all attempts to bypass switch restrictions to the telecommunications department for repairs or to the corporate security office for investigation.
- Restrict the numbers for outcalling with a disallowed list.
- Do not use default initial passwords that follow any scheme. Have a list of random passwords and select one when you create the mailbox. Require that the mailbox owner personally appear at the corporate security office or telecommunications office to obtain the initial password. Go over the subscriber password guidelines with the subscriber when you give out the initial password.
- Make sure subscribers change the initial password the first time they log in to the AUDIX system by making the initial password shorter than the minimum password length.
- Use the password aging feature so that users must change their passwords monthly.
- Discourage the practice of writing down passwords, storing them, or sharing them with others.
- Inform employees on how to report suspected toll fraud to the corporate security office.

Security measures

The following are suggested security measures to be used with the INTUITY AUDIX Voice Messaging System.

Basic call transfer

With the Basic Call Transfer feature, after a voice mail system caller enters ***T**, the system performs the following steps:

1. The voice mail system verifies that the digits entered contain the same number of digits administered for extension lengths.

   If call transfer is restricted to subscribers (for the DEFINITY AUDIX System and the Avaya INTUITY System only), the voice mail system also verifies that the digits entered match the extension number of an administered subscriber.

2. If Step 1 is successful, the voice mail system performs a switch-hook flash, putting the caller on hold.

   NOTE:
   If Step 1 is unsuccessful, the voice mail system plays an error message and prompts the caller for another try.

3. The voice mail system sends the digits to the switch.
4. The voice mail system completes the transfer.

With this feature, a caller can dial any number provided the number of digits matches the length of a valid extension. So, if an unauthorized caller dials a transfer code followed by the first digits of a long-distance telephone number, such as 91809, the voice mail system passes the numbers on to the switch. (This is an example showing a 5-digit plan.) The switch interprets the first digit (9) as an access code, and the following digits as the prefix digit and area code. At this point, the caller enters the remaining digits of the phone number to complete the call.

If call transfer is restricted to subscribers (for the DEFINITY AUDIX System and the Avaya INTUITY System only), the caller cannot initiate a transfer to an off-premises destination unless the digits entered match an administered subscriber's mailbox identifier; for example, 91809. To ensure the integrity of the subscriber restriction, do not administer mailboxes that start with the same digit(s) as a valid trunk access code. It is strongly recommended that all transfers be restricted to subscribers when the Basic Call Transfer feature is used.

Closely monitor all mailboxes

The use of INTUITY AUDIX system security features in combination with mailbox administration can help reduce the risk of unauthorized use of mailboxes.

- Lock out multiple consecutive attempts to enter a voice mailbox. The INTUITY AUDIX system has a password time-out feature that allows callers three attempts in one call to correctly enter their password before they are automatically disconnected. You can also specify how many consecutive invalid attempts are allowed before a voice mailbox is locked.
- Deactivate unassigned voice mailboxes. When an employee leaves the company, close or reassign the voice mailbox.

- Do not create voice mailboxes before they are needed.
- Avoid or closely monitor the use of “guest” mailboxes (mailboxes without a physical extension that are loaned to outsiders for the duration of a project). If you need a guest mailbox, assign it when it is needed and deactivate or change its password immediately after it is no longer needed. Do not reassign a guest mailbox without changing the password.

Restrict outcalling

Outcalling uses the voice messaging ports. If mailbox security is broken, unauthorized persons can use outcalling to transfer messages at your expense. If you need outcalling, restrict it as far as possible to eliminate the possibilities for theft of services.

- Do not enable outcalling at all if you do not need it. Do not enable outcalling for any subscribers who do not need it.
- If outcalling is used only to ring in-house telephones that do not have message waiting lights, restrict the number of digits to the maximum length of extension.
- If possible, restrict outcalling to the local area (7 digits), or North American (10 digits).
- If outcalling must be done to pagers, use pagers that have individual DID numbers so that pager identification digits are not required and restrict any additional digits for call identification to the minimum possible.
- If a limited number of pagers are in use, consider putting the pager numbers on all unrestricted calling list so that outcalling can be effectively limited to only those numbers.

Detecting toll fraud

With SMDR activated for incoming calls, you can check the calls into your voice mail ports. A series of short holding times may indicate repeated attempts to enter voice mailbox passwords.

Review SMDR reports for the following symptoms of voice messaging abuse:

- Short holding times on calls where voice messaging is the originating endpoint or terminating endpoint
- Calls to international locations not normal for your business
- Calls to suspicious destinations
- Numerous calls to the same number
- Undefined account codes

NOTE:
The MERLIN LEGEND system only records the last extension on the call. Internal toll abusers transfer unauthorized calls to another extension before they disconnect so that the SMDR does not track the originating station. If the transfer is to your voice messaging system, it could give a false indication that your voice messaging system is the source of the toll fraud.

Protecting the MERLIN MAIL, MERLIN MAIL-ML, MERLIN MAIL R3, and MERLIN LEGEND Mail voice messaging systems

The MERLIN MAIL, MERLIN MAIL-ML, MERLIN MAIL R3, and MERLIN LEGEND Mail voice messaging systems provide automated attendant, call answer, and voice mail functionality. The Automated Attendant feature answers incoming calls and routes them to the appropriate department, person, or mailbox. The Call Answer feature provides call coverage to voice mailboxes. The Voice Mail feature provides a variety of voice messaging features.

Beginning with Release 3.1, ports assigned for use by voice messaging systems (including generic or integrated VMI ports) are now assigned outward restrictions by default. Also, FRL 0 and Disallowed List #7 are used. Prior to Release 3.1, FRL 3 is used. If a voice messaging system should be allowed to call out (for example, to send calls to a user's home office), the system manager must remove these restrictions. Provide outcalling only to mailboxes that have a business need for the feature.

NOTE:
Unauthorized persons concentrate their activities in two areas: they try to transfer out of the voice messaging system to gain access to an outgoing trunk and make long distance calls; or they try to locate unused or unprotected mailboxes and use them as dropoff points for their own messages.

Protecting automated attendant

Two areas of toll fraud risk are associated with the Automated Attendant feature. These are listed below.

- Pooled facility (line/trunk) access codes are translated to a selector code to allow remote access. If a hacker chooses this selector code, the hacker has immediate access.
- If the automated attendant prompts callers to use the host switch's remote call forwarding (RCF) to reach an outside telephone number, the system may be susceptible to toll fraud. An example of this application is a menu or submenu that says, "To reach our answering service, press 5," then transfers the caller to an external telephone number.

  Remote call forwarding can only be used securely when the central office provides "reliable disconnect." This is sometimes referred to as a forward disconnect or disconnect supervision. This guarantees that the central office will not return a dial tone after the called party hangs up. In many cases, the central office facility is a loop-start line/trunk which does not provide reliable disconnect. When loop-start lines/trunks are used, if the calling party stays on the line, the central office will return a dial tone at the conclusion of the call, enabling the caller to place another call as if it were being placed from your company.

Take the following preventative measures to limit the risk of unauthorized use of the Automated Attendant feature by hackers:

- Do not use automated attendant selector codes for automatic route selection (ARS) codes or pooled facility codes.
- Assign all unused automated attendant selector codes to zero, so that attempts to dial these will be routed to the system operator or General Mailbox.
- If RCF is required, coordinate with your Avaya Account Team or authorized dealer to verify the type of central office facility used for RCF. If a ground-start line/trunk, or a loop-start line/trunk and central office reliable disconnect can be ensured, then nothing else need be done.

  NOTE:
  In many cases these will be loop-start lines/trunks without reliable disconnect. The local telephone company will need to be involved to change the facilities used for RCF to ground start lines/trunks. Usually a charge applies for this change. Also, hardware and software changes may need to be made in the MERLIN LEGEND Communications System. The Automated Attendant feature merely accesses the RCF feature in the MERLIN LEGEND Communications System. Without these changes being made, this feature is highly susceptible to toll fraud. The same preventative measures must be taken if the RCF feature is active for MERLIN LEGEND Communications System extensions, whether or not accessed by an automated attendant menu.

Protecting passwords

For the MERLIN MAIL and MERLIN MAIL-ML voice messaging systems, passwords can be up to four digits. For the MERLIN MAIL R3 and MERLIN LEGEND Mail Voice Messaging System, passwords can be up to 15 digits. See "Administration / maintenance access" on page 4-4 and "General security measures" on page 4-8 for secure password guidelines. See Chapter 14 for information on how to change passwords.

Security tips

The MERLIN MAIL, MERLIN MAIL-ML, MERLIN MAIL R3, and MERLIN LEGEND Mail voice messaging systems, through proper administration, can help you reduce the risk of unauthorized persons gaining access to the network. However, phone numbers and authorization codes can be compromised when overheard in a public location, lost through theft of a wallet or purse containing access information, or when treated carelessly (writing codes on a piece of paper and improperly discarding them).

Hackers may also use a computer to dial an access code and then publish the information for other hackers. Substantial charges can accumulate quickly. It is your responsibility to take appropriate steps to implement the features properly, to evaluate and administer the various restriction levels, and to protect and carefully distribute access codes.

To reduce the risk of unauthorized access through your voice messaging system, also observe the following procedures:

- Monitor SMDR reports and/or Call Accounting System reports for outgoing calls that might be originated by internal and external abusers.
- If the MERLIN MAIL, MERLIN MAIL-ML, MERLIN MAIL R3, and/or MERLIN LEGEND Mail Voice Messaging System outcalling feature will be used, on the MERLIN LEGEND Communications System, outward restrict (FRL 0) all voice messaging system ports not used for outcalling. This denies access to facilities (lines/trunks).
    - The two-port systems (MERLIN MAIL Voice Messaging System, MERLIN MAIL-ML Voice Messaging System, MERLIN MAIL R3 Voice Messaging System, and MERLIN LEGEND Mail Voice Messaging System) use port 2 for outcalling; outward restrict port 1.
    - The four-port systems (MERLIN MAIL Voice Messaging System, MERLIN MAIL-ML Voice Messaging System, MERLIN MAIL R3 Voice Messaging System, and MERLIN LEGEND Mail Voice Messaging System) use port 4 for outcalling; outward restrict ports 1, 2, and 3.
    - The six-port systems (MERLIN MAIL R3 and MERLIN LEGEND Mail voice messaging systems) uses ports 5 and 6 for outcalling; outward restrict ports 1, 2, 3, and 4.
- Require employees who have voice mailboxes to use passwords to protect their mailboxes. For the MERLIN MAIL and MERLIN MAIL-ML voice messaging systems, passwords should be four digits long. For MERLIN MAIL R3 and MERLIN LEGEND Mail voice messaging systems, passwords should be at least six digits long.
- Require the system administrator and all voice mailbox owners to change their password from the default.
- Have employees use random sequence passwords.
- Impress upon employees the importance of keeping their passwords a secret.
- Encourage employees to change their passwords regularly.
- Use a secure password for the general mailbox.
- Reassign the system administrator’s mailbox/extension number from the default of 9997. Be certain to password-protect the new mailbox.
- Have the system administrator delete unneeded voice mailboxes from the system immediately.

- Set the maximum number of digits in an extension parameter appropriate to your dial plan. The voice messaging system will not perform transfers to extensions greater than that number.
- When possible, restrict the off-network capability of callers by using calling restrictions, FRLs, and disallowed list features.
- Outward restrict all MERLIN LEGEND voice mail port extensions not used for outcalling. This denies access to facilities (lines/trunks). Beginning with Release 3.1, this is the default. You should change this setting only after careful consideration.
- Create a disallowed list to disallow dialing 0, 70, 011, 809, 1809, 0809, 10, 9999, 411, 1411, 800, 888, 700, 900, 976, 550, 1800, 1888, 1700, 1500, 1900, 1976, 1550, 0800, 0888, 0700, 0500, 0900, 0976, and 0550. Assign all voice mail ports to this list. Avaya recommends using List 7 — the last disallowed list. This is an added layer of security, in case other restrictions are inadvertently removed.
- If outcalling is required by users of the voice messaging system:
  - Program an ARS FRL of 2 for voice mail port extension(s) used for outcalling.
  - If 800 and 888 numbers are used as outcalling destinations, remove 1800 and 1888 from Disallowed List Number 7.
  - If outcalling is allowed to long distance numbers, build an allowed list and assign it to the voice mail port extension(s) used for outcalling. On a two-port system, port 2 is used for outcalling. On a four-port system, port 4 is used for outcalling. On a 6-port system, ports 5 and 6 are used for outcalling. This list should contain the area code and first three digits of the local exchange telephone numbers to be allowed.
- When possible, block out-of-hours calling.
- Limit outcalling to persons on a need-to-have basis.
- Use the Transfer to Subscribers Only feature (MERLIN MAIL R3 Voice Messaging System only).
- Require network dialing for all extensions, including voice mail port extensions, to be through ARS using dial access code 9.
- Deny access to pooled facility codes by removing pool dial-out codes 70, 890-899, or any others on your system.
- Instruct employees to contact their system administrator immediately if any of the following occur:
  - Strange voice mail messages are received
  - Their personal greeting has been changed
  - They suspect their MERLIN MAIL Voice Messaging System mailbox is being used by someone else

Additional MERLIN MAIL R3 and MERLIN LEGEND Mail Voice Messaging System security features

The MERLIN MAIL R3 and MERLIN LEGEND Mail Voice Messaging System includes the following additional security features:

- The Transfer to Registered Subscribers Only setting of the Transfer Restrictions feature allows callers to be transferred only to users who have mailboxes in the system. Avaya strongly recommends using this feature to guard against toll fraud.
- Transfer-only mailboxes allow callers to reach extensions that need to be transfer destinations but do not need to receive messages. A maximum of 255 transfer-only mailboxes are available.
- The system administrator can set the minimum password length to any value from 0-15 digits. The default value is six digits. Every subscriber's mailbox password and the system administration password must be *at least* six digits.

  NOTE:
  A minimum password length of at least six digits is strongly recommended. The shorter the minimum password length, the more vulnerable your system is to abuse by unauthorized persons. Choose the largest acceptable minimum length in order to maximize the security of your system.

- The Security Violation Notification feature enables the system administrator to choose to be warned about possible mailbox break-in attempts. The system administrator can choose from the following options:
  - Mailbox Lock — Locks the subscriber's mailbox and sends a warning message to the mailbox owner's mailbox and the system administrator's mailbox.
  - Warning Message — Sends a warning message to the mailbox owner's mailbox and the system administrator's mailbox (factory setting).
  - No security notification (strongly discouraged).

  When a caller reaches the maximum number of unsuccessful login attempts, and Security Violation Notification is set to either Mailbox Lock or Warning Message, the system plays the message, "Login incorrect. Too many unsuccessful login attempts. The System Administrator has been notified. Good-bye." The system sends a warning message to the mailbox owner and to the system administrator.

  NOTE:
  The system administrator should use the most restrictive form of the feature that the business allows. Use the Mailbox Lock option unless this is too restrictive for your business. Use the Warning Message option otherwise. It is strongly discouraged to administer a system without security violation notification. The system administrator should investigate all warning messages received.

Messaging 2000 System

The Messaging 2000 (M2000) System provides voice mail services for the MERLIN Legend Communication System. The system is PC-based and uses the IBM OS-2 operating system. The system is connected to the Legend system via line-side VMI ports. These ports allow access to the voice mailboxes associated with each PBX subscriber.

Maintaining Message 2000 system security

The M2000 System includes security features. It is recommended that the end-user review the following security measures and implement them as appropriate.

- Preventing callers from transferring to extensions not assigned M2000 System mailboxes

  On some phone systems, callers can transfer to a system extension and then use that extension to access an outside line. This is most relevant for M2000 ports used for outcalls for networking or message notification to a beeper. By preventing callers from accessing system extensions not assigned M2000 system mailboxes, the risk of outside callers accessing an outside line may be reduced. Setting the following parameters on the Invalid Mailbox tab in System Setup can prevent callers from accessing non-assigned extensions.

  — Transfer Invalid Mailboxes During Hours

  — Transfer Invalid Mailboxes After Hours

  When these parameters are disabled, callers dialing an extension that has not been assigned an M2000 mailbox will hear, “Mailbox number is not valid. Please redial the number of the person you are calling.”

NOTE:
It is recommended that these parameters are set to disable transfer to invalid mailboxes.

- Impeding callers from accessing the quick assist maintenance mailbox

  When Quick Assist is run in Recover Mode, the system can automatically assign messages with invalid header information to a default mailbox. This allows the system manager to then copy the messages to the correct subscriber mailbox. The default for this maintenance mailbox is the last mailbox number available on the system. For example, on an M2000 system with 4-digit mailboxes, mailbox 9999 is used.

  Since it is easier for an outside caller attempting to gain unauthorized mailbox access to guess a mailbox number such as 9999, it is recommended that the system mailbox in which unattached messages will be placed, be specified explicitly. In addition, it is strongly recommended that this mailbox be assigned a long password that could not easily be guessed by an outside caller attempting to access the system.

When Quick Assist is run in Recover Mode from the Quick Assist icon in the Avaya folder, use the `Mailbox to Receive Unattached Messages` field on the Recover Files dialog box to specify a mailbox in which to place messages with invalid header information. When Quick Assist is run from the \CVR prompt or in batch mode as part of regular system maintenance, specify this mailbox by including the -M*n* parameter, where *n* indicates the number of the mailbox to be used, in the Quick Assist command line.

- Assigning randomly-generated passwords to M2000 System mailboxes

  During system setup, M2000 allows selection of the type of password assigned to new system mailboxes. You may assign the same default password to all new mailboxes, *or* not require a password, *or* have the M2000 system automatically assign a random password to each new mailbox. For security purposes, it is recommended that random password assignment be used. This makes it much more difficult for a caller to guess a mailbox's password. When random password assignment is used, the M2000 system displays the passwords assigned to the new mailboxes when they are created.

- Requiring passwords at least 1 digit longer than mailbox numbers

  The longer the passwords assigned to system mailboxes, the harder it is for a caller to guess them. The Minimum Length of Password parameter on the Subscriber parameters tab in the System Setup utility allows you to set the least number of digits required in a mailbox password. It is recommended that this parameter be set to at least 1 digit higher than the length of the system's mailbox numbers. For example, if the system uses 4-digit mailboxes, it is recommended that the Minimum Length of Password parameter be set to at least 5. Note that the length of this parameter must be set to balance system security against ease of use for the subscribers. Setting this parameter too high may make it difficult for system subscribers to remember their passwords.

- Requiring subscribers to regularly change their passwords

  The requirement that subscribers regularly change their passwords helps prevent outside callers from determining subscriber passwords and gaining unauthorized access to system mailboxes. The Days Before Forced Password Change parameter on the Subscriber tab in the System Setup utility should be used to specify the required internal before subscribers are required to change their mailbox passwords. When this parameter is enabled, subscribers must change their password the first time they log into their mailboxes and after the number of specified days expires before they can proceed to the main menu.

- Monitoring uninitialized mailboxes

  If the Days Before Forced Password Change parameter in the System Setup utility is disabled, subscribers are not required to change their passwords. This can make it easier for a caller to guess a subscriber's password, especially if a default password is used for all mailboxes instead of randomly assigned passwords for each mailbox.

The Uninitialized Mailbox report lists all mailboxes for which the password has not yet been changed from the initially assigned password. It is recommended that this report be regularly reviewed to determine which subscribers have not yet changed their passwords. Subscribers should be reminded that they should change their passwords regularly to prevent anyone but themselves from accessing their mailboxes. If it is found that many subscribers are not changing their passwords, the Days Before Forced Password Change parameter in the System Setup utility should be enabled to require them to regularly change their passwords.

- Using extended password security

  Extended password security requires subscribers to press the "#" key after entering their passwords to access their mailboxes. If subscribers do not press the "#" key, the system pauses before allowing mailbox access. The Enable Extended Password Security parameter on the Subscriber tab in the System Setup utility determines whether the system waits for the subscriber to press "#" or allows immediate mailbox access after successful password entry.

  This parameter helps prevent unauthorized users from determining the number of digits in M2000 system mailbox passwords.

NOTE:
It is recommended that this feature be enabled.

- Providing notification of unsuccessful mailbox login attempts

  The M2000 system can send voice notification to subscribers when one or more unsuccessful login attempts have been made to their mailboxes. This feature informs subscribers that someone may have attempted to gain unauthorized access to their mailboxes.

  The Failed Login Notification option on the Class of Service dialog box determines whether this feature is enabled. The Failed Login Notify option on the Subscriber Settings dialog box controls this feature by individual mailbox.

  When an unsuccessful login attempt occurs, it is recommended that the subscriber change their mailbox password immediately and notify the system manager of the attempted login.

NOTE:
It is recommended that this feature be enabled for all mailboxes.

- Locking subscriber mailboxes after unsuccessful login attempts

  The M2000 system can lock a mailbox when a caller attempting to log into the mailbox is disconnected after entering the incorrect password a specified number of times. A locked mailbox prevents any caller, including the subscriber, from logging into the mailbox until the system manager manually unlocks the mailbox.

The Mailbox Lock-Out Option on the Class of Service dialog box determines whether this feature is enabled. The Mailbox Lock-Out option on the Subscriber Settings dialog box controls this feature by individual mailbox. The Consecutive Login Failures Before Lock-Out parameter on the Subscriber Parameters tab in the System Setup utility determines the number of failed login attempts allowed before the mailbox is locked, if the Mailbox Lock-Out option is enabled for the mailbox.

NOTE:
It is recommended that this feature be enabled for all mailboxes.

- Monitoring failed login attempts

  The Login Failure report provides a list of all unsuccessful login attempts to system mailboxes. This report should be reviewed periodically to determine if there are a lot of failed login attempts to a particular mailbox and when the failed attempts occur. A high number of failed login attempts may indicate the mailbox owner requires additional training or that an unauthorized user is attempting to gain access to the mailbox.

- Having subscribers record their name prompts

  When subscribers record their name prompts, those prompts are voiced as confirmation to callers sending messages to system mailboxes. This ensures that messages will be sent to the correct mailboxes. If a name prompt is not recorded for a subscriber mailbox, only the mailbox number is voiced to callers sending messages to that mailbox.

- Deleting unused mailboxes immediately

  If a mailbox is no longer being used, it is recommended that the mailbox be immediately deleted from the M2000 system. This will prevent anyone from gaining unauthorized system access through the mailbox. If a mailbox is being reassigned to a new mailbox owner, it is strongly recommended that the mailbox be deleted, then re-created.

- Requiring callers to enter passwords to proceed in v-trees

  If v-trees are used to distribute or collect sensitive information, such as pricing data or customer data, it is strongly recommended that you use the Require Password to Proceed to Next Level option. This option requires callers to a v-tree to correctly enter a predefined password before they are allowed to proceed in the v-tree. You can use this option on multiple levels to protect individual options, or it can be used on the first level of the v-trees to limit access to the entire v-tree. This ensures that only authorized callers can gain access to the information provided in the v-tree.

- Securing the M2000 system PC

  It is imperative that the M2000 system PC be protected from unauthorized system management access. Unauthorized access to the M2000 system PC could result in system setup changes, loss of mailboxes and messages, and database corruption. The best way to prevent unauthorized system management access to the M2000 system PC is to store the PC in a secure area, such as a locked room.

  If the M2000 system PC cannot be stored in a secure area, the built-in PC security features, such as passwords, must be used to provide a degree of protection. Refer to your PC documentation for information on security features available on the PC.

  Note that before implementing security features on the PC, an Avaya technical support representative should be contacted to assure that these features will not disrupt M2000 system performance.

- Utilizing phone system security features

  Avaya communication systems have security features that allow one to help prevent unauthorized access to system ports. An Avaya system representative should be contacted to determine what security features are available for the Merlin Legend system and how to implement them.

- Using supervisor passwords to restrict system management access

  Access to M2000 system management features is password-protected. There are two levels of system manager passwords. Level 2 access allows a system manager to create/edit/delete mailboxes, access reports and system statistics, create and specify prompts, maintain network nodes, and create v-trees. Level 3 access allows a system manager to perform all level 2 tasks, to set system parameters using the System Setup module, configure greetings by port, modify classes of service, and configure multilingual M2000 systems.

  It is recommended that at least a 6-digit password be used for both the level 2 and level 3 passwords. The longer the level 2 and level 3 passwords, the more difficult it becomes for someone to guess them. It is also recommended that all supervisor passwords be changed on a regular basis to further protect against unauthorized system manager access.

- Using the Auto Logoff feature to restrict system management access

  The M2000 system's Auto Logoff feature allows one to specify the maximum amount of time a system management session can remain inactive before the M2000 system automatically logs out that user and terminates the session. This feature helps prevent unauthorized system manager access. To set the auto logoff, the number of minutes of inactivity allowed before logoff must be entered in the `Logoff In_____ Minutes` field on the Supervisor Password dialog box when logging into the system.

Security recommendations for remote access

Remote access to the system should be secured via the following guidelines:

- All remote access logins to the system must be administered to require the use of a secondary password
- The end-user must periodically/frequently change all secondary passwords. After changing the secondary passwords, the end-user should notify the appropriate Avaya support organization(s) that the passwords have been changed.
- The modem connection to the system should be disabled when it is not required for use by benefit personnel. This connection should be enabled only by the system administrator on an as-needed basis.

PARTNER II Communications System

The PARTNER II Communications System R3, and later releases, supports the PARTNER MAIL System. The PARTNER II Communications System R3.1 and later releases support the PARTNER MAIL System and the PARTNER MAIL VS System.

For information on these systems, see ''Protecting the PARTNER MAIL and PARTNER MAIL VS systems'' on page 7-55.

Also see ''Related documentation'' in the ''About this document'' section for a list of manuals on these products.

Protecting the PARTNER MAIL and PARTNER MAIL VS systems

The PARTNER MAIL and PARTNER MAIL VS systems provide automated attendant, call answer, and voice mail functionality. The Automated Attendant feature answers incoming calls and routes them to the appropriate department, person, or mailbox. The Call Answer feature provides call coverage to voice mailboxes.The Voice Mail feature provides a variety of voice messaging features.

Unauthorized persons try to locate unused or unprotected mailboxes and use them as dropoff points for their own messages, especially if inbound calls are free (for example, 800 inbound service).

Protecting passwords

For PARTNER MAIL Release 1 and all releases of PARTNER MAIL VS, passwords can be up to four digits. For PARTNER MAIL Release 3, passwords can be up to 15 digits in length. See ''Administration / maintenance access'' on page 4-4 and ''General security measures'' on page 4-8 for secure password guidelines. See Chapter 14 for information on how to change the passwords.

Security tips

- Monitor SMDR reports and/or Call Accounting System reports for outgoing calls that might be originated by internal and external abusers.
- For PARTNER MAIL System mailboxes, exercise caution when assigning a class of service (C)OS).
  - — Assign a COS that provides outcalling privileges (for PARTNER MAIL Release 1, assign 4, 5, 6, or 8; for PARTNER MAIL Release 3, assign 3,4, or 6) only to those mailboxes requiring these privileges.
  - — Assign COSs 1-6 (for PARTNER MAIL Release 1) or 1-4 and 20-23 (for PARTNER MAIL Release 3), transfer permitted, only to mailboxes for which the mailbox number is a real extension on the PARTNER II Communications System. Use COSs 7-9 (for PARTNER MAIL Release 1) or 5, 6, and 15-19 (for PARTNER MAIL Release 3), transfer not permitted, for all mailboxes for which there is no corresponding extension on the PARTNER II Communications System.
  - — If outcalling is not used, assign system mailboxes (90 to 98, and 9997 to 9999) to COS 7 or 9 (for PARTNER MAIL Release 1) or 5, 15-17,18, 19 (for PARTNER MAIL Release 3).
- Require employees who have voice mailboxes to use passwords to protect their mailboxes.
- Require the system administrator and all voice mailbox owners to change their password from the default.
- The system administrator can set the minimum password length to any value from 0-15 digits. The default value is six digits. Every subscriber's mailbox password and the system administration password must be *at least* six digits.

  NOTE:
  A minimum password length of at least six digits is strongly recommended. The shorter the minimum password length, the more vulnerable your system is to abuse by unauthorized persons. Choose the largest acceptable minimum length in order to maximize the security of your system.

- Instruct employees not to make a statement, in their recorded greeting, indicating that they will accept collect calls.
- Have the voice messaging system administrator delete unneeded voice mailboxes from the system immediately.
- The Security Violation Notification feature enables the system administrator to choose to be warned about possible mailbox break-in attempts. The system administrator can choose from the following options:

- Mailbox Lock — Locks the subscriber's mailbox and sends a warning message to the mailbox owner's mailbox and the system administrator's mailbox.
- Warning Message — Sends a warning message to the mailbox owner's mailbox and the system administrator's mailbox (factory setting).
- No Security Notification (strongly discouraged).

- Program the PARTNER II Communications System to:
  - — Block direct access to outgoing lines and force the use of account codes and/or authorization codes.
  - — Assign toll restrictions to individual's phones, especially in public areas.
  - — If you do not need to use the Outcalling feature of the PARTNER MAIL System, completely restrict the outward calling capability of its system ports by using inside calls only.
  - — If outcalling is required, assign outgoing call restriction local only with the appropriate toll call prefix to ports used for outcalling. Assign applicable allowed and disallowed number lists to the PARTNER MAIL System ports used for outcalling. Two-port PARTNER MAIL Systems use port 2 for outcalling. Four-port systems use port 4 for outcalling. Six-port systems use ports 5 and 6 for outcalling. Outward restrict all other ports.

PARTNER Plus Communications System

The PARTNER Plus Communications System R3.1 and later releases support the PARTNER MAIL System, and the PARTNER MAIL VS System.

For information on these systems, see ''Protecting the PARTNER MAIL and PARTNER MAIL VS systems'' on page 7-58.

Also see ''Related documentation'' in the ''About this document'' section for a list of manuals on these products.

Protecting the PARTNER MAIL and PARTNER MAIL VS systems

The PARTNER MAIL and PARTNER MAIL VS Systems provide automated attendant, call answer, and voice mail functionality. The Automated Attendant feature answers incoming calls and routes them to the appropriate department or person. The Call Answer feature provides call coverage to voice mailboxes. The voice mail feature provides a variety of voice messaging features.

Unauthorized persons try to locate unused or unprotected mailboxes and use them as dropoff points for their own messages, especially if inbound calls are free (for example, 800 inbound service).

Protecting passwords

For PARTNER MAIL Release 1 and all releases of PARTNER MAIL VS, passwords can be up to four digits. For PARTNER MAIL Release 3, passwords can be up to 15 digits in length. See "Administration / maintenance access" on page 4-4 and "General security measures" on page 4-8 for secure password guidelines. See Chapter 14 for information on how to change passwords in the PARTNER MAIL System and the PARTNER MAIL VS System.

Security tips

- Monitor SMDR reports and/or Call Accounting System reports for outgoing calls that might be originated by internal and external abusers.
- For PARTNER MAIL System mailboxes, exercise caution when assigning a class of service (COS).
  - — Assign a COS that provides outcalling privileges (for PARTNER MAIL Release 1 and PARTNER VS, assign 4, 5, 6, or 8; for PARTNER MAIL Release 3, assign 3,4, or 6) only to those mailboxes requiring these privileges.
  - — Assign COSs 1-6 (for PARTNER MAIL Release 1 and PARTNER VS) or 1-4 and 20-23 (for PARTNER MAIL Release 3), transfer permitted, only to mailboxes for which the mailbox number is a real extension on the PARTNER Plus Communications System. Use COSs 7-9 (for PARTNER MAIL Release 1 and PARTNER VS) or 5, 6, and 15-19 (for PARTNER MAIL Release 3), transfer not permitted, for all mailboxes for which there is no corresponding extension on the PARTNER Plus Communications System.
  - — If outcalling is not used, assign system mailboxes (90 to 98, and 9997 to 9999) to COS 7 or 9 (for PARTNER MAIL Release 1) or 5, 15-17,18, 19 (for PARTNER MAIL Release 3).
- Require employees who have voice mailboxes to use passwords to protect their mailboxes.

- Require the system administrator and all voice mailbox owners to change their password from the default.
- The System Administrator can set the minimum password length to any value from 0-15 digits. The default value is six digits. Every subscriber's mailbox password and the system administration password must be *at least* six digits.

  NOTE:
  A minimum password length of at least six digits is strongly recommended. The shorter the minimum password length, the more vulnerable your system is to abuse by unauthorized persons. Choose the largest acceptable minimum length in order to maximize the security of your system.

- Instruct employees not to make a statement, in their recorded greeting, indicating that they will accept collect calls.
- Have the voice messaging system administrator delete unneeded voice mailboxes from the system immediately.
- The Security Violation Notification feature enables the system administrator to choose to be warned about possible mailbox break-in attempts. The system administrator can choose from the following options:
  - — Mailbox Lock — Locks the subscriber's mailbox and sends a warning message to the mailbox owner's mailbox and the system administrator's mailbox.
  - — Warning Message — Sends a warning message to the mailbox owner's mailbox and the system administrator's mailbox (factory setting).
  - — No Security Notification (strongly discouraged).
- Program the PARTNER Plus Communications System to:
  - — Block direct access to outgoing lines and force the use of account codes and/or authorization codes.
  - — Assign toll restrictions to individual's phones, especially in public areas.
  - — If you do not need to use the Outcalling feature of the PARTNER MAIL System, completely restrict the outward calling capability of its system ports by using inside calls only.
  - — If outcalling is required, assign outgoing call restriction local only with the appropriate toll call prefix to ports used for outcalling. Assign applicable allowed and disallowed number lists to the PARTNER MAIL System ports used for outcalling. Two-port PARTNER MAIL Systems use port 2 for outcalling. Four-port systems use port 4 for outcalling. Six-port systems use ports 5 and 6 for outcalling. Outward restrict all other ports.

System 25

System 25 may be used with the AUDIX Voice Power System. (For information on this system, see ''Protecting the AUDIX Voice Power System'' on page 7-60.)

Also see ''Related documentation'' in the ''About this document'' section for a list of manuals on this product.

Follow the steps listed below for securing a voice processing system on the System 25.

- Outward restrict the voice processing ports whenever possible.
- Use the voice processing system's maximum extension length, valid extension range, and transfer to subscriber only feature, if available.
- Tightly control system administration access to these systems.
- Program the System 25 to:
  - — Block direct access to outgoing lines and force the use of account codes and/or authorization codes.
  - — Disallow trunk-to-trunk transfer unless it is required.

    NOTE:
    This parameter only applies to loop start lines.
- Do not administer the voice mail/coverage ports for remote call forwarding.
- Monitor SMDR reports and/or Call Accounting System reports for outgoing calls that might be originated by internal and external abusers.

Protecting the AUDIX Voice Power System

The AUDIX Voice Power System provides both automated attendant and voice mail functionality. The Automated Attendant feature answers incoming calls and routes them to the appropriate department or person. The Voice Mail feature provides call coverage to voice mailboxes along with a variety of voice messaging features.

Unauthorized persons concentrate their activities in two areas with the AUDIX Voice Power System:

- They try to transfer out of the AUDIX Voice Power System to gain access to an outgoing trunk and make long distance calls.
- They try to locate unused or unprotected mailboxes and use them as dropoff points for their own messages.

Protecting passwords

The AUDIX Voice Power System offers password protection to help restrict unauthorized access. Subscribers should use a maximum length password and should change it routinely. Passwords can be up to 9 digits. See ''Administration / maintenance access'' on page 4-4 and ''General security measures'' on page 4-8 for secure password guidelines. See Chapter 14 for information on how to change passwords.

Security tips

The following security measures assist you in managing features of the AUDIX Voice Power System to help prevent unauthorized use.

- Set `Transfer to Subscribers Only` to **yes**. This limits transfers to valid extensions.
- If you have Release 1.0 of the AUDIX Voice Power System, implement all appropriate security measures on the PBX side.
- Require employees who have voice mailboxes to use passwords to protect their mailboxes. See ''Administration / maintenance access'' on page 4-4 and ''General security measures'' on page 4-8 for secure password guidelines.
- Make sure subscribers change the default password the first time they log in to the AUDIX Voice Power System.
- Have the AUDIX Voice Power system administrator delete unneeded voice mailboxes from the system immediately.
- On the System Parameters screen, use the maximum number of digits allowable for extension entry (six). This will make it more difficult for criminals to guess the login and password combinations of your users.
- Set up automated attendant selection codes so that they do not permit outside line selection.
- Assign toll restriction levels to the AUDIX Voice Power System ports.
- If you do not need to use the Outcalling feature of the AUDIX Voice Power System, completely restrict the outward calling capability of the AUDIX Voice Power System ports.
- Disallow transfers to extensions not registered as valid subscribers.

WARNING:

Entering "#" transfers calls to the switch; that is, the transfer feature is always available and appropriate outgoing port restrictions must be in place to avoid toll fraud.

Security measures

The security measures described in this section do not apply if you are using Release 1.0 of the AUDIX Voice Power System. In this case, use PBX restrictions.

Transfer only to system subscribers

The AUDIX Voice Power System has the ability to allow callers to transfer only to mailbox subscribers. When an AUDIX Voice Power System caller requests a transfer using ***T** followed by an extension number, the AUDIX Voice Power System can compare the extension number entered with the valid extension numbers administered in the subscriber database.

If the extension is invalid, the transfer is denied and an error message is played to the caller. However, it does not prevent transfers from pre-administered dial strings in the automated attendant from accessing the outgoing facilities. Refer to Chapter 8 for procedures to restrict the automated attendant ports.

- On the AUDIX Voice Power System, within the System Parameter Administration screen, enter **yes** in the `Transfer to Subscribers Only` field.

  NOTE:
  You cannot use this security measure if calls are transferred to people in your company who are not AUDIX Voice Power System subscribers (see "Limit transfers out of the system" on page 7-32).

Limit transfers out of the system

When you need to allow transfers to people who are not AUDIX Voice Power System subscribers, you can add their extension numbers to the AUDIX Voice Power System subscriber database, but restrict access to their voice mailboxes.

- On the System Parameter Administration screen, enter **yes in** the `Transfer to Subscriber Only` field.
- On the Subscriber Administration screen, add each extension number for non-AUDIX Voice Power System subscribers.
- Enter **#** in the `Subscriber Password` field to prevent access to the corresponding voice mail.
- Enter **yes** in the `Does the subscriber have switch call coverage` field. On the switch side, do not specify the AUDIX Voice Power System extension as a coverage point for any of these added extensions.

NOTE:
Although these restricted voice mailboxes cannot receive call answer messages, they do receive broadcast messages and even may receive a misdirected message from another subscriber. To save storage space, you should periodically clean out these mailboxes by accessing the restricted mailboxes and deleting all messages.

NOTE:
On AUDIX Voice Power System 2.1.1, mailboxes can be set individually to "1 minute," reducing the clean-up required to service these mailboxes.

Automated attendant

8

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY communications systems, System 75, and System 85

Automated attendant is a service that connects to the PBX/communications system to help route calls to the appropriate extension. A menu of options allows callers to choose a predefined destination, such as a department, announcement, or an attendant, or a user-defined destination, such as an extension number.

Many automated attendant systems are vulnerable to toll fraud and are easy targets for toll hackers. Although there are some steps you can take to tighten the security of the automated attendant itself, **additional steps must be taken on the switch side to reduce the risk of toll fraud**.

Security tips

- Never allow a menu choice to transfer to an outgoing trunk without a specific destination.
- When a digit (1 through 9) is not a menu option, program it to transfer to an attendant, an announcement, a disconnect, or other intercept treatment.
- This tip does not apply to the AUDIX Voice Mail System:

  When 8 or 9 are feature access codes for the switch or media server, make sure the same numbers on the Automated Attendant menu are either translated to an extension or, if not a menu option, are programmed to transfer to an attendant, an announcement, a disconnect, or other intercept treatment.

- AUDIX Voice Mail System owners: use the Enhanced Call Transfer feature. Apply the appropriate security measures described in Chapter 7.

Tools that prevent unauthorized calls

You can help prevent unauthorized callers who enter the automated attendant system from obtaining an outgoing facility by using the security tools shown in Table 8-1.

Table 8-1. Automated attendant security tools

Security Tool	Switch	Page #
Enhanced call transfer (see ‘‘Protecting the AUDIX, DEFINITY AUDIX, and Avaya INTUITY Voice Mail Systems’’)	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 75 R1V3 Issue 2.0, System 85 R2V4	7-16
Facility restriction levels* (FRLs)	All	8-2
Station-to-trunk restrictions*	All	8-3
Class of restriction (COR)	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75	8-3
Class of service (COS)	DEFINITY G2 and System 85	8-4
Toll analysis	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, and System 85	8-5

Facility restriction levels

The switch treats all the PBX ports used by automated attendant systems as stations. Therefore, each automated attendant port can be assigned a COR with an associated FRL. FRLs provide for eight different levels of restrictions for AAR/ARS/WCR calls. FRLs are used in combination with calling permissions and routing patterns and/or preferences to determine where calls can be made. FRLs range from 0 to 7, with each number representing a different level of restriction (or no restrictions at all).

The FRL is used for the AAR/ARS/WCR feature to determine call access to an outgoing trunk group. Outgoing call routing is determined by a comparison of the FRLs in the AAR/ARS/WCR routing pattern to the FRL associated with the COR/COS of the call originator.

The higher the station FRL number, the greater the calling privileges. For example, if a station is not permitted to make outside calls, assign it an FRL value of 0. Then ensure that the FRLs on the trunk group preferences in the routing patterns are 1 or higher.

For example, when automated attendant ports are assigned to a COR with an FRL of 0, outside calls are disallowed. If that is too restrictive, the automated attendant ports can be assigned to a COR with an FRL that is low enough to limit calls to the calling area needed.

NOTE:
Stations that are outward restricted cannot use AAR/ARS/WCR trunks. Therefore, the FRL level does not matter since FRLs are not checked.

Station-to-trunk restrictions

Station-to-trunk restrictions can be assigned to disallow the automated attendant ports from dialing specific outside trunks. By implementing these restrictions, callers cannot transfer out of the Automated Attendant menu to an outside facility using trunk access codes.

For DEFINITY G2 and System 85, if TACs are necessary for certain users to allow direct dial access to specific facilities, such as tie trunks, use the Miscellaneous Trunk Restriction feature to deny access to others. For those stations and all trunk-originated calls, always use ARS/AAR/WCR for outside calling.

NOTE:
Allowing TAC access to tie trunks on your switch may give the caller access to the Trunk Verification feature on the next switch. If not properly administered, the caller may be able to dial 9 or the TACs in the other switch.

Class of restriction (System 75, DEFINITY G1, and G3, Communication Manager, MultiVantage Software, DEFINITY ECS)

Since automated attendant adjunct equipment is considered an extension to the switch, it should be assigned its own COR. Up to 64 CORs can be defined in the system. For DEFINITY G3rVi, G3i-Global, and G3V2, this has been increased to 96 CORs.

The CORs are assigned to stations and trunks to provide or prevent the ability to make specific types of calls, or calls to other specified CORs. For example, the automated attendant extension could be assigned to a COR that prohibits any outgoing calls.

Class of service

An automated attendant port can be assigned a COS. The following COS options relate to toll fraud prevention:

- Call Forward Off-Net: allows a user to call forward outside the switch to non-toll locations.
- Call Forward Follow Me: allows a user to forward calls outside the switch when other options are set.
- Miscellaneous Trunk Restrictions: restricts certain stations from calling certain trunk groups via dial access codes.
- Outward Restriction: restricts the user from placing calls over CO, FX, or WATS trunks using dial access codes to trunks. Outward restriction also restricts the user from placing calls via ARS/WCR. Use ARS/WCR with WCR toll restrictions instead.
- Toll Restriction: prevents users from placing toll calls over CO, FX, or WATS trunks using dial access codes to trunks. Use ARS/WCR with WCR toll restrictions instead.
- WCR Toll Restriction: restricts users from dialing the ARS or WCR Network I toll access code, or from completing a toll call over ARS/WCR.
- Terminal-to-Terminal Restrictions: restricts the user from placing or receiving any calls except from and to other stations on the switch.

In addition, the following COS options are available on System 85 and G2:

- Code Restriction Level: allows restriction of calls, by selected extension numbers, to areas defined by specific area codes and/or office codes. The switch returns intercept tone whenever the caller dials a code that is not allowed to the caller.
- DID Restriction: denies DID access to specified terminals; preventing these terminals from receiving private network inward dialed calls.
- Terminal-to-Terminal Only Calling Restriction: restricts the user from placing or receiving any calls except to and from other stations on the switch.
- Inward Restriction: prevents voice terminal users at specified extensions from receiving public network calls (DID and CO trunk calls).
- Manual Terminating Line Restriction: prevents voice terminal users at specified extensions from receiving calls other than direct or extended calls from a local attendant (or an attendant within the DCS network).
- Origination Restriction: prevents callers on specified extensions from directly accessing outgoing trunks to the public network.
- Outward Restriction: restricts the user from placing calls over the CO, FX, or WATS trunks using dial access codes to trunks. Outward restriction also restricts the user from placing calls via ARS/WCR. Use ARS/WCR with WCR toll restrictions instead.

- Termination Restriction: prevents voice terminal users on specified extensions from receiving calls, but not from originating calls.
- Toll Restriction: prevents users from placing toll calls over CO, FX, or WATS trunks using dial access codes to trunks. Use ARS/WCR with WCR toll restrictions instead.
- ARS/WCR Toll Restriction: restricts users from dialing the ARS or WCR Network I toll access code or from completing a toll call over ARS/WCR.
- FRL: establishes the user's access to AAR/ARS/WCR routes.

Toll analysis

When an automated attendant system transfers calls to locations outside the switch, you can use the Toll Analysis screen to limit call transfers to the numbers you identify. You can also specify toll calls to be assigned to a restricted call list so automated attendant callers cannot dial the numbers on the list. Call lists can be specified for CO/FX/WATS, TAC, and ARS calls, but not for tie TAC or AAR calls.

Security measures

The security measures described in this section use switch restrictions on the automated attendant ports. A disadvantage to this approach is that these restrictions are transparent to the caller; unaware of restrictions, determined toll hackers may keep trying to get through.

NOTE:
Even if you do not use the Remote Access feature, you should review the security measures found in Chapter 5. Some of the security measures described in that chapter can also be used to help secure your automated attendant system.

Limit transfers to internal destinations

You can restrict Automated Attendant menu options to transfer only to internal extension numbers or announcements by making the automated attendant ports outward-restricted.

WARNING:
Entering "#" transfers calls to the switch; that is, the transfer feature is always available in AVP Auto Attendant and appropriate outgoing port restrictions must be in place to avoid toll fraud.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- On the Class of Restriction screen, create an outward-restricted COR by entering **outward** in the `Calling Party Restriction` field.
- Assign the outward-restricted COR to the automated attendant port.
- Assign an FRL of 0 and enter **n** for all trunk group CORs.

For DEFINITY G2 and System 85:

- Use **PROC010 WORD3 FIELD19** to assign outward restriction to the automated attendant port COS. To secure the port, assign toll, ARS toll, and miscellaneous trunk group restrictions, and an FRL of 0.

Prevent calls to certain numbers

If some menu options transfer to locations off-premises, you can still protect the system from unauthorized calls. You can restrict calls to certain area codes and/or country codes, and even to specific telephone numbers.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1 and G3:

- On the Class of Restriction screen for the automated attendant ports, enter **y** in the `Restricted Call List` field.
- On the Toll Analysis screen, specify phone numbers you want to prevent automated attendant callers from dialing.

For DEFINITY G2:

- For DEFINITY G2.2, send disallowed destinations to action object “0.” Do not use **PROC314** to mark disallowed destinations with a higher FRL value. **PROC314 WORD1** assigns a Virtual Nodepoint Identifier to the restricted dial string. **PROC317 WORD2** maps the VNI to the pattern, and **PROC317 WORD2** shows the pattern preference, with the FRL in field 4.

  For earlier releases, use **PROC313** to enter disallowed destinations in the Unauthorized Call Control table.

Allow calling to specified numbers

A reverse strategy to preventing calls is to allow outbound calls only to certain numbers. For DEFINITY G1 and System 75, you must specify both the area code and the office code of the allowable numbers. For G3, you can specify the area code or telephone number of calls you allow.

For DEFINITY G1 and System 75:

- Use **change ars fnpa xxx** to display the ARS FNPA Table, where **xxx** is the NPA that will have some unrestricted exchanges.
- Route the NPA to an RHNPA table (for example, **r1**).

- Use **change rnhpa r1: xxx** to route unrestricted exchanges to a pattern choice with an FRL equal to or lower than the originating FRL of the voice mail ports.
- If the unrestricted exchanges are in the Home NPA, and the Home NPA routes to **h** on the FNPA Table, use **change hnpa xxx** to route unrestricted exchanges to a pattern with a low FRL.

NOTE:
If assigning a low FRL to a pattern preference conflicts with requirements for other callers (it allows calls that should not be allowed), use ARS partitioning to establish separate FNPA/HNPA/RHNPA tables for the voice mail ports.

For DEFINITY G2 and System 85:

- Use **PROC311 WORD2** to establish 6-digit translation tables for foreign NPAs, and assign up to 10 different routing designators to each foreign NPA (area code).
- Use **PROC311 WORD3** to map restricted and unrestricted exchanges to different routing designators.
- If the unrestricted toll exchanges are in the Home NPA, use **PROC311 WORD1** to map them to a routing designator.
- If the Tenant Services feature is used, use **PROC314 WORD1** to map routing designators to patterns. If the Tenant Services feature is not used, the pattern number will be the same as the routing designator number.
- Use **PROC309 WORD3** to define the restricted and unrestricted patterns.

For DEFINITY G2.2:

- Use **PROC314 WORD1** to assign a Virtual Nodepoint Identifier (VNI) to the unrestricted dial string. Map the VNI to a routing pattern in **PROC317 WORD2**, and assign a low FRL to the pattern in **PROC318 WORD1**. If you permit only certain numbers, consider using Network 3, which contains only those numbers.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3:

- Use **change ars analysis** to display the ARS Analysis screen.
- Enter the area codes or telephone numbers that you want to allow and assign an available routing pattern to each of them.
- Use **change route-pattern** to give the pattern preference an FRL that is equal to or lower than the FRL of the voice mail ports.

Detecting automated attendant toll fraud

Table 8-2 shows the reports that help determine if your automated attendant system is being used for fraudulent purposes.

Table 8-2. Automated attendant monitoring techniques

Monitoring Technique	Switch	Page #
Call detail recording (SMDR)	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 75, System 85	8-9
Traffic measurements and performance	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 75, System 85	8-10
Automatic circuit assurance	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 75, System 85	8-11
Busy verification	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 75, System 85	8-12
Call Traffic report	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, G3, System 75, System 85	8-10
Trunk Group report	Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, System 75	8-10
AUDIX Voice Mail System traffic reports	Any with the AUDIX Voice Mail or AUDIX Voice Power Systems	8-13
AUDIX Voice Mail System call detail recording	Any with AUDIX Voice Mail System R1V5 and later with digital networking	8-13

Call detail recording / station message detail recording

With CDR activated for the incoming trunk groups, you can monitor the number of calls into your automated attendant ports. See also "Security violation notification (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3)" on page 5-59.

NOTE:
Most call accounting packages discard this valuable security information. If you are using a call accounting package, check to see if the information you need can be stored by making adjustments in the software. If it cannot be stored, be sure to check the raw data supplied by the CDR.

Review CDR for the following symptoms of automated attendant abuse:

- Short holding times on any trunk group where automated attendant is the originating endpoint or terminating endpoint
- Calls to international locations not normal for your business
- Calls to suspicious destinations
- Numerous calls to the same number
- Undefined account codes

NOTE:
For DEFINITY G2 and System 85, since the CDR only records the last extension on the call, internal toll abusers transfer unauthorized calls to another extension before they disconnect so that the CDR does not track the originating station. If the transfer is to your automated attendant system, it could give a false indication that your automated attendant system is the source of the toll fraud.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Display the Features-Related System Parameters screen by using **change system-parameters features** (G1 and System 75 only) or **change system-parameters cdr** (G3 and later).
- Administer the appropriate format to collect the most information. The format depends on the capabilities of your CDR analyzing/recording device.
- Use **change trunk-group** to display the Trunk Group screen.
- Enter **y** in the `SMDR/CDR Reports` field.

For DEFINITY G2:

- Use **PROC275 WORD1 FIELD14** to turn on CDR for incoming calls.
- Use **PROC101 WORD1 FIELD8** to specify the trunk groups.

Call Traffic report

This report provides hourly port usage data and counts the number of calls originated by each port. By tracking normal traffic patterns, you can respond quickly if an unusually high volume of calls begins to appear, especially after business hours or during weekends, which might indicate hacker activity.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, traffic data reports are maintained for the last hour and the peak hour. For DEFINITY G2 and System 85, traffic data is available via Monitor I which can store the data and analyze it over specified periods.

Trunk Group report

This report tracks call traffic on trunk groups at hourly intervals. Since trunk traffic is fairly predictable, you can easily establish, over time, what is normal usage for each trunk group. Use this report to watch for abnormal traffic patterns, such as unusually high off-hour loading.

SAT, Manager I, and G3-MT reporting

Traffic reporting capabilities are built-in and are obtained through the System Access Terminal (SAT), Manager I, and G3-MT terminals. These programs track and record the usage of hardware and software features. The measurements include peg counts (number of times accessed) and call seconds of usage. Traffic measurements are maintained constantly and are available on demand. However, reports are not archived and should therefore be printed to monitor a history of traffic patterns.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- To record traffic measurements:
  - Use **change trunk-group** to display the Trunk Group screen.
  - In the `Measured` field, enter **both** if you have BCMS and CMS, **internal** if you have only BCMS, or **external** if you have only CMS.
- To review the traffic measurements, use **list measurements** followed by one of the measurement types (**trunk-groups**, **call-rate**, **call-summary**, or **outage-trunk**) and the timeframe (**yesterday-peak**, **today-peak**, or **last-hour**).
- To review performance, use **list performance** followed by one of the performance types (summary or **trunk-group**) and the timeframe (**yesterday** or **today**).

ARS measurement selection

The ARS Measurement Selection feature can monitor up to 20 routing patterns (25 for G3 and later for traffic flow and usage.

For Communication Manager and MultiVantage™ Software:

- Use **change meas-selection route-pattern** to choose the routing patterns you want to track.
- Use **list measurements route-pattern** followed by the timeframe (**yesterday**, **today**, or **last-hour**) to review the measurements.

For DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change ars meas-selection** to choose the routing patterns you want to track.
- Use **list measurements route-pattern** followed by the timeframe (**yesterday**, **today**, or **last-hour**) to review the measurements.

For DEFINITY G2, use Monitor I to perform the same function.

Automatic circuit assurance

This monitoring technique detects a number of short holding time calls or a single long holding time call, both of which may indicate hacker activity. Long holding times on trunk-to-trunk calls can be a warning sign. The ACA feature allows you to establish time limit thresholds defining what is considered a short holding time and a long holding time. When a violation occurs, a designated station is visually notified.

When a notification occurs, determine if the call is still active. If toll fraud is suspected (for example, **aca-short** or **aca-long** is displayed on the designated phone), use the busy verification feature (see "Busy verification" on page 8-12) to monitor the call in progress.

With remote access, when hacker activity is present, there is usually a burst of short holding times as the hacker attempts to break the barrier code or authorization code protection, or long holding time calls after the hacker is successful. An ACA alarm on a remote access trunk should be considered a potential threat and investigated immediately. If the call is answered by an automated attendant, a hacker may be attempting to gain access to the system facilities using TACs.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change system-parameters features** to display the Features-Related System Parameters screen.
- Enter **y** in the `Automatic Circuit Assurance (ACA) Enabled` field.

- Enter **local**, **primary**, or **remote** in the `ACA Referral Calls` field. If **primary** is selected, calls can be received from other switches. **Remote** applies if the PBX being administered is a DCS node, perhaps unattended, that wants ACA referral calls to an extension or console at another DCS node.
- Complete the following fields as well: `ACA Referral Destination`, `ACA Short Holding Time Originating Extension`, `ACA Long Holding Time Originating Extension`, and `ACA Remote PBX Identification`.

  NOTE:
  The `ACA Remote PBX Identification` field only appears if the `ACA Referral Calls` field is set to **remote**.

- Assign an **aca referra**l button on that station (or the attendant station).
- Use **change trunk group** to display the Trunk Group screen.
- Enter **y** in the `ACA Assignment` field.
- Establish short and long holding times. The defaults are 10 seconds (short holding time) and one hour (long holding time).
- To review, use **list measurements aca**.
- Administer an **aca** button on the console or display station to which the referral will be sent.

For DEFINITY G2 and System 85:

- Use **PROC285 WORD1 FIELD5** and **PROC286 WORD1 FIELD1** to enable ACA system-wide.
- Use **PROC120 WORD1** to set ACA call limits and number of calls threshold.
- Choose the appropriate option:
  - To send the alarms and/or reports to an attendant, use **PROC286 WORD1 FIELD3**.

Busy verification

When toll fraud is suspected, you can interrupt the call on a specified trunk group and monitor the call in progress. Callers will hear a long tone to indicate the call is being monitored.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75:

- Use **change station** to display the Station screen for the station that will be assigned the Busy Verification button.
- In the `Feature Button Assignment` field, enter **verify**.

- To activate the feature, press the **Verify** button and then enter the trunk access code and member number to be monitored.

For DEFINITY G2 and System 85:

- Administer a Busy Verification button on the attendant console.
- To activate the feature, press the button and enter the trunk access code and the member number.

Call Traffic report

This report provides hourly port usage data and counts the number of calls originated by each port. By tracking normal traffic patterns, you can respond quickly if an unusually high volume of calls begins to appear, especially after business hours or during weekends, which might indicate hacker activity.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, traffic data reports are maintained for the last hour and the peak hour. For G2 and System 85, traffic data is available via Monitor I which can store the data and analyze it over specified periods.

Trunk Group report

This report tracks call traffic on trunk groups at hourly intervals. Since trunk traffic is fairly predictable, you can easily establish, over time, what is normal usage for each trunk group. Use this report to watch for abnormal traffic patterns, such as unusually high off-hour loading.

Traffic reports

Both the AUDIX Voice Mail System and the AUDIX Voice Power System track traffic data over various timespans. Reviewing these reports on a regular basis helps to establish traffic trends. If increased activity or unusual usage patterns occur, they can be investigated immediately. Beginning with AUDIX Voice Mail System R1V2, the AUDIX Data Acquisition Package (ADAP) uses a PC to provide extended storage and analysis capabilities for the traffic data.

Call detail recording

For AUDIX Voice Mail System R1V5 and later, this optional feature provides a detailed view of the activity associated with each voice mail session, outgoing calls, and system-wide activity.

Voice session record

A voice session begins whenever a caller attempts to log into the AUDIX Voice Mail System, is redirected to the AUDIX Voice Mail System for call answering, enters *R or **R, transfers from one automated attendant to another automated attendant (nested), or is transferred by the Enhanced Automated Attendant feature.

The record reveals the routing of the call, including the caller (if internal), recipient, port, community, mail IDs (corresponds to the AUDIX Voice Mail System subscriber's extension number input during a login or as input by the calling party), the time and duration of the call, the type of session (voice mail, call answer, guest password, or automated attendant), the message activity, and number of login attempts.

Also reported is the session termination method. Each possible termination method is assigned a value as shown in Table 8-3. This information can be downloaded to a PC using ADAP to be available on demand or at scheduled intervals.

Table 8-3. AUDIX Voice Mail System session termination values

Value	Reason for Session Termination
01	Caller transferred out of the AUDIX Voice Mail System
02	Caller disconnected established call
03	Caller abandoned call before the AUDIX Voice Mail System answered
04	Caller entered **X
05	Caller entered *R from call answer
06	Caller entered **R from voice mail
07	The AUDIX Voice Mail System terminated the call due to a system problem
08	The AUDIX Voice Mail System terminated the call due to a caller problem (for example, full mailbox timeout)
09	The AUDIX Voice Mail System terminated a call originated by another AUDIX Voice Mail System
10	Transfer from an automated attendant to another automated attendant mailbox
11	Transfer from an automated attendant to a call answer mailbox
12	Transfer from an automated attendant to a mailbox with guest greeting

Outgoing voice call detail record

An outgoing call record is also created for every outbound call that is originated by the AUDIX Voice Mail System via a voice port. This includes call transfers, outcalling, and message waiting activation and/or deactivation via access codes. A record is also created for call attempts for the Message Delivery feature.

The outgoing voice call detail record supplies the date the call was placed, the time, the AUDIX Voice Mail System port number used for the call, the duration of the call, the voice mailbox id, the number dialed, and the call type. These values are shown in Table 8-4.

Table 8-4. Outgoing Call Type Values

Value	Outgoing Call Type
10	Transfer from voice mail with *T or *0
11	Transfer from voice mail via return call
12	Transfer from call answer with *T, *0 or 0
13	Transfer from automated attendant via menu selection
14	Transfer from automated attendant via extension specification
15	Transfer from automated attendant via time out
16	Transfer from automated attendant via *T
17	Transfer from bulletin board via *T, *0 or 0
20	Outcalling for any message
21	Outcalling for priority message
30	Message waiting activation/deactivation
40	Call delivery

Unsuccessful call transfer attempts can result in multiple records being created for a single session. Review these records regularly for the following signs of hacker activity:

- Failed login attempts
- Multiple call transfers for a single session
- Numerous outbound calls from the same voice mailbox
- Calls to strange places
- Heavy volume of Transfer Out of AUDIX Voice Mail System calls

The AUDIX Voice Power System tracks traffic data over various timespans. Reviewing these reports on a regular basis helps to establish traffic trends. If increased activity or unusual usage patterns occur, they can be investigated immediately.

Protecting automated attendant on the AUDIX Voice Mail System

This section discusses security measures implemented directly on the AUDIX Voice Mail System automated attendant.

Disallow outside calls

The AUDIX Voice Mail System integrated with Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G2, and G3, System 85 R2V4, and System 75 R1V3 (Issue 2.0) and later, provide a feature called Enhanced Call Transfer that only transfers AUDIX Voice Mail System calls to valid PBX extension numbers. With this feature, when an automated attendant caller enters an extension as a menu choice, the AUDIX Voice Mail System checks the digits to see if they match the extension length before sending the digits to the switch.

CAUTION:

If trunk access code (TAC) calls are permitted, they may be accepted as a valid extension number. Even with the Enhanced Call Transfer feature activated, toll hackers can choose a menu option that allows an extension number, and then enter a TAC to get an outside line.

Another advantage of this feature is that when a toll hacker tries to enter an unauthorized number, the AUDIX Voice Mail System error message notifies the hacker that this automated attendant system is secure.

For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G1 and G3:

1. On the AUDIX Voice Mail System system:appearance screen, enter **y** in the `Call Transfer Out of AUDIX` field.
2. Enter **y** in the `Enhanced Call Transfer` field.
3. Press **Change/Run**.
4. On the AUDIX Voice Mail System maintenance:audits:fp screen, tab to the `Service Dispatcher` field and enter **x**.
5. Tab to the `Start` field and enter **x**.
6. Press **Change/Run**.
7. On the switch, use **change listed-directory-numbers** to add a valid extension for your attendant.

For DEFINITY G2 and System 85:

1. On the AUDIX Voice Mail System system:appearance screen, enter **y** in the `Call Transfer Out of AUDIX` field.
2. Enter **y** in the `Enhanced Call Transfer` field.
3. Press **Change/Run**.
4. On the AUDIX Voice Mail System maintenance:audits:fp screen, tab to the `Service Dispatcher` field and enter **x**.
5. Tab to the `Start` field and enter **x**.
6. Press **Change/Run**.
7. On the switch, use **PROC204** to assign a Listed Directory Number for the attendant console.

After you activate Enhanced Call Transfer, test it by following the steps below:

1. Dial into your AUDIX Voice Mail System automated attendant.
2. Press the menu choice to transfer to an extension.
3. Enter an invalid extension number followed by #.

   The failed announcement should play, followed by a prompt for another extension number.
4. Enter a valid extension number followed by #.

   You should notice that the call transfers much faster than with Basic Call Transfer.

NOTE:
In order to test correctly, you must first dial outside of the system, then dial back in on the number assigned to the automated attendant. A station to station connection will not test correctly.

Protecting automated attendant on the AUDIX Voice Power System

The AUDIX Voice Power System provides automated attendant functionality. Follow all recommendations for protecting the switch in Chapter 6, as well as those for protecting the AUDIX Voice Power System for the switch in Chapter 7. In addition, make sure that automated attendant selector codes do not permit outside line selection.

Protecting automated attendant on the CONVERSANT Voice Information System

The CONVERSANT Voice Information System provides automated attendant functionality. Follow all recommendations for protecting the switch in Chapter 6, as well as those for protecting the CONVERSANT Voice Information System for the switch in Chapter 7. In addition, make sure that automated attendant selector codes do not permit outside line selection.

Protecting automated attendant on the DEFINITY AUDIX System

The DEFINITY AUDIX System provides automated attendant functionality. Follow all recommendations for protecting the switch in Chapter 6, as well as those for protecting the DEFINITY AUDIX System for the switch in Chapter 7. In addition, make sure that automated attendant selector codes do not permit outside line selection.

Protecting automated attendant on the Avaya INTUITY System

The Avaya INTUITY System provides automated attendant functionality. Follow all recommendations for protecting the switch in Chapter 6, as well as those for protecting the Avaya INTUITY System for the switch in Chapter 7. In addition, make sure that automated attendant selector codes do not permit outside line selection.

MERLIN II Communications System R3

MERLIN MAIL Voice Messaging System

The MERLIN MAIL Voice Messaging System provides the Automated Attendant feature. Follow all recommendations for protecting the MERLIN MAIL Voice Messaging System in Chapter 7. In addition, make sure that automated attendant selector codes do not permit outside line selection.

MERLIN Attendant

To help secure MERLIN Attendant against toll fraud, do the following:

- Administer the lowest valid extension number (Lowest Extension) and the highest valid extension number (Highest Extension) for the range of valid extensions. Transfer attempts to extensions that fall outside the range will be disallowed.
- Administer the maximum number of digits in the extension to match the dial plan.
- Change the default system password.

MERLIN LEGEND Communications System

AUDIX Voice Power System

The MERLIN LEGEND Communications System supports the AUDIX Voice Power System, which provides automated attendant functionality. Follow all recommendations for protecting the MERLIN LEGEND Communications System switch in Chapter 6, as well as those for protecting the AUDIX Voice Power System for the MERLIN LEGEND Communications System in Chapter 7. In addition, make sure that automated attendant selector codes do not permit outside line selection.

The AUDIX Voice Power System tracks traffic data over various timespans. Reviewing these reports on a regular basis helps to establish traffic trends. If increased activity or unusual usage patterns occur, they can be investigated immediately.

MERLIN MAIL, MERLIN MAIL-ML, and MERLIN MAIL R3 voice messaging systems

The MERLIN MAIL, MERLIN MAIL-ML, and MERLIN MAIL R3 voice messaging systems provide the automated attendant feature. Follow all recommendations for protecting these systems in Chapter 7. In addition, make sure that automated attendant selector codes do not permit outside line selection.

MERLIN Attendant

To help secure MERLIN Attendant against toll fraud, do the following:

- Administer the lowest valid extension number (Lowest Extension) and the highest valid extension number (Highest Extension) for the range of valid extensions. Transfer attempts to extensions that fall outside the range will be disallowed.
- Administer the maximum number of digits in the extension to match the dial plan.
- Change the default system password.

PARTNER II Communications System

The PARTNER II Communications System supports the PARTNER MAIL System, and the PARTNER MAIL VS System.

PARTNER MAIL and PARTNER MAIL VS systems

The PARTNER MAIL and PARTNER MAIL VS Systems provide the Automated Attendant feature. Follow all recommendations for protecting these systems in Chapter 7.

PARTNER Attendant

To help secure PARTNER Attendant against toll fraud, do the following:

- Administer the lowest valid extension number (Lowest Extension) and the highest valid extension number (Highest Extension) for the range of valid extensions. Transfer attempts to extensions that fall outside the range will be disallowed.
- Administer the maximum number of digits in the extension to match the dial plan.
- Change the default system password.

PARTNER Plus Communications System

The PARTNER Plus Communications System R3.1 and later releases, supports the PARTNER MAIL System, and the PARTNER MAIL VS System.

PARTNER MAIL and PARTNER MAIL VS systems

The PARTNER MAIL and PARTNER MAIL VS Systems provide the Automated Attendant feature. Follow all recommendations for protecting these systems in Chapter 7.

PARTNER Attendant

To help secure PARTNER Attendant against toll fraud, do the following:

- Administer the lowest valid extension number (Lowest Extension) and the highest valid extension number (Highest Extension) for the range of valid extensions. Transfer attempts to extensions that fall outside the range will be disallowed.
- Administer the maximum number of digits in the extension to match the dial plan.
- Change the default system password.

System 25

AUDIX Voice Power System

System 25 supports the AUDIX Voice Power System, which provides automated attendant functionality. Follow all recommendations for protecting the System 25 switch in Chapter 6, as well as those for protecting the AUDIX Voice Power System for System 25 in Chapter 7. In addition, make sure that automated attendant selector codes do not permit outside line selection.

The AUDIX Voice Power System tracks traffic data over various timespans. Reviewing these reports on a regular basis helps to establish traffic trends. If increased activity or unusual usage patterns occur, they can be investigated immediately.

Other products and services

9

NOTE:
Unless specifically stated otherwise, references in this document to "G3Vx and later" include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

This chapter contains security information for Avaya products other than PBXs and adjuncts that have become available since Issue 2 of this handbook. For information on the Avaya INTUITY System and the PARTNER MAIL VS System, see Chapter 7.

Call Management System (R3V4)

Call Management System (R3V4) is an MIS system for call centers that provides real time and historical data about the status and performance of a customer's call including information about agents, trunks, trunk groups, splits/skills, busy hours, forecasts, and so on. The application currently resides on personal computer platforms as an adjunct to the Avaya Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY communications systems.

Security could be breached if a customer adds modems to the platform for supervisor access from remote locations. If access to UNIX is allowed, and the modems and station lines from the PBX are not secured, it would be possible to make data calls to other computers via the platform. If the customer has modem access to CMS, then the possibility for toll fraud exists if a hacker can get into the switch from CMS.

Security tips

The following considerations are for the CMS administrator.

- When setting up the ports, modems should be defined in UNIX (using the FACE administration tool) for inbound access only.
- If station lines are used for the modems, the COS or COR should be set to disallow outbound dialing capabilities.

- Switchhook flash and distinctive audible alert should be set to **no** on the Station screens.
- Remote users should not have access to UNIX via the CMS application. Restrict access by means of the User Permissions feature of CMS.

For additional information on administering CMS, refer to the most recent release of the following documents:

- *Avaya™ Call Management System Administration*
- *Avaya™ CMS Software Installation, Maintenance, and Troubleshooting Guide*
- Any of the hardware component planning, installation, maintenance, and/or quick reference information listed under the Call Management System (CMS) product documentation heading on http://www.avaya.com/support.

For switch restrictions, consult the applicable chapter in this guide as well as the applicable switch administration manual for the pertinent PBX.

CMS helplines

If an installation problem that requires assistance arises, Avaya technicians or the customer may call the appropriate number:

- **Customer number: 1 800 344-9670**

  The problem will be reported, and a trouble ticket will be generated so that the problem can be escalated through the services organization. The customer will be prompted to identify the type of problem (for example, ACD, hardware, CMS R3V4, etc.). The customer will then be connected to the appropriate service organization.

- **Technician number: 1 800 248-1234**

  The technician should provide the TSC personnel with the customer's name, the password for the root login ID on the Sun workstation, the phone number of the dial-in port, and a description of the problem. If the TSC engineers cannot resolve the problem, they will escalate it to the customer support organization for Avaya.

For international support, contact your Avaya representative or distributor for more information.

CallMaster PC

CallMaster PC, a software application used with Communication Manager, MultiVantage™ Software, and DEFINITY ECS, gives call center agents and supervisors the ability to access and control their CallMaster or CallMaster II telephone sets through a Microsoft Windows™-compatible PC. If call center employees use remote access software such as Norton pcANYWHERE® software or Microcom's Carbon Copy Plus™ for Windows, or similar software that allows applications to run on their PC from a remote location, their system might be susceptible to toll fraud, as follows:

An agent dials in from home, provides a password (if required), and may then use any software, including CallMaster PC, on the remote computer. If a hacker can crack the password for the remote software, he or she can access the remote computer, run the victim's CallMaster PC on it, and set up a conference call between the hacker's phone and another phone, at the company's expense.

Security tips

Warn customers with remote access software that they must administer the software's password protection to prevent unauthorized access to the computer, and they should change the password frequently.

For additional information, refer to the CALLMASTER PC product documentation (shipped with the unit; not available from the Publication Center), and the documentation for any remote access software you use.

Multipoint Conferencing Unit (MCU)/Conference Reservation and Control System (CRCS)

The MCU has a DEFINITY ECS/MultiVantage™/Communication Manager-based architecture. The primary component of the MCU is the Multimedia Server Module (MSM), which is similar to the most basic version of the DEFINITY ECS Processor Port Network (PPN). MSM security concerns are similar to those for the Communication Manager, MultiVantage™ Software, and DEFINITY ECS (including, for example, trunking, COR, and COS). Therefore, refer to the appropriate sections in this document regarding Communication Manager, MultiVantage™ Software, and DEFINITY ECS for more information on MSM security.

The MCU system includes two possible adjuncts: the Expansion Services Module (ESM) and the Conference Reservation and Control System (CRCS).

The ESM is a data conferencing module that communicates with the MSM. The ESM does not provide network access and is therefore not a source of toll fraud; however, the ESM requires proper password management on the part of system administrators and users to preserve the functionality of the ESM.

CRCS is the automated conference reservation and control system for the MCU product. CRCS is in part an extension of the DEFINITY SAT; therefore, once CRCS is installed, CRCS server and client logins should be set with passwords immediately. Also, ensure that CRCS is installed in a secure area or room that can be locked.

PassageWay Telephony Services for NetWare and Windows NT

NOTE:
The following information applies to PassageWay Telephony Services connected to either the Communication Manager, MultiVantage™ Software, DEFINITY ECS or MERLIN LEGEND driver.

The PassageWay Telephony Services product provides computer/telephony integration for applications running in a Novell NetWare or a Microsoft Windows NT Local Area Network (LAN) environment. These applications may be able to control phones on a PBX, monitor phones, monitor calls passing through ACD splits and VDNs, and invoke PBX features on behalf of station set users. Different switches provide different capabilities to applications.

The major components of the PassageWay Telephony Services product are as follows:

- PBX driver: Interfaces the other product components in this list to a specific vendor's PBX
- Telephony Server Main Module (**TSERVER NLM**: for NetWare or **TSERV.EXE**: for Windows NT): Enforces license restrictions, provides a security database to manage user permissions, and provides connectivity between client applications and PBX drivers
- Administration Application: Administers the Security Database, a Windows PC application that runs on a LAN client PC.
- Telephony Services API (TSAPI): Provides a programming interface for applications. Client libraries make the programming interface available in application environments, which may include Windows 3.1 and 3.11, Windows for Workgroups, Win 95, Windows NT, Windows 2000, Windows Me, Windows XP, OS/2®, HP-UX, Macintosh, Unixware, and Netware.

The PassageWay Telephony Services product may be vulnerable to toll fraud if the Telephony Server is not configured and administered properly. For example, even if the switch provides restrictions, the PassageWay Telephony Server administration may allow an end user to monitor and control phones other than their own.

Security tips

The following tips are for the PassageWay Telephony Server administrator.

When the product is installed, do the following:

For Netware only:

- Use the NetWare Administrator feature (NetWare 4.10 and 4.11) or SYSCON utility (NetWare 3.12) to set the appropriate login and password restrictions (for example, require users to have passwords with a minimum length of 7 characters, enable password aging, and so forth).
- Use the NetWare Administrator feature (NetWare 4.10 and 4.11) or SYSCON utility (NetWare 3.12) to enable the Intruder Detection feature and to lock accounts after several invalid login attempts have been made.
- Enable the “Restrict users to Home Worktop” feature.

For Windows NT only:

- Disable the Extended Worktop Access feature.
- Take full advantage of Windows NT user manager administration, including password options.
- Take full advantage of Windows NT event log (for example, for monitoring failed login attempts).

- Educate administrative personnel about the capabilities of the PassageWay Telephony Server. Administrators must understand that the programming interface provides “third party control” capabilities. These capabilities allow an end user application to monitor and control phones other than the user's to the extent that the PassageWay Telephony Server's security database will permit. Therefore, administrators must be familiar with the procedures in the PassageWay documentation that regulate what features a user may request and the phones and other devices for which a user may request a feature.
- There is little need for a device group that contains all devices, except perhaps for tracking, billing, or a similar application. The presence of such groups may be an indicator of unauthorized control, monitoring, or other security problem. Limit the use of these groups to those who need them.
- Similarly, minimize the use of the “exception list” feature in defining device groups. An exception list gives permission to operate on all devices except those explicitly named; therefore, an exception list is often a large device group and has the same vulnerabilities as a device group containing all devices.

- PassageWay Telephony Server administrators should be aware of switch COS and COR assignments and should not define device groups that allow applications to use third party call control to originate from an unrestricted phone and then transfer the call to a restricted phone. Such programs might also act as agents for setting up trunk-to-trunk calls (where permitted by the PBX) from phones other than the requesting user's phone.
- Since a user with PassageWay Telephony Server administration privileges can open an administrative door to toll fraud just as a Communication Manager, MultiVantage™ Software, DEFINITY ECS or MERLIN LEGEND administrator can, protect administrative privileges for the PassageWay Telephony Server as closely as switch administrative restrictions.
- PassageWay Telephony Server administration permissions should be given only to a small number of trusted users since a user with administration privileges may grant other users full administration privileges. Only give users the privileges they need.
- Any PBX used in a development environment should not be connected to the public network (or networked with general use PBXs) since development environments may be informal, minimally protected environments.
- Exercise caution when using pcANYWHERE. PassageWay Telephony Services technical staff use this tool to diagnose and maintain their products on the customer premises. Simply having pcANYWHERE installed on a PC does not pose a security risk; it must be up and running and administered to receive calls. In addition, pcANYWHERE offers a number of security features. General tips for protecting the PassageWay product at the customer site when pcANYWHERE is used include the following:
  - — Only run pcANYWHERE as necessary.
  - — Do not publish the phone number for the modem.
  - — Use the return call option with Avaya phone number. (Do not set up pcANYWHERE without the callback option.)
  - — For added security, unplug the phone jack from the modem when pcANYWHERE is not in use.
  - — Change your password after services leaves and after remote access.
  - — Configure the following security options:
    - Require login names for callers.
    - Make passwords case-sensitive.
    - Log all failed connection attempts.

        - Set a maximum number of login attempts per call.
        - Allow time to enter the complete login.
        - Disconnect if inactive.
    - — Configure pcANYWHERE to log remote control and online sessions. (Set the `Save Session Statistics in Activity Log File` checkbox in the Other Session Parameters group box.)

- PassageWay Telephony Services communicates with the enterprise communications server through Communication Manager, MultiVantage™ Software, or the DEFINITY ECS LAN Gateway. Security features are not provided in this system component. For example, there is no encryption or password to prevent unauthorized use of the Ethernet link into the PBX. The following are recommendations:
    - — Customers are warned that the LAN Gateway link is not intended for wide area networking. It is recommended that customers not configure a LAN in such a way as to use the LAN Gateway link for local or wide area data networking.
    - — Customers should provide a separate, secure link between their PBXs and PassageWay Telephony Server(s). This presupposes a separate network adapter and hub used only for the LAN Gateway interface.

      In the Tserver, there should be no routing between the Network Interface Card (NIC) used for the DEFINITY LAN Gateway and the NIC used for client access. (This does not mean to imply, however, that all Telephony Server clients have to be on the same LAN.)

      For NetWare, if TCP/IP support is provided on a separate LAN, keep this support isolated from the LAN Gateway. For Windows NT, configure the NT machine for a secure LAN Gateway connection. Refer to Chapter 2 in the *PassageWay® Telephony Services for Windows NT® DEFINITY Enterprise Communications Server Network Manager's Guide*.
- The PassageWay Telephony Server is only as secure as the underlying system, either NetWare or Windows NT. Observe the security requirements of your operating system.

In addition, for Windows NT, it is recommended that the following be used:

- Multiple level administration permissions to control which administrators are allowed to pass on administration permission.
- Secure version of Windows NT with NTFS (NT File System). For additional security information on Windows NT, consult a reference book such as *Inside Windows NT* by Helen Custer or *Windows NT Resource Guide* by Microsoft Press.

TransTalk 9000 Digital Wireless System

The TransTalk 9000 Digital Wireless System is a flexible wireless adjunct for use with the Communication Manager, MultiVantage™ Software, DEFINITY ECS, MERLIN LEGEND, PARTNER II, PARTNER Plus, System 25, System 75, and System 85 communications systems, as well as the MERLIN MAIL Voice Messaging System. It provides employees up to 500 feet of mobility from the radio base station, allowing them to make and answer calls when they are away from their desk.

From a security standpoint, the handset for the TransTalk 9000 Digital Wireless System, the MDW 9000, has the same vulnerabilities as any desk set. If calling restrictions are required for the user or location where the handset is placed, the handset must be restricted at the switch.

In addition, since the MDW 9000 allows freedom of movement, the potential for employee abuse may be increased with this product. For example, employees could move to secluded areas, where they would not be seen or overheard, and make personal calls. For this reason, if restrictions are required, you should restrict the station ports in the same way as you would a desk set.

Security tips

- Educate customers about the possibility of employee abuse. Make sure they understand the potential risks.
- If your business needs warrant a number of MDW 9000 sets, make sure you understand each employee's calling needs. For instance, if your business does not require that employees make outgoing business calls, restrict the MDW handset(s) to internal or local calls.

Refer to the applicable section of this guide for information on switch restrictions to utilize with the TransTalk 9000 Digital Wireless System.

Call routing

10

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

Call routing call flow

The following is the basic call flow through Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1 and G3, or System 75:

- Endpoint signals switch to start call.
  - If originating endpoint is a station, the request for service is an off-hook.
  - If originating endpoint is a trunk, the request for service is seizure signal (wink start, off-hook, ground start).
- The switch signals endpoint to start dialing.
  - If the endpoint is a station, dial tone is played for the caller.
  - If the endpoint is a trunk, a start dial signal (wink dial tone, etc.) is sent to the originating end.
- The digit string is dialed.
- The first digit dialed is compared to dial plan record.
- The type of call is identified depending on the dialed digit.
- The calls can be to an extension number, trunk access code, attendant, or feature access code.
- The number of digits needed is known after the first digit is dialed.

Example 1: User dials 0. Call is routed to an attendant because zero is defined as an attendant call requiring one digit.

Example 2: User dials 2. Digit two is defined as a 4-digit extension code on in the dial plan. Three more digits are required to place the call. The three additional digits are dialed. The four digits dialed determine the destination called.

The system checks the calling permissions of the originator's COR to see if the COR of the originator is allowed to call the COR of the destination dialed. If the COR of the originator is set to **y** for the COR of the destination, the call will complete. If the COR of the originator is set to **n** for the COR of the destination, the intercept tone is returned to the caller.

Example 3: User dials 2. Digit nine is defined as feature access code for ARS. More digits will follow. As the digits are dialed they are checked against the ARS analysis table until a unique match is found. When the singular match is found, a check is made to see if a route pattern is identified. If a route pattern is not identified, the call is routed to intercept. If a route pattern is identified, the call is routed to that pattern.

When the call reaches the route, the trunk group identified as the first choice is checked for an available member. If a member is not available, the next choice in the pattern is checked for an available member.

When an available member is found, the FRL of the originating endpoint is checked against the FRL of the choice selected. If the FRL of the endpoint is greater than or equal to the FRL on the choice, the call completes. If the FRL is less than all the choices in the route pattern, intercept is returned to the caller.

Blocking calls

11

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

Country codes

The following is a list of international country codes for direct dialing. In developing your ARS patterns, you may want to consider blocking access to those countries that you do not want users to dial. Keep in mind that calls to Canada and the Caribbean are part of the North American Dialing Plan and should be treated, for ARS purposes, as you would calls to domestic locations. These locations are starred (*) in the following list.

You should check with your long distance carrier to receive updates to the country code list.

Afghanistan	93
Albania	355
Algeria	213
American Samoa	684
Andorra	376
Angola	244
Anguilla	1-264*
Antarctica	672
Antigua and Barbuda	1-268*
Argentina	54
Armenia	374

Aruba	297
Ascension Island	247
Australia	61
Austria	43
Azerbaijan	994
Bahamas	1-242*
Bahrain	973
Bangladesh	880
Barbados	1-246*
Barbuda	1-268*
Belarus	375
Belgium	32
Belize	501
Benin	229
Bermuda	1-441*
Bhutan	975
Bolivia	591
Bosnia & Herzegovina	387
Botswana	267
Brazil	55
British Virgin Islands	1-284*
Brunei	673
Bulgaria	359
Burkina Faso	226
Burundi	257
Cambodia	855
Cameroon	237
Canada	1*
Cape Verde Islands	238
Cayman Islands	1-345*
Central African Republic	236
Chad	235

Chatham Island (New Zealand)	64
Chile	56
China (PRC)	86
Christmas Island	61
Cocos-Keeling Islands	61
Colombia	57
Comoros	269
Congo	242
Cook Islands	682
Costa Rica	506
Croatia	385
Cuba	53
Cuba (Guantanamo Bay)	5399
Curacao	599
Cyprus	357
Czech Republic	420
Denmark	45
Diego Garcia	246
Djibouti	253
Dominica	1-767*
Dominican Republic	1-809*
East Timor	670
Easter Island	56
Ecuador	593
Egypt	20
El Salvador	503
Equatorial Guinea	240
Eritrea	291
Estonia	372
Ethiopia	251
Faeroe Islands	298
Falkland Islands	500

Fiji Islands	679
Finland	358
France	33
French Antilles	596
French Guiana	594
French Polynesia	689
Gabon	241
Gambia	220
Georgia	995
Germany	49
Ghana	233
Gibraltar	350
Global Mobile Satellite System (GMSS)	881
Greece	30
Greenland	299
Grenada	1-473*
Guadeloupe	590
Guam	1-671*
Guantanamo Bay	5399
Guatemala	502
Guinea-Bissau	245
Guinea (PRP)	224
Guyana	592
Haiti	509
Honduras	504
Hong Kong	852
Hungary	36
Iceland	354
India	91
Indonesia	62
Inmarsat (Atlantic Ocean - East)	871

Inmarsat (Atlantic Ocean - West)	874
Inmarsat (Indian Ocean)	873
Inmarsat (Pacific Ocean)	872
Inmarsat SNAC	870
Iran	98
Iraq	964
Ireland	353
Iridium (under deactivation)	8816, 8817
Israel	972
Italy	39
Ivory Coast	225
Jamaica	1-876*
Japan	81
Jordan	962
Kazakhstan	7
Kenya	254
Kiribati	686
Korea (North)	850
Korea (South)	82
Kuwait	965
Kyrgyz Republic	996
Laos	856
Latvia	371
Lebanon	961
Lesotho	266
Liberia	231
Libya	218
Liechtenstein	423
Luxembourg	352
Macau	853
Macedonia (former Yugoslav Republic)	389

Madagascar	261
Malawi	265
Malaysia	60
Maldives	960
Mali Republic	223
Malta	356
Marshall Islands	692
Martinique	596
Mauritania	222
Mauritius	230
Maayotte Island	269
Mexico	52
Micronesia (Federal States of)	691
Midway Island	808
Moldova	373
Monaco	377
Mongolia	976
Montserrat	1-664*
Morocco	212
Mozambique	258
Myanmar	95
Namibia	264
Nauru	674
Nepal	977
Netherlands	31
Netherland Antilles	599
Nevis	1-869*
New Caledonia	687
New Zealand	64
Nicaragua	505
Niger	227
Nigeria	234

Niue	683
Norfolk Island	672
Northern Marianas Islands (Saipan, Rota, & Tinian)	1-670
Norway	47
Oman	968
Pakistan	92
Palau	680
Palestine	970
Panama	507
Papua New Guinea	675
Paraguay	595
Peru	51
Philippines	63
Poland	48
Portugal	351
Puerto Rico	1-787*
Qatar	974
Reunion Island	262
Romania	40
Russia	7
Rwanda	250
St. Helena	290
St. Kitts/Nevis	1-869*
St. Lucia	1-758*
St. Pierre and Miquelon	508
St. Vincent and the Grenadines	1-784*
San Marino	378
Sao Tome and Principe	239
Saudi Arabia	966
Senegal	221
Serbia	381
Seychelles Islands	248

Sierra Leone	232
Singapore	65
Slovak Republic	421
Slovenia	386
Solomon Islands	677
South Africa	27
Spain	34
Sri Lanka	94
Sudan	249
Suriname	597
Swaziland	268
Sweden	46
Switzerland	41
Syria	963
Taiwan	886
Tajikistan	992
Tanzania	255
Thailand	66
Togo	228
Tokelau	690
Tonga Islands	676
Trinidad and Tobago	1-868*
Tunisia	216
Turkey	90
Turkmenistan	993
Turks and Caicos Islands	1-649*
Tuvalu	688
Uganda	256
Ukraine	380
United Arab Emirates	971
United Kingdom	44
United States of America	1
US Virgin Islands	1-340*

Universal Personal Telecommunications (UPT)	878
Uruguay	598
Uzbekistan	998
Vanuatu	678
Vatican CIty	39
Venezuela	58
Vietnam	84
Wake Island	808
Wallis and Futuna Islands	681
Western Samoa	685
Yemen	967
Yugoslavia	381
Zambia	260
Zanzibar	255
Zimbabwe	263

Blocking toll fraud destinations

Toll fraud calls are placed to locations all over the world. Table 11-1, used for illustrative purposes only, highlights some of the destinations where fraudulent calls may terminate. In the table, the destination is followed by the country code or Numbering Plan Area (NPA) you can enter to block calls to that location.

Table 11-1. Toll fraud calling destinations

Destination	Country Code/NPA
Dominican Republic	809xxx
Pakistan	92
Columbia	57
Jordan	962
Israel	972
Iran	98
Iraq	964
Kuwait	966
U.A.E.	971

NOTE:
To block calls to the Dominican Republic, you also need to enter the 3-digit office codes (shown as xxx in Table 11-1). The codes are 052 through 053, 188, 220 through 223, 241, 320, 350, 521 through 533, 535 through 547, 549 through 554, 556 through 569, 571 through 589, 592 through 598, and 681 through 689.

Blocking ARS calls on DEFINITY G1 and System 75

Use the following procedure to block calls to the destinations listed in Table 11-1. This procedure does not prohibit dialing calls via TAC (refer to "Disable direct access to trunks" on page 5-39 for details).

1. Use **change ars fnpa 000** to display the ARS FNPA Table screen.
2. Enter the routing pattern changes to ARS FNPA Tables 000 to 019, 100 to 119, and 800 to 819 as shown:

ARS FNPA TABLE

Partitioned Group Number: 1

Pattern Assignments

000-019		**100-119**		**800-819**	
00:2	10:	00:2	10:	00:2	10:2
01:2	11:r32	01:2	11:r32	01:2	11:2
02:h	12:r32	02:2	12:r32	02:2	12:2
03:2	13:	03:2	13:1	03:2	13:2
04:	14:	04:	14:	04:2	14:2
05:2	15:	05:	15:	05:2	15:2
06:	16:	06:	16:	06:2	16:2
07:	17:	07:	17:	07:2	17:2
08:	18:	08:	18:	08:2	18:2
09:	19:	09:	19:	09:r31	19:2

3. Use **change ars fnpa 32** to display the ARS FNPA Table screen.

4. Enter the routing pattern changes to ARS FNPA tables 500 to 599 and 900 to 999 as shown in the table below:

ARS RHNPA TABLE: 32

OFFICE CODES: 500-599

Pattern Choices

01:2 03: 05: 07: 09: 11:

02: 04: 06: 08: 10: 12:

Office Code - Pattern Choice Assignments (from 1 to 12 above)

70:12

71:12

72:12

73:12

74:12

75:12

76:12

77:12

78:12

79:12

ARS RHNPA TABLE: 32

OFFICE CODES: 900-999

Pattern Choices

01:2 03: 05: 07: 09: 11:

02: 04: 06: 08: 10: 12:

Office Code - Pattern Choice Assignments (from 1 to 12 above)

00:1	10:12	20:12	60:1	70:1	80:12
01:1	11:12	21:12	61:1	71:12	81:12
02:1	12:12	22:12	62:12	72:12	82:12
03:1	13:12	23:12	63:1	73:1	83:12
04:1	14:12	24;12	64:12	74:1	84:12
05:1	15:12	25:12	65:1	75:1	85:12
06:1	16:12	26:12	66:12	76:1	86:12
07:1	17:12	27:12	67:1	77:1	87:12
08:1	18:12	28:12	68:1	78:1	88:12
09:1	19:12	29:12	69:1	79:1	89:12

5. Use **change rhnpa table 31** to display the RHNPA Table 31 screen.
6. Enter the routing pattern changes to RHNPA Table 31 200 to 299, 300 to 399, and 500 to 599.

ARS RHNPA TABLE: 31

OFFICE CODES: 200-299

Pattern Choices

01:2 03: 05: 07: 09: 11:

02: 04: 06: 08: 10: 12:

Office Code - Pattern Choice Assignments (from 1 to 12 above)

20:1	40:1
21:12	41:12
22:12	42:1
23:12	43:1
24:1	44:1
25:1	45:1
26:1	46:1
27:1	47:1
28:1	48:1
29:1	49:1

ARS RHNPA TABLE: 31

OFFICE CODES: 300-399

Pattern Choices

01:2 03: 05: 07: 09: 11:

02: 04: 06: 08: 10: 12:

Office Code - Pattern Choice Assignments (from 1 to 12 above)

20:12	50:12
21:1	51:1
22:1	52:1
23:1	54:1
24:1	54:1
25:1	55:1
26:1	56:1
27:1	57:1
28:1	58:1
29:1	59:1

ARS RHNPA TABLE: 31

OFFICE CODES: 500-599

Pattern Choices

01:2 03: 05: 07: 09: 11:

02: 04: 06: 08: 10: 12:

Office Code - Pattern Choice Assignments (from 1 to 12 above)

20:12	30:12	40:12	50:12	60:12	70:1	80:12	90:1
21:12	31:12	41:12	51:12	61:12	71:12	81:12	91:1
22:12	32:12	42:12	52:12	62:12	72:12	82:12	92:12
23:12	33:12	43:12	53:12	63:12	73:12	83:12	93:12
24:12	34:12	44:12	54:12	64:12	74:12	84:12	94:12
25:12	35:12	45:12	55:2	65:12	75:12	85:12	95:12
26:12	36:12	46:12	56:12	66:12	76:12	86:12	96:12
27:12	37:12	47:12	57:12	67:12	77:12	87:12	97:12
28:12	38:12	48:12	58:12	68:12	78:12	88:12	98:1
29:12	39:12	49:12	59:12	69:12	79:12	89:12	99:1

Blocking ARS calls on G2.1 and System 85

Use the following procedure to block calls to the destinations listed in Table 11-1 on page 11-10. This procedure does not prohibit dialing calls via TAC (refer to ''Disable direct access to trunks'' on page 5-39 for details).

- To block calls to the Dominican Republic, use **PROC311 WORD3** (6-digit table for NPA=809) to route each specified NXX combination to an empty pattern.
- 011 calls must be blocked using **PROC313 WORD1** and at least seven digits must be administered. There are a total of 350 entries required to prohibit calling the destinations listed in Table 11-1 on page 11-10. Adjust your FRL level to restrict all stations or features from accessing unauthorized numbers.

Country	Entries	Translations
Pakistan	100	**011 920 0** through **011 929 9**
Columbia	100	**011 570 0** through **011 579 9**
Jordan	10	**011 962 0** through **011 962 9**
Israel	10	**011 972 0** through **011 972 9**
Iran	100	**011 980 0** through **011 989 9**
Iraq	10	**011 964 0** through **011 964 9**
Kuwait	10	**011 966 0** through **011 966 9**
U.A.E.	10	**011 971 0** through **011 971 9**

- To block 01 + calls, call your Central Office. Up to 3,500 entries are required to block 01 + calls, which is beyond the capacity of the table (maximum 2048 entries).

Blocking WCR calls on DEFINITY G2.2

Use the following procedure to block calls to the destinations listed in Table 11-1 on page 11-10.

- For calls to the Dominican Republic, specifically add the allowed NXX as **809***NXX*, length **10**, to the appropriate VNI (routing pattern).
- For 011 calls, use **PROC314 WORD1** to enter the following translations:

Country	Code	Length	Route Pattern
Pakistan	01192	5	0
Columbia	01157	5	0
Jordan	011962	6	0
Israel	011972	6	0
Iran	01198	5	0
Iraq	011964	6	0
Kuwait	011966	6	0
U.A.E.	011971	6	0

- For 01 calls, use **PROC314 WORD1** to enter the following translations:

Country	Code	Length	VNI
Pakistan	0192	4	0
Columbia	0157	4	0
Jordan	01962	5	0
Israel	01972	5	0
Iran	0198	4	0
Iraq	01964	5	0
Kuwait	01966	5	0
U.A.E.	01971	5	0

Blocking ARS calls on G3

This section contains a sample ARS Digit Analysis Table for G3. In the example, international and operator-assisted numbers are allowed, but 0700 calls are denied, as well as high toll destinations to these countries: Colombia, Pakistan, Jordan, Iraq, Saudi Arabia, United Arab Republic, Israel, Iran, Kuwait, and Puerto Rico.

Use the following procedure to block calls to the destinations listed in Table 11-1 on page 11-10.

- To access the section of the ARS Digit Analysis Table to be changed, use **change ars analysis (Enter digits between 0-9 "x," or "X" ["partition" (1-8)], ["min" (1-23)])**.
- Enter the following data:
  a. `Dialed String` field: Enter the digits to be collected (**0-9**, **x**, or **X**).
  b. `Total` field: Enter the minimum (**1-23** or **blank**) and maximum (**1-23** or **blank**) number of digits.
  c. `Route Pattern` field: For G3iV1, enter **1-254**, **r1-r32**, **blank** or **ign** (ignore). For G3rV1, G3V1.1 and later releases, enter **1-254**, **r1-r32**, **n/a** or **den** (denied).
  d. `Call Type` field: Enter **fnpa**, **hnpa**, **int**, **iop**, **natl, op**, **svc** or **unk**.

ARS DIGIT ANALYSIS TABLE

Partitioned Group Number: 1

Dialed String	Total Min	Total Max	Route Pat	Call Type
0	11	11	1	op
01	10	23	1	iop
011	10	23	1	int
01157	10	23		int
01192	10	23		int
011962	10	23		int
011964	10	23		int
011965	10	23		int
011966	10	23		int
011971	10	23		int
011972	10	23		int

Continued on next page

ARS DIGIT ANALYSIS TABLE — *Continued*

Partitioned Group Number: 1

Dialed String	Total Min	Total Max	Route Pat	Call Type
01198	10	23		int
0700	11	11		op
101xxxx	5	5		op
101xxxx	12	12		hnpa
101xxxx0	6	6	1	op
101xxxx0	16	16	1	op
101xxxx00	7	7	1	op
101xxxx01	15	23	1	iop
101xxxx01157	15	23		int
101xxxx01192	15	23		int
101xxxx011962	15	23		int
101xxxx011962	15	23		int
101xxxx011964	15	23		int
101xxxx011965	15	23		int
101xxxx011966	15	23		int
101xxxx011971	15	23		int
101xxxx011972	15	23		int
101xxxx01198	15	23		int
101xxxx0157	15	23		iop
101xxxx0192	15	23		iop
101xxxx01962	15	23		iop
101xxxx01964	15	23		iop
101xxxx01965	15	23		iop
101xxxx01966	15	23		iop
101xxxx01971	15	23		iop
101xxxx01972	15	23		iop
101xxxx0198	15	23		iop

Continued on next page

ARS DIGIT ANALYSIS TABLE — *Continued*

Partitioned Group Number: 1

Dialed String	Total Min	Total Max	Route Pat	Call Type
101xxxx0700	16	16		op
101xxxx1	16	16	1	fnpa
101xxxx1809	16	16		fnpa
180	11	11	1	fnpa
1809	11	11		fnpa

Blocking ARS calls on System 25 R3V3

The toll call allowed/disallowed lists, available in System 25 R3V3, permit the administrator to restrict international calling.

- To block calls to a specified country code, enter **0** and the country code to be disallowed. This entry blocks calls to the specified country code for stations assigned to that list.
- To block all international calling, use the wildcard character (.) to specify all country codes. Enter **0... .** This entry blocks calls to all countries for stations assigned to that list.

Remote access example (Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY G1, G3, and System 75)

12

NOTE:
Unless specifically stated otherwise, references in this document to "G3Vx and later" include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

This chapter provides procedures for setting up and disabling the Remote Access feature for Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75.

Setting up remote access

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G1, G3, and System 75, use the example below to set up the Remote Access feature to help prevent unauthorized use. This example creates a new ARS/AAR networking plan in a separate Partitioned Group Number (PGN) for remote access only. By using the ARS/ARS Analysis table that corresponds with the remote access PGN, you can easily control the numbers that are allowed and the numbers that are disallowed.

1. Enter **change remote-access** to display the Remote Access screen.
2. Enter **7** in the `Barrier Code Length` field.
3. Enter **n** in the `Authorization Code Required` field.
4. Select a 7-digit random number and enter it into the first `Barrier Code` field.
5. Select a unique COR (**0** through **63**, or **0** through **95** for G3) that is not used for any facility other than remote access.

   For this example, we will use **63**.
6. Enter the COR in the first `COR` field corresponding to the barrier code you entered in Step 4.

   For example, we would enter **63** in the first `COR` field.

7. Select a unique COS (**0** through **15**) that is not used for any facility other than remote access, and does not allow console permissions.

   For this example, we will use **15**.

8. Enter the COS in the first `COS` field corresponding to the barrier code you entered in Step 4.

   For example, we would enter **15** in the first `COS` field.

9. Use **change cor 63** (or the number of the COR you selected in Step 5) to administer the COR screen as shown in Steps 10 through 12.

10. Enter **0** in the `FRL` field.

11. Select a PGN (**1** through **8**) that is not in use in any other COR.

    This PGN will be reserved for remote access only. Enter this number in the `Partitioned Group Number` field. For this example, we will use PGN **8**.

    NOTE:
    Do not use the default PGN, which is generally **1**. If you do not see the `Partitioned Group Number` field on the COR screen, call your Avaya Technical Representative to enable the ARS/AAR Partitioning feature on the System-Parameters Customer-Options screen.

12. Use **change cos** and advance to the 15th column (or go to the COS that you selected in Step 7).

13. Enter **n** in *all* the fields associated with the COS.

14. Use **change trunk-group** (and the trunk group number) to administer each trunk group.

15. Enter **n** in the `Dial Access` field, or to limit TAC access, refer to "Disable direct access to trunks" on page 5-39.

    NOTE:
    Repeat Steps 14 and 15 for all the trunk groups in the system so that all outgoing calls route via ARS/AAR.

16. For Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3, use **change ars analysis x partition 8** and **change aar analysis x partition 8** (**x** equals **0** through **9**) to enter the dialed strings and the route pattern (and other pertinent information for the entry) where you want to allow calls.

    You may need to delete some default entries that are already there.

17. For DEFINITY G1 and System 75, use **change ars fnpa a00 group 8** (**a** equals **0** through **5**), **change ars hnpa n00 group 8** (**n** equals **2** through **9**), and **change rnx n00 group 8** (**n** equals **2** through **9**) to enter the Route Pattern where you want to allow calls.

    The dialed string entries are already specified, so enter the Route Pattern number only. Here are some considerations:

    — The HNPA table has the default value for the route pattern set to **1**, so you may not want to administer any trunk group to that route pattern. Use **change route-pattern 1** to delete any trunk groups already there.

    — Similarly, the RNX table has the default value for the Route Pattern set to **254**. Use **change route-pattern 254** to delete any trunk groups administered there.

18. Leave the `Route Pattern` field **blank** for all dialed strings that you want to disallow the calls, such as international and operator calls.

    Any ARS/AAR calls starting with that dialed string will be blocked.

19. For all the route patterns assigned to ARS/AAR Partition 8, use **change route-pattern** to administer an appropriate FRL (**1** through **7**) in the FRL field.

    Since the FRL on the COR reserved for remote access is **0**, the remote access caller will always be prompted for an authorization code for outside calls.

20. Assign authorization codes for your remote access users that provide the lowest possible FRL to match each user's calling requirements.

    See Chapter 3, ''IP security'' for additional security measures.

Permanently disabling remote access

For Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY G3, System 85 R2V4n 3.0 and later, and the "n" versions of G1 and System 75V3, as an additional step to ensure system security, the Remote Access feature can be permanently removed. Permanent removal protects against unauthorized remote access usage even if criminals break into the maintenance port. See your account representative for information on the "n" upgrade.

To permanently disable the Remote Access feature in System 85R2V4n 3.0 and later, or G2.2 3.0 and later:

- Use **PROC275 WORD4 FIELD2**, and change the value to 1.

To permanently disable the Remote Access feature in System 75V3, G3, and the "n" versions of G1:

- Enter **change remote-access** to display the Remote Access screen.
- Make sure the `Remote Access Extension` field is blank.
- Enter **y** in the `Permanently Disable` field.
- Enter **save translation**. *You MUST enter this command or the change will be lost if the switch is rebooted*.
- Enter **display remote-access** to verify the changes. If you get an error message or you cannot display the screen, then you know it worked.

To permanently disable the Remote Access feature in Communication Manager and MultiVantage™ Software:

- Enter **change remote-access** to display the Remote Access screen.
- Make sure the `Remote Access Extension` field is blank.
- Enter **y** in the `Permanently Disable` field.
- Log off. (You must log off to enable the change.)
- Log back in and enter **display remote-access** to verify the changes. If you get an error message or you cannot display the screen, then you know it worked.

The Remote Access feature is disabled after you log off from the switch.

For System 85 R2V4n 3.0 and G2.23.0 and later, to permanently disable the Remote Access feature:

- Use **PROC275 WORD4 FIELD2**, and change the value to 1.

NOTE:
Once the Remote Access feature has been permanently disabled, only the Avaya Technical Service Center can reenable it. Charges may apply for this service.

Administering features of the DEFINITY G3V3 and later

13

NOTE:
Unless specifically stated otherwise, references in this document to "G3Vx and later" include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

This chapter provides information on administering these features in Communication Manager, MultiVantage™ Software, DEFINITY ECS and DEFINITY G3.

DEFINITY G3V3 and later:

- Enhanced Security Violation Notification (SVN)
- Barrier code aging
- Customer logins and forced password aging

DEFINITY G3V4 and later:

- Logoff notification
- Customer login accessible through INADS remote administration port
- Facility test call notification
- Remote access notification

In addition, Chapter 16 describes "Securing DEFINITY systems (Release 7.2 and Later) with Access Security Gateway" on page 16-4.

Administering the SVN feature

This section contains the following subsections:

- Administering the login component
- Administering the barrier code security violations parameters of the SVN feature
- Administering the authorization code component
- Administering the station security code component

Administering the login component

To administer system parameters for the login component of the SVN feature, do the following:

1. To access the Security-Related System Parameters screen from the command line interface, enter **change system-parameters security** (G3V3 and later) or **change system-parameters** (releases prior to G3V3).
2. Enter **y** in the `SVN Login Violation Notification Enabled` field.

   When this field is set to **y**, the following fields appear on the Security-Related System Parameters screen:

   - `Originating Extension`

     Enter an unassigned extension, local to the switch and conforming to the dial plan, for the purpose of originating and identifying SVN referral calls for login security violations.

     The originating extension initiates the referral call in the event of a login security violation. It also sends the appropriate alerting message or display to the referral destination.

   - `Referral Destination`

     Enter an extension assigned to a station or attendant console that will receive the referral call when a security violation occurs. The referral destination must be equipped with a display module unless the Announcement Extension has been assigned.

     For G3V3 and later, call vectoring using time of day routing allows security notification to be extended off-premises.

   - `Login Threshold`

     Enter the minimum number of login attempts that will be permitted before a referral call is made. The value assigned to this field, in conjunction with the `Time Interval` field, determines whether a security violation has occurred. The system default is **5**.

- Time Interval

  Enter the time interval within which a login security violation must occur. The range is one minute to eight hours (0:01 to 7:59), and is entered in the form x:xx. For example, if you want the time interval to be 1 minute, enter **0:01**. If you want the time interval to be seven and one-half hours, enter **7:30**. The system default is **0:03**.

- Announcement Extension

  Enter an extension that is assigned to the login SVN announcement. The announcement must be recorded for the SVN referral call to be made. A repeating announcement is suggested, especially if the SVN referral call might go to an answering machine.

3. For releases before DEFINITY G3V3, administer an “lsvn-call” button on any station/attendant console (maximum 1 per system).

   The SVN button location can be determined by entering the command **display svn-button-location**. Activation of this feature button initiates the placement of login referral calls, until the button is deactivated.

4. For DEFINITY G3V3 and later releases, administer an “lsvn-halt” button on any station/attendant console (maximum 1 per system).

   The SVN button location can be determined by entering the command **display svn-button-location**. Activation of this button stops the placement of all login referral calls, until the button is deactivated.

Enable/disable a login ID

The Disable Following a Security Violation field on the Login Administration screen is used to set the SVN parameters for a single login.

- Enter **y** in this field to have the SVN feature disable the specified login when a security violation is detected for that login ID. The system default is **y**.
- Enter **n** in this field if you don’t want to have the SVN feature disable the specified login if a security violation is detected for that login ID.

The Disable Following a Security Violation field is dynamic and will only appear on the Login Administration screen when the login component of the SVN feature is enabled.

To enable a login that has been disabled by a security violation, or disabled manually with the **disable login** command:

1. Log in to the switch using a login ID with the proper permissions.
2. Enter the command **enable login <login>**.

To disable a login:

1. Log in to the switch using a login ID with the proper permissions.
2. Enter the command **disable login <login>**.

List the status of a login ID

To list the status of a login:

1. Log in to the switch using a login ID with the proper permissions.
2. Enter the command **list logins**.

A display indicating the status of all logins appears. Possible login ID statuses are:

- disabled — The login was disabled manually using the **disable login** command.
- svn-disabled — A security violation was detected for that login and the login was disabled by the SVN feature.
- active — The login is currently logged in.
- inactive — The login is not logged in.
- void — The password associated with the login has been set to **void**.

Administering the barrier code security violations parameters of the SVN feature

To administer the (barrier code) security violation parameters of the SVN feature, do the following:

1. To access the Security-Related System Parameters screen, enter **change system-parameters security** (G3V3 and later) or **change system-parameters** (releases prior to G3V3).
2. Enable the component of the feature by entering **y** in the `SVN Remote Access Violation Notification` field.

   When this field is enabled, the following additional fields appear on the Security-Related System Parameters screen:

   - `Originating Extension`

     Enter an unassigned extension that is local to the switch and conforms to the dial plan, for the purpose of originating and identifying SVN referral calls for login security violations.

     The originating extension initiates the referral call in the event of a login security violation. It also sends the appropriate alerting message or display to the referral destination.

   - `Referral Destination`

     Enter an extension assigned to a station or attendant console that will receive the referral call when a security violation occurs. The referral destination must be equipped with a display module unless the Announcement Extension has been assigned.

     For DEFINITY G3V3 and later, call vectoring using time of day routing allows security notification to be extended off-premises.

- `Login Threshold`

  Enter the minimum number of login attempts that will be permitted before a referral call is made. The value assigned to this field, in conjunction with the `Time Interval` field, determines whether a security violation has occurred. The system default is **5**.

- `Time Interval`

  Enter the time interval within which a login security violation must occur. The range is one minute to eight hours (0:01 to 7:59), and is entered in the form x:xx. For example, if you want the time interval to be 1 minute, enter **0:01**. If you want the time interval to be seven and one-half hours, enter **7:30**. The system default is **0:03**.

- `Announcement Extension`

  Enter an extension that is assigned to the SVN announcement. The announcement must be recorded for the SVN referral call to be made. A repeating announcement is suggested, especially if the SVN referral call might go to an answering machine.

3. To activate the Disable Following A Security Violation feature, display the Remote Access screen and enter **y** in the `Disable Following a Security Violation` field.
4. For releases before G3V3, administer an “rsvn-call” button on any station/attendant console (maximum 1 per system).

   The SVN button location can be determined by entering the command **display svn-button-location**. Activation of this feature button initiates the placement of referral calls, until the button is deactivated.
5. For G3V3 and later releases, administer an “rsvn-halt” button on any station/attendant console (maximum 1 per system).

   The SVN button location can be determined by entering the command **display svn-button-location**. Activation of this feature button stops the placement of all referral calls until the button is deactivated.

Enable/disable remote access code

To enable a remote access code that has been disabled following a security violation, or disabled manually with the **disable remote-access** command:

1. Log in to the switch using a login ID with the proper permissions.
2. Enter the command **enable remote-access**.

To disable a remote access code:

1. Log in to the switch using a login ID with the proper permissions.
2. Enter the command **disable remote-access**.

Administering the Remote Access Kill After N Attempts feature

Following is an example of how to administer this feature.

1. Enter **change system-parameters features security** (G3V3 and later) or **change system-parameters features** (releases prior to G3V3).

   When the system-parameters features screen appears, complete the following fields:

   - `SVN Remote Access Violation Notification Enabled` field — Enter **y** to enable the remote access component of the SVN feature.
   - `Originating Extension` field — Enter an unassigned extension that conforms to the switch dial plan.
   - `Referral Destination` field — Enter an extension that is assigned to a station equipped with a display module.
   - `Barrier Code Threshold` field — Enter the number of times entry of an invalid barrier code will be permitted before a security violation is detected.
   - `Time Interval` field — Enter the duration of time that the invalid barrier code attempts must occur within.

2. Enter the **change remote-access** command to access the Remote Access screen.

   - `Disable Following A Security Violation` field — If not already assigned, enter **y** to disable remote access following a security violation.

     NOTE:
     The `Disable Following A Security Violation` field is dynamic. It will only appear if the remote access component of the SVN feature is enabled.

In the event of a remote access barrier code security violation, a referral call is generated, alerting the switch administrator of the violation. When the violation is detected, the Remote Access feature is disabled, prohibiting any further use until the security violation is investigated.

Consult the monitor security-violations report, trunk group measurements reports, and security measurements reports to determine the nature and source of the security violation. Local exchange and long distance carriers may provide assistance in tracing the source of the violation. The Remote Access feature should not be re-enabled until the source of the violation is identified, and you are confident that the feature is secure.

Enter the **enable remote-access** command to re-enable the Remote Access feature.

If the Remote Access feature is to be dormant for a period of time, the feature can be disabled using the **disable remote-access** command. Entry of this command will disable the Remote Access feature until it is re-enabled using the **enable remote-access** command.

Administering the Login ID Kill After N Attempts feature

Following is an example of how to administer this feature.

1. Enter the **change system-parameters features** command to assign Security Violation Notification (SVN) parameters.

   When the system-parameters features screen appears, complete the following fields:

   - `SVN Login Violation Notification Enabled` field — Enter **y** to enable the login component of the SVN feature.
   - `Originating Extension` field — Enter an unassigned extension that conforms to the switch dial plan.
   - `Referral Destination` field — Enter an extension that is assigned to a station equipped with a display module.
   - `Login Threshold` field — Enter the number of times entry of an invalid login ID, or valid login ID/invalid password combination will be permitted before a security violation is detected.
   - `Time Interval` field — Enter the duration of time that the invalid login attempts must occur within.

2. Enter the **add/change login <login ID>** command to access the Login Administration screen.

   - `Disable Following A Security Violation` field — If not already assigned, enter **y** to disable the login ID following a security violation involving the login ID.

In the event a security violation involving the login ID is detected, a referral call is generated, alerting the switch administrator of the violation. When a login violation is detected for a valid login ID, the login ID is disabled, prohibiting any further use until the security violation is investigated and the login ID is re-enabled.

Consult the monitor security-violation report and security measurements report to determine the nature and source of the security violation. If the attempts to access the switch administration originated from a remote source, the local exchange and long distance carriers may provide assistance in tracing the source of the invalid access attempts. The affected login ID should not be re-enabled until the source of the violation is identified and you are confident that the switch administration maintenance interface is secure.

Enter the **enable login <login ID>** command to re-enable the login ID.

If a login ID is to be dormant for a period of time, the login ID can be disabled using the **disable login <login ID>** command. Entry of this command will disable the login ID until it is re-enabled using the **enable login <login ID>** command.

Administering the authorization code component

To administer the authorization code component of the SVN feature in G3V3 and later releases, do the following:

1. Access the Security-Related System Parameters screen by entering **change system-parameters security** from the command line interface.

   When the `SVN Authorization Code Violation Notification Enabled` field is set to **y**, the following additional fields appear on the Security-Related System Parameters screen:

   - `Originating Extension`

     Enter an unassigned extension that is local to the switch and conforms to the dial plan, for the purpose of originating and identifying SVN referral calls for authorization code security violations.

     The originating extension initiates the referral call in the event of an authorization code security violation. It also sends the appropriate alerting message or display to the referral destination.

   - `Referral Destination`

     Enter an extension assigned to a station or attendant console that will receive the referral call when an authorization code security violation occurs.

     If the announcement extension field is blank, the referral destination must be on the switch and a display module is required. Call vectoring, using time of day routing, allows security notification to be extended off-premises.

   - `Authorization Code Threshold`

     Enter the minimum number of invalid authorization code attempts that will be permitted before a referral call is made. The value assigned to this field, in conjunction with the `Time Interval` field, will determine whether a security violation has occurred. The system default for this threshold is **10**.

- `Time Interval`

  Enter the time interval within which the authorization code security violations must occur. The range for the time interval is one minute to eight hours (0:01 to 7:59), and is entered in the form x:xx. For example, if you want the time interval to be one minute, enter **0:01**. If you want the time interval to be seven and one-half hours, enter **7:30**. The system default is **0:03**.

- `Announcement Extension`

  Enter an extension that is assigned to an SVN authorization code announcement. The announcement must be recorded for the SVN referral call to be made. A repeating announcement is suggested, especially if the SVN referral call might go to an answering machine.

2. Administer an “asvn-halt” button on any station/attendant console.

   The location of the SVN button can be determined by entering the **display svn-button-location** command. Activation of this button stops the placement of authorization code referral calls until the button is deactivated.

Administering the station security code component

Page 2 of the Security-Related System Parameters screen allows the user to administer parameters relevant to Station Security Codes. This page appears only for Release 5 versions or later of G3. To administer parameters for station security codes:

1. Access the Security-Related System Parameters screen by entering the **change system-parameters security** command from the command line interface.
2. Populate the following fields:

   - `Minimum Station Security Code Length`

     Enter a minimum station security code length (3 through 8). This value is used to verify all subsequent security code changes; however, any existing security codes are assumed to be valid. Default is **4**.

   - `SVN Station Security Code Violation Notification Enabled?`

     Activate (by entering **y**) or deactivate (by entering **n**) the security violation notification for station security codes. Default is **n**.

- Originating Extension

  This is a dynamic field that is displayed only whenever the SVN Station Security Code Violation Enabled field is set to **y**. Whenever a Station Security Code SVN Referral call is made, the extension in this field is internally the originating extension. It has no other significance than that it is not available for use as a normal extension. Enter any unassigned extension containing five digits.

- Referral Destination

  This is a dynamic field that is displayed only whenever the SVN Station Security Code Violation Notification Enabled field is set to **y**. Whenever a station security code SVN referral call is made, it is made either to the extension (if provided) in this field or to the attendant (if the field contains **attd**). If the destination is a station, and if the Announcement Extension field is set to **blank**, the destination must be equipped with a display module. Enter one of the following: an assigned extension containing 5 digits or **attd** for attendant.

- Station Security Code Threshold

  This value in this field functions in conjunction with the value in the Time Interval field. The value in the former field indicates a noteworthy count of invalid attempts in using station security codes which, if exceeded within the time period indicated in the latter field, constitutes a security violation. Whenever this occurs, a station security code SVN referral call is made. Also, invalid attempts are logged, but they are ignored unless the count of such attempts exceeds the administered threshold. This is a dynamic field that is displayed only whenever the SVN Station Security Code Violation Notification Enabled field is set to **y**. Enter a number between **1** and **255**. Default is **10**.

- Time Interval

  This value in this field functions in conjunction with the value in the Station Security Code Threshold field. The value in the latter field indicates a noteworthy count of invalid attempts in using station security codes which, if exceeded within the time period indicated in the former field, constitutes a security violation. Whenever this occurs, a station security code SVN referral call is made (unless this capability has been suppressed). This is a dynamic field that is displayed only whenever the SVN Station Security Code Violation Notification Enabled field is set to **y**. Enter a value from **0:01** to **7:59**. The first digit represents the hour, and the second and third digits represent the minutes. Default is **0:03**.

- Announcement Extension

  This field contains an extension corresponding to a recorded announcement that is to be played whenever a station security code SVN referral call is made. This allows the referral destination to be a phone without a display. This is a dynamic field that is displayed whenever the corresponding SVN Violation Notification Enabled field is set to **y**. Enter a 5-digit extension to be assigned to the appropriate announcement.

Administering barrier code aging

To administer the Barrier Code Aging feature:

1. Log in with the proper permissions and display the Remote Access screen by entering the command **change remote-access**.
2. Once the Remote Access screen is displayed, administer Remote Access/Barrier Code Aging by filling in the following fields:

   - Remote Access Extension

     Enter an extension number (not a VDN extension) for remote access. This extension is associated with each trunk that supports the Remote Access feature. The default for this field is blank.

     The remote access extension is used as if it were a DID extension. Only one DID extension may be assigned as the remote access extension. Calls to that number are treated the same as calls on the remote access trunk.

     When a trunk group is dedicated to remote access, the remote access extension number is administered on the trunk group's incoming destination field.

   - Barrier Code Length

     Enter the desired barrier code length (**4** to **7** digits), or leave this field **blank** indicating that a barrier code is not required. Assigning a barrier code length of **7** provides maximum security.

   - Authorization Code Required

     Enter **y** if an authorization code must be dialed by Remote Access users to access the system's remote access facilities. The default for this field is **n**. Use of an authorization code in conjunction with barrier codes increases the security of the Remote Access feature.

   - Remote Access Dial Tone

     This field appears on the form if the Authorization Code Required field has been set to **yes**. Enter **y** in this field if remote access dial tone is required as a prompt to the user. For maximum security do not use authorization code dial tone.

- Barrier Code

  Assign a barrier code that conforms to the number entered in the Barrier Code Length field. All codes must be 4- to 7-digits. The code can be any combination of the digits **0** through **9**.

  If the Barrier Code Length field is blank, the first barrier code field must be specified as **none**. Duplicate entries are not allowed. The system default for this field is a **blank**. Assign a 7-digit number in this field for maximum security.

- Class of Restriction (COR)

  Enter the COR (**0** through **95**) associated with the barrier code that defines the call restriction features. The default for this field is **1**. Assigning the most restrictive COR that will provide only the level of service required will provided the maximum security.

- Class of Service (COS)

  Enter the COS (**0** through **15**) associated with the barrier code that defines access permissions for call processing features. The system default for this field is **1**. Assigning the most restrictive COS that will provide only the level of service required will provide the maximum security.

- Expiration Date

  Assign an expiration date for the remote access barrier code based on the expected length of time the barrier code will be needed. Valid entries are a date greater than the current date or a blank; the default is the following day's date. If an expiration date is assigned, a warning message displays on the system copyright screen seven days prior to the expiration date, indicating that a barrier code is due to expire. The system administer may modify the expiration date to extend the time interval if needed.

- No. of Calls

  This field specifies the number of remote access calls that can be placed using the associated barrier code. Valid entries are **1** to **9999**, or **blank**. The default is **1**. The Expiration Date field and No. of Calls field can be used independently or, to provide maximum security, they can be used in conjunction with each other. If both the Expiration Date and No. of Calls fields are assigned, the corresponding barrier code will expire when the first of these criteria is satisfied.

- `Calls Used`

  This field is a display-only field that specifies the number of calls that have been placed using the corresponding barrier code. The `Calls Used` field is incremented each time a barrier code is successfully used to access the Remote Access feature.

  NOTE:
  A usage that exceeds the expected rate may indicate improper use.

- `Permanently Disable`

  Enter **y** to permanently disable the Remote Access feature. The Remote Access screen will no longer be accessible.

- `Disable following a Security Violation?`

  Enter **y** to disable the Remote Access feature following a remote access security violation. The system administrator may re-enable Remote Access with the **enable remote-access** command.

Administering customer logins and forced password aging

This section contains the following subsections:

- Adding customer logins and assigning initial password
- Changing a login's attributes
- Administering login command permissions

Adding customer logins and assigning initial password

For DEFINITY G3V3 and later releases, the two types of customer logins are:

- superuser—Provides access to the **add, change, display, list,** and **remove** commands for all customer logins and passwords.

  The superuser can administer any mix of superuser/nonsuperuser logins up to ten system logins.

- nonsuperuser—Limits permissions according to restrictions specified by the superuser when administering the non-superuser login.

  A nonsuperuser may change his/her password with permission set by the superuser; however, once a password has been changed, the nonsuperuser must wait 24 hours before changing the password again. The superuser may administer up to 10 non-superuser logins.

To add a customer login you must be a superuser, have administrative permissions, and follow these steps:

NOTE:
Always use your own unique login — never a Avaya customer login or variation thereof (for example, “cust,” “rcust,” “cust1,” “rcust1,” etc.).

1. Access the Login Administration screen by entering **add login <name>**.

   The 3- to 6-character login name (numbers 0 to 9, characters a to z or A to Z) you entered is displayed in the `Login's Name` field.

2. Enter your superuser password in the `Password of Login Making Change` field.

3. Enter **customer** in the `Login Type` field.

   The system default for this field is **customer**. The maximum number of customer logins of all types is 11.

4. Enter **super-user** or **non-super-user** in the `Service Level` field.

5. Enter **y** in the `Disable Following a Security Violation` field to disable a login following a login security threshold violation.

   This field is a dynamic field and only appears on the Login Administration screen when the SVN Login Violation Notification feature is enabled. The system default for this field is **y**.

6. For G3V4 only, enter **y** or **n** in the `Access to INADS Port?` field to specify whether the customer login will be accessible through the INADS remote administration port.

   The system default for this field is **n**. This field is a dynamic field and only appears on the Login Administration screen if the `Login Type` field is set to **customer**, and the `Customer Access to INADS Port` field (on the Maintenance-Related System Parameters screen) is set to **y**.

   NOTE:
   In DEFINITY G3V4, the Avaya login must be through the INADS port.

7. Enter a password for the new login in the `Login's Password` field.

   A password must be 4 to 11 characters and contain at least one alphabetic and one numeric symbol; valid characters include numbers, and the following symbols: ! & * ? ; ' ^ ( ) , : - @ # $ % .

   The system does not echo the password to the screen as you type.

8. Re-enter the password in the `Re-enter Login's Password` field.

   The system does not echo the password to the screen as you type.

9. In the `Password Aging Cycle Length (Days)` field, enter the number of days (from the current day) when you wish the password to expire.

   If a blank is entered in this field, password aging will not apply to the specified login. Valid entries are from **1** to **99** days or a **blank**. When a login password is within seven days or less from the expiration date, a warning message is displayed when the user logs in:

   `WARNING: your password will expire in xx days.`

10. For DEFINITY G3V4 and later only, enter **y** or **n** in the `Facility Test Call Notification?` field to specify whether this login will be notified in the event that Facility Test Call feature is used.

    The system default for this field is y.

11. If y was entered in step 10, enter **y** or **n** in the `Acknowledgment Required?` field to specify whether acknowledgment of the notification is required before logoff is permitted.

    The system default for this field is **y**. This field is a dynamic field and only appears on the Login Administration screen if the `Facility Test Call Notification?` field is set to **y**.

12. For DEFINITY G3V4 and later, enter **y** or **n** in the `Remote Access Notification?` field to specify whether this login will be notified in the event that remote access is used.

    The system default for this field is **y**.

13. If **y** was entered in step 12, enter **y** or **n** in the `Acknowledgment Required?` field to specify whether acknowledgment of the notification is required before logoff is permitted.

    The system default for this field is **y**. This field is a dynamic field and only appears on the Login Administration screen if the `Remote Access Notification?` field is set to **y**.

Changing a login's attributes

To change a customer login's attributes, you must be a superuser, have administrative permissions, and do the following:

1. Access the Login Administration screen by entering the **change login <name>** command.

   The 3- to 6-character login name (numbers 0 to 9, characters a to z or A to Z) you entered is displayed in the Login's Name field.

2. Enter your superuser password in the `Password of Login Making Change` field.

3. Enter **customer** in the `Login Type` field.

   The system default for this field is **customer**. The maximum number of customer logins of all types is **11**.

4. Enter **super-user** or **non-super-user** in the `Service Level` field.

5. Enter **y** in the `Disable Following a Security Violation` field to disable a login following a login security threshold violation.

   This field is a dynamic field and will only appear on the Login Administration screen when the SVN Login Violation Notification feature is enabled. The system default for this field is **y**.

6. Enter a password for the new login in the `Login's Password` field.

   A password must be 4 to 11 characters and contain at least 1 alphabetic and 1 numeric symbol; valid characters include numbers, and the following symbols: ! & * ? ; ' ^ ( ) , : - .

   The system will not echo the password to the screen as you type.

7. Re-enter the password in the `Re-enter Login's Password` field.

   The system will not echo the password to the screen as you type.

8. In the `Password Aging Cycle Length` field, enter the number of days (from the current day) when you wish the password to expire.

   If a blank is entered in this field, password aging will not apply to the specified login. Valid entries are from **1** to **99** days or a **blank**. When a login password is within seven days or less from the expiration date, a warning message is displayed when the user logs in:

   `WARNING: your password will expire in xx days.`

Administering login command permissions

Users with superuser permissions can set the permissions of the logins they create by means of the Command Permissions Categories screen. The DEFINITY commands for G3V3 and later releases are divided into three categories:

- Common commands
- Administration commands
- Maintenance commands

Each category has subcategories that, when set to **y**, give permission to use the commands sets associated with that category. When the Command Permissions Categories screen is displayed for a login, the subcategory fields appear with the fields set to give the login full permissions for that login type. The superuser administering login permissions can set any fields to deny access to a command category for the specified login.

To administer command permissions, log in as superuser and do the following:

1. Enter **change permissions login <login name>** to access the Command Permissions Categories screen.

   When the screen is displayed for a login, the default permissions for that login type appear on the screen.

2. Select a category for the login and enter **y** in each field where permission to perform an administrative or maintenance action is needed.

   The command object you select must be within the permissions for the login type you are administering.

   If the `Maintenance` option is set to **y** on the Customer Options screen, the superuser may enter **y** in the `Maintain Switch Circuit Packs` or `Maintain Process Circuit Packs` fields.

   NOTE:
   A superuser with full superuser permissions can restrict additional administrative or maintenance actions for a specified login by entering **y** in the `Additional Restrictions` field on the Command Permission Categories screen. (A superuser administering the login must not have the `Additional Restrictions` field set to **y** for his/her own login.)

3. Enter the additional restrictions for a login in the `Restricted Object List` field on the Command Permission Categories Restricted Object List screen.

   You may enter up to 40 command names (object names) to block actions associated with a command category for a specified login. You may enter two pages of commands (objects) to be restricted (20 commands per page, for a total of 40 commands per login).

Display a specified login

To display a specified login, enter the command **display login <login name>**. The system displays the specified login's service level, status, and password aging cycle length.

List logins

To list all of the system logins and the status of each login, enter the command **list logins**. The system displays a list of all current logins and their service level, status, and password aging cycle length.

Remove a login

To remove a login from the system, enter the command **remove login <login name>**. The system displays the Login Administration screen. Press **Return** to remove the login, or select **Cancel** to exit the remove login procedure without making a change.

Administering the security violations reports

The security viiolations reports provide current status information for invalid login or remote access (barrier code) or authorization code attempts. The following security violations reports are available:

- Login Violations
- Remote Access Barrier Code Violations
- Authorization Code Violations
- Station Security Code (SSC) Violations

NOTE:
Station security codes are used with the Personal Station Access feature and the Extended User Administration of Redirected Calls feature.

The data displayed in these reports is updated at 30 second intervals. A total of 16 entries are maintained for each type of violation. The oldest information is overwritten by the new entries at each 30-second update.

To access the security violations reports, enter the **monitor security-violations <report name>** command, where **report name** is either **login**, **remote-access**, **station-security-codes**, or **authorization-code**.

Changing your password

14

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

This chapter provides steps for changing passwords for systems listed in this handbook, where applicable.

AUDIX Voice Mail System

- System administrators:

  Use the Identification screen to change your login password.

  1. To access this screen, with the cursor on the PATH line, type **id** (identification) and press **F8** (Enter).
  2. Move the cursor to the `New Password` field and type the password you have selected.
  3. Move the cursor to the `Old Password` field and type **CUST**.
  4. Press **F1** (Change or Run) to save the new password.
  5. Press **F7** (EXIT) to exit this screen.

- End users:

  1. Press **5** at the main AUDIX Voice Mail System menu.
  2. Follow the prompts to change your password.

AUDIX Voice Power System

- System administrators:
  1. Access the AUDIX Voice Power System main menu.
  2. Select **Subscriber Administration**.
  3. On the Subscriber Administration screen, enter a password, a name, and an extension.
  4. Press **F3** (Exit).
- End users:
  1. Enter your extension and password.
  2. Press **5**.
  3. Follow the prompts to change your password.

CONVERSANT Voice Information System

- System administrators:
  1. Log in using the login name associated with the password you want to change.
  2. From the Avaya FACE screen, highlight **System Administration** and press **Enter**.
  3. From the System Administration screen, highlight **Change Password** and press **Enter**.

     The screen clears and the UNIX system **passwd** command is executed. At the top of the screen, the following message is displayed:

     ```
     Strike BREAK or DEL to return to Avaya
     Administration without changing your password.
     ```
  4. When prompted for your current password (old password), type the password you used when you logged in.
  5. When prompted for the new password (new password), enter the new password.

     The password you enter is not displayed on the screen.

6. When prompted to repeat the new password (re-enter new password), enter the new password again.

   If the two password entries are the same, the password is assigned. If the two password entries do not match, the following message is displayed:

   ```
   They don't match; try again.
   New password:
   ```

   You receive an error message if:

   — You enter the old password incorrectly.

   — The new password is not at least six characters long.

   — The new password does not have two alphabetic characters and at least one special character in the first eight.

   — The password resembles the login name by being a reverse or circular shift.

   — The new password does not differ from the old password by three or more characters.

   — The new password includes a space or colon (:).

   After you reenter the new password, you are prompted to press **Enter** to continue.

7. Press **Enter** to return to the System Administration screen.

- End users:

  None

DEFINITY AUDIX System

- System administrators:

  You can change two passwords: that of the currently logged-in user, and the system password. (You need *cust* or higher-level login permissions.)

  — Currently logged-in user's password

  Use the Password screen to change the password of the currently logged-in user.

  1. To access the Password Administration screen, type **change password** and press **Enter**.
  2. Type the currently logged-in user's login ID in the `Login ID` field.
  3. Enter the current system password in the `Old Password` field.
  4. Enter the new system password in the `New Password` field.
  5. Enter the new system password again in the `Confirm New Password` field.
  6. Press **Enter**.

  — System password

  Use the System Password screen to change the system password.

  1. To access the System Password screen, type **change system-parameters password** and press **Enter**.
  2. Type the customer login ID password in the `Customer Login Password` field.
  3. Enter the current system password in the `Old System Password` field.
  4. Enter the new system password in the `New Password` field.
  5. Enter the new system password again in the `Confirm New Password` field.
  6. Press **Enter**.

- End users:

  1. Press **5** at the main AUDIX Voice Mail System menu.
  2. Follow the prompts to change your password.

  NOTE:
  If you are a new subscriber and the system administrator has not specified a password for you, you will be prompted to enter one when you first log on.

Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G1 and G3

- System administrators:

  Use the Change Password screen to change the login password.

  1. Log in as **cust**, or for G3V3 or later, as the customer superuser login you have defined.
  2. Enter **change password <login>**, where <login> is the login you want to change.

     For example, if you want to change the login password for **cust**, enter **change password cust** and then press **Return**.
  3. Verify that the screen displays the Password Administration screen.

     The cursor is positioned on the `Your Current Password` field.
  4. Enter the password of the login you logged in with, then press **Return**.

     The cursor is now positioned on the `New Password for Login Name` field.
  5. Enter the new password you want to be associated with the login you're changing, then press **Return**.

     The cursor is now positioned on the `New Password (enter again)` field.
  6. Enter the new password (from the previous step) again, then press **Return**.
  7. Verify that the screen displays:

     `command successfully completed`

- End users:

  Use the Change Password screen to change the login password.

  1. Verify that the screen displays:

     `command:`
  2. Enter **change password <login>**, where <login> is the login you want to change.

     For example, if you want to change the login password for **dopg1**, enter **change password dopg1** and then press **Return**.
  3. Verify that the screen displays the Change Password screen.

     The cursor is positioned on the `Your Current Password` field.

4. Enter your current password, then press **Return**.

   The cursor is now positioned on the `New Password for Login Name` field.

5. Enter your new password, then press **Return**.

   The cursor is now positioned on the `New Password (enter again)` field.

6. Enter your new password again, then press **Return**.
7. Verify that the screen displays:

   `command successfully completed`

DEFINITY G2

For DEFINITY G2, passwords are shared between the customer and Avaya. Contact the Database Administration group at the TSC for help in changing your password on these systems.

Avaya INTUITY System

- System administrators:

  Logins for both the system administrator (**sa**) and the voice messaging (**vm**) (AUDIX Voice Mail System) administrator come with a default password. AUDIX Voice Mail System administrators who log in with the **vm** login can change the password for the **vm** login only. System administrators who log in with the **sa** login can change the password for the **sa** login and the **vm** login.

  — AUDIX Voice Mail System password

  To change your AUDIX Voice Mail System password, type **change password** and follow the prompts.

  — System password

  1. Access the Avaya INTUITY System administration menu and select the following sequence of choices:

     Customer/Services Administration

     System Management

     UNIX Management

     Password Administration

  2. Select the login whose password you would like to change from the Password Administration screen.
  3. Enter **y** to confirm you want to change the password for the login selected.

4. Enter your new password at the following prompt:

   `New password`

   Passwords must be at least six characters.
5. Enter the new password again at the following prompt:

   `Re-enter new password`
6. Press **Cancel** to return to the UNIX Management screen.

- End users:
  1. Press **5** at the main AUDIX Voice Mail System menu.
  2. Follow the prompts to change your password.

MERLIN MAIL or MERLIN MAIL-ML Voice Messaging System

NOTE:
No default password is initially assigned for the system administrator, system administration password, or a new user. When prompted for the password, press **#.** After you have successfully logged in, the system will prompt you to change the password. Follow the prompts to change the password.

- System administrators:
  1. Dial the MERLIN MAIL or MERLIN MAIL-ML Voice Messaging System or press a programmed button.
  2. Enter the system administrator mailbox number (initially 9997) and press #.
  3. Enter the system administrator password (initially 1234) and press #.
  4. Press **5** and follow the prompts to change the password.
- End users:
  1. Dial the MERLIN MAIL or MERLIN MAIL-ML Voice Messaging System or press a programmed button.
  2. Enter your mailbox number and press #.
  3. Enter your password and press #.
  4. Press **5** and follow the prompts to change your password.

MERLIN MAIL R3, MERLIN LEGEND Mail, or PARTNER MAIL R3 Voice Messaging System

- System administrators:

  You can change two passwords: 1) the system administrator's mailbox password, and 2) the system administration password.

  — The System Administrator's Mailbox Password

  1. Dial the MERLIN MAIL R3, MERLIN LEGEND Mail, or PARTNER MAIL R3 Voice Messaging System or press a programmed button.
  2. Enter the system administrator mailbox number (initially 9997) and press #.
  3. Enter the system administrator mailbox password and press #.
  4. Press 5 and follow the prompts to change the password.

  — The System Administration Password

  1. Dial the MERLIN MAIL R3 Voice Messaging System or press a programmed button.
  2. Enter the system administrator mailbox number (initially 9997) and press #.
  3. Enter the system administrator's mailbox password and press #.
  4. Press 9 to access system administration.
  5. Enter the system administration password and press #.
  6. Press 8 for system security.
  7. Press 4 and follow the prompts to change the password.

- End users:

  1. Dial the MERLIN MAIL R3, MERLIN LEGEND Mail, or PARTNER MAIL R3 Voice Messaging System or press a programmed button.
  2. Enter your mailbox number and press #.
  3. Enter your password and press #.
  4. Press 5 and follow the prompts to change your password.

PARTNER MAIL System

- System administrators:

  Change your password by means of the Voice Mail menu.

  1. To access this menu, press Intercom 777 or a programmed button.
  2. Enter your mailbox number (initially 9997) and press #.
  3. Enter your password (initially 1234) and press #.
  4. Press 5 and follow the prompts to change your password.

- End users:

  Change your password by means of the Voice Mail menu.

  1. To access this menu, press Intercom 777 or a programmed button.
  2. Enter your mailbox number (initially 9997) and press #.
  3. Enter your password and press #.
  4. Press 5 and follow the prompts to change your password.

PARTNER MAIL VS System

- System administrators:

  Change your password by means of the Voice Mail menu.

  1. To access this menu, press Intercom 777 or a pre-programmed button.
  2. Enter 99#.
  3. Enter your password and press #. (The factory-set password is 1234.)
  4. Press 5 and follow the prompts to change your password.

- End users:

  Change your password by means of the Voice Mail menu.

  1. To access this menu, press Intercom 777 or a pre-programmed button.
  2. Enter your mailbox number and press #.
  3. Enter your password and press #.
  4. Press 5 and follow the prompts to change your password.

System 25

- System administrators:

  1. From the Main Menu prompt, enter **4**.
  2. At `Action =` enter **75**.
  3. At `Data =` enter the new password.

     For security, the display always shows????????. The default is **systemx5**.

     NOTE:
     The password reverts to the default when the system cold starts. The following message is displayed when a cold start occurs:

     ```
     WARNING: Default Password in effect.
     ```

- End users:

  None

System 75

- System administrators:

  Use the Change Password screen to change the login password.

  1. Log in as **cust**.
  2. Enter **change password <insert>**, where <insert> is the login you want to change.

     For example, if you want to change the login password **cust**, enter **change password cust** and then press **Return**.
  3. Verify that the screen displays the Change Password screen.

     The cursor is positioned on the `Your Current Password` field.
  4. Enter the password of the login you logged in with, then press **Return**.

     The cursor is now positioned on the `New Password for Login Name` field.
  5. Enter the new password you want to be associated with the login you are changing, then press **Return**.

     The cursor is now positioned on the `New Password (enter again)` field.

6. Enter the new password (from the previous step) again, then press **Return**.
7. Verify that the screen displays:

   `command successfully completed`

- End users:

  Use the Change Password screen to change the login password.

  1. Verify that the screen displays:

     `command:`

  2. Enter **change password <insert>**, where <insert> is the login you want to change.

     For example, if you want to change the login password for **dopg1**, enter **change password dopg1** and then press **Return**.

  3. Verify that the screen displays the Change Password screen.

     The cursor is positioned on the `Your Current Password` field.

  4. Enter your current password, then press **Return**.

     The cursor is now positioned on the `New Password for Login Name` field.

  5. Enter your new password, then press **Return**.

     The cursor is now positioned on the `New Password (enter again)` field.

  6. Enter your new password again, then press **Return**.
  7. Verify that the screen displays:

     `command successfully completed`

System 85

For System 85, passwords are shared between the customer and Avaya. Contact the Database Administration group at the TSC for help in changing your password on these systems.

Toll fraud job aids

15

NOTE:
Unless specifically stated otherwise, references in this document to “G3Vx and later” include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

The job aids in this appendix are tools for your organization to use in securing your system against toll fraud. Copy them and distribute them to your staff to post or use in any other manner that meets their needs.

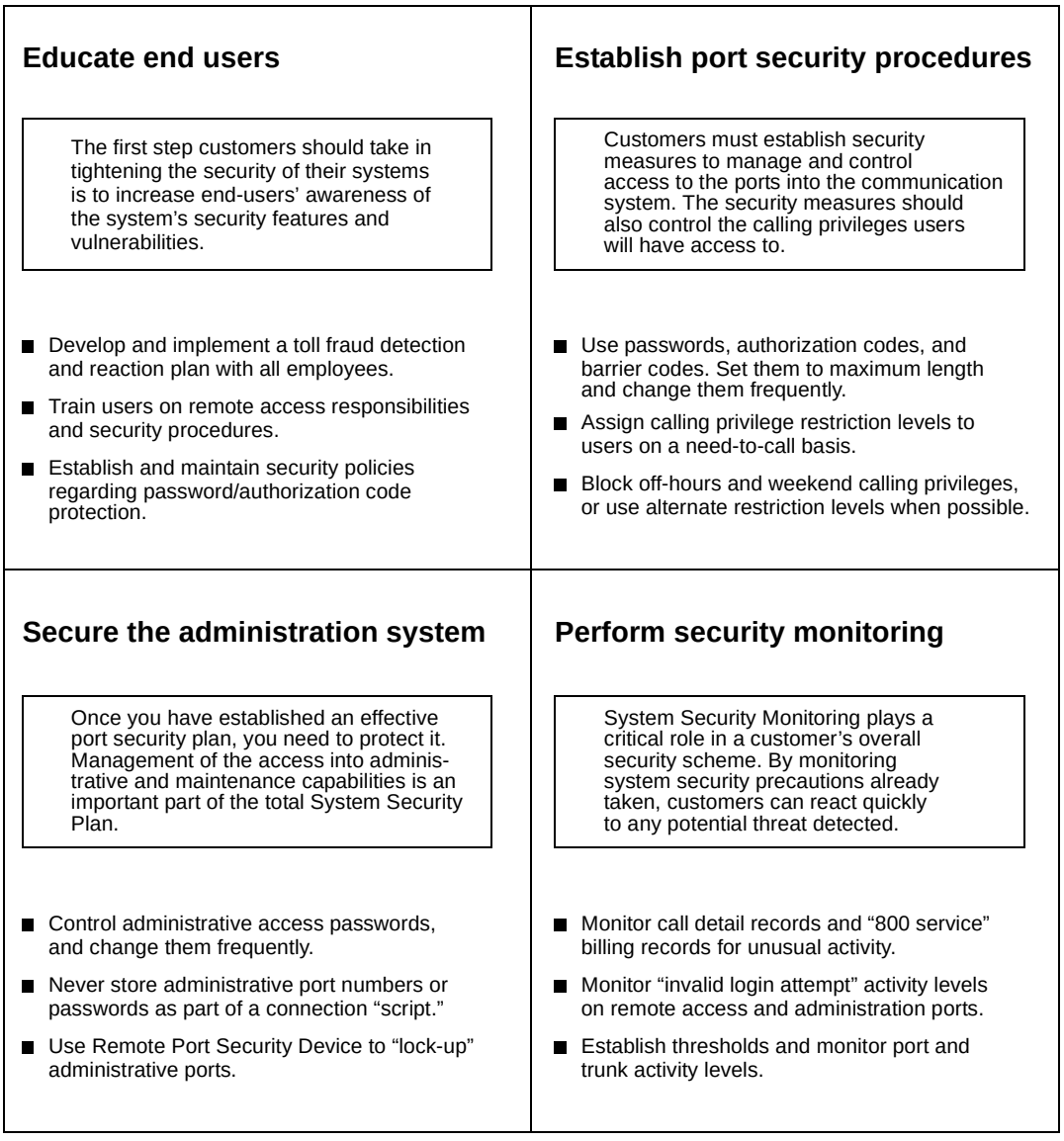
Toll fraud warning signs

- Customers or employees complain that the 800 number is always busy. The busy line could even impact local DID lines.
- Switchboard operators complain of frequent hang-ups or touch-tone sounds when they answer.
- Significant increase in “internal” requests for “operator assistance” in making outbound calls, particularly international ones.
- Unexplained increase in long distance usage.
- Increase in short duration calls.
- Heavy call volume on nights, weekends, and/or holidays.
- Station message detail recording (SMDR) shows an unusual amount of short duration calls.
- Established thresholds on trunk groups are exceeded.
- Switchboard operators note or complain about frequent calls from individuals with foreign accents.
- Staff or customer complaints of inability to enter voice mail system.
- Any attempts by outsiders to obtain sensitive information regarding the telecommunications system or calls from individuals posing as employees when they clearly are not.

- Sudden or unexplained inability to access specific administrative functions within the system.
- Employees complain of difficulty in obtaining an outside line.
- Simultaneous direct inward system access (DISA) authorization code use coming from two different places at the same time.
- An upsurge in use on DISA or other trunks.
- Unusual increase in customer premises equipment-based system memory usage.
- Unexplained changes in system software parameters.
- Unexplained problems related to being “locked out” of the system or PIN changes in the voice mail system.
- Significant increase in calls from a single geographic area or from the same automatic number identification (ANI).
- Any discrepancies in telephone bills, such as unusual calling patterns, calls to international locations with which the user does not normally interact, and calls for which you cannot account.

System security action plan

Figure 15-1. System security action plan



Ten tips to help prevent phone fraud

- **Protect system administration access**

  Insure secure passwords exist for all logins that allow system administration or maintenance access to the system. Change the passwords frequently.

- **Prevent voice mail system transfer to dial tone**

  Activate “secure transfer” features in voice mail systems.

  Place appropriate restrictions on voice mail access/egress ports.

- **Deny unauthorized users direct inward system access (remote access)**

  If you are not using Remote Access features, deactivate or disable them.

  If you are using remote access, require the use of barrier codes and/or authorization codes set for maximum length. Change the codes frequently.

- **Place protection on systems that prompt callers to input digits**

  Callers should be prevented from dialing unintended digit combinations at prompts.

  Auto attendants and call vectors should be restricted from allowing access to dial tone.

- **Use system software to intelligently control call routing**

  Create ARS or WCR patterns to control how each call is to be handled.

  Use “Time Of Day” routing capabilities to limit facilities available on nights and weekends.

  Deny all end-points the ability to directly access outgoing trunks.

- **Block access to international calling capability**

  When international access is required, establish permission groups.

  Limit access to only the specific destinations required for business.

- **Protect access to information stored as voice**

  Password restrict access to voice mail mailboxes.

  Use non-trivial passwords and change passwords regularly.

- **Provide physical security for telecommunications assets**

  Restrict unauthorized access to equipment rooms and wire connection closets.

  Protect system documentation and reports data from being compromised.

- **Monitor traffic and system activity for normal patterns**

  Activate features that “Turn Off” access in response to unauthorized access attempts.

  Use Traffic and Call Detail reports to monitor call activity levels.

- **Educate system users to recognize toll fraud activity and react appropriately**

  From safely using calling cards to securing voice mailbox passwords, users need to be trained on how to protect themselves from inadvertent compromises to the system’s security.

Special security product and service offers

16

NOTE:
Unless specifically stated otherwise, references in this document to "G3Vx and later" include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

Remote port security device

The remote port security device (RPSD)[1] offers enhanced protection for dial-up data access. Communications systems typically consist of a mix of digital PBXs, voice mail systems, and adjunct applications computers. Dial-up ports on these systems provide remote access for maintenance and administration support. They also provide potential access to the hackers or thieves who use easily obtainable computers and software to gain unauthorized access to your systems.

NOTE:
Since the RPSD contains a Data Encryption Standard (DES) algorithm, its use outside the United States and Canada is prohibited by law.

Once a hacker gains access to your systems, he or she can explore sensitive information, disrupt voice and data communications, and manipulate software applications. This access can result in unauthorized use of network facilities and the theft of long distance services.

While effective system security management can usually stop the hacker, the Avaya Remote Port Security Device (RPSD) gives you a state-of-the-art single channel protection system that enhances your ability to prevent unauthorized users or hackers from accessing your system's dial-up communications ports.

1. The RPSD is compatible with: DEFINITY ECS, DEFINITY communications systems, System 75 (V2 or higher), System 85 and DIMENSION PBX Systems; the AUDIX, DEFINITY AUDIX, and AUDIX Voice Power Systems; and all System Management products.

Dial-up ports provide access to data networks and computers that contain critical data and software applications. While these ports help to improve productivity and increase customer satisfaction, they also provide potential access to hackers.

The “key and lock” authentication process uses a sophisticated dynamic challenge/response technique to assist you in preventing unauthorized access to your administration and maintenance ports. This authentication process is as follows:

- The lock answers the incoming call destined for the dial-up modem port. It generates a dynamic challenge, unique to every call, and transmits it to the RPSD installed at the calling end. The lock and key must be initialized with the same secret encryption key value. This secret encryption key has approximately 70 quadrillion combinations.
- When the RPSD key receives the challenge, it generates a response using the secret encryption key. It then transmits the expected response back to the RPSD lock. If the RPSD lock successfully authenticates the response, it provides ringing to the terminating modem and the call completes. The RPSD terminates a call immediately if any step in the challenge/response authentication process is not completed successfully.

The RPSD helps to:

- Protect remote locations that communicate with a central network via dial-up lines
- Safeguard companies that remotely administer PBX and voice mail systems
- Ensure that critical network routing information and PBX feature translations are not compromised
- control access of dial-up ports by remote maintenance or service personnel

Key and lock features

- Uses randomly-generated encrypted data to perform key/lock authentication handshake.
- Time of Day/Day of Week restrictions can control key access to locks. Each user profile can have up to 14 restrictions set.
- History logs provide audit trails of the last 500 administrative changes, accesses, and failures.
- System administration provides menu-driven commands with online help and security options for administrative access.
- Self-check and built-in diagnostics enable simple and fast problem diagnosis.

- A power monitor circuit allows you to fail or bypass calls to the lock during a power failure.
- An alarm contact closure interface is provided to generate an alarm when the lock loses power.

Lock and keys work with all data communications protocols.

Securing DEFINITY Systems (prior to Release 7.2) with the remote port security device

If your telephones are connected to a DEFINITY switch or DEFINITY ECS prior to Release 7.2 (which is the same as DEFINITY G3V7.2), you may wish to use a remote port security device. (Note that this lock and key system is available only in the United States.) The RPSD hardware offers enhanced protection for dial-up data access so that hackers and other unauthorized users cannot gain access to your systems.

NOTE:
Specifically, the RPSD can be used with Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY communications systems, System 75 (V2 or higher), System 85 and DIMENSION PBX Systems; the AUDIX, DEFINITY AUDIX, and AUDIX Voice Power Systems; and all System Management products

DANGER:
IMPORTANT NOTE: Since the RPSD contains a Data Encryption Standard (DES) algorithm, its use outside the United States and Canada is prohibited by law.

On the RSPD, the lock and key authentication process is as follows:

- The lock answers the incoming call destined for the dial-up modem port. It generates a dynamic challenge, unique to every call, and transmits it to the RPSD installed at the calling end. The lock and key must be initialized with the same secret encryption key value. This secret encryption key has approximately 70 quadrillion combinations.
- When the RPSD key receives the challenge, it generates a response using the secret encryption key. It then transmits the expected response back to the RPSD lock. If the RPSD lock successfully authenticates the response, it provides ringing to the terminating modem and the call completes. The RPSD terminates a call immediately if any step in the challenge/response authentication process is not completed successfully.

For more information about the RPSD hardware, see the *DEFINITY® Communications System Remote Port Security Device User's Manual,* 555-025-400.

Avaya support

Avaya provides RPSD keys to their maintenance centers to accommodate access to systems you secure with the RPSD lock.

For more information on the RPSD, see the *DEFINITY® Communications Systems Remote Port Security Device User's Manual*.

Securing DEFINITY systems (Release 7.2 and Later) with Access Security Gateway

The Access Security Gateway (ASG) integrates challenge/response technology into Avaya products and is available, beginning with the DEFINITY ECS Release 7.2 (that is, DEFINITY G3V7.2), to secure the DEFINITY switch administration and maintenance ports and logins and thus reduce the possibility of unauthorized access to the system.

The challenge/response negotiation starts after you have established an RS-232 session and have entered a valid Communication Manager, MultiVantage™ Software, or DEFINITY ECS login ID. The authentication transaction consists of a *challenge*, issued based on the login ID that you have just entered, followed by the expected *response*, which you must enter. The core of this transaction is a secret key, which is information-possessed by both the lock (ASG) and the key. Interception of either the challenge or response during transmission does not compromise the security of the system. The relevance of the authentication token used to perform the challenge/response is limited to the current challenge/response exchange (session).

Currently-supported keys consist of a hand-held token generating device (ASG key). The ASG key (response generator) device is pre-programmed with the appropriate secret key to communicate with corresponding ASG-protected login IDs on Communication Manager, MultiVantage™ Software, and DEFINITY ECS.

ASG administration parameters specify whether access to the system administration or maintenance interface requires ASG authentication. This security software can be assigned to all system administration maintenance ports or to a subset of those ports. If the port being accessed is not protected by ASG, the standard DEFINITY login and password procedure will be satisfactory for the user to enter the system.

For more information about Access Security Gateway and required ASG forms, see the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506.

NOTE:
ASG does not protect login access to a multiple application platform for DEFINITY (MAPD).

Administering the Access Security Gateway

Use the following procedure to administer the ASG.

1. On the Optional Features (**change system-parameters customer-options**) screen, do the following:

   NOTE:
   Only Avaya technicians can access this screen.

   - Set the `G3 Version` field to **V6** or later configuration.
   - Set the `Access Security Gateway (ASG)` field to **y**.

2. On the Login Administration screen, do the following:

   - On page 1 of this screen, set the `Access Security Gateway` field to **y**.
   - On page 2, complete one of these two options for the `Secret Key` field:
     - — If you are using a system-generated secret key, set the `System Generated Secret Key` field to **y**

       or

     - — If you are using a self-defined secret key, enter your unique secret key in the `Secret Key` field.

   NOTE:
   All other fields on page 2 of the Login Administration screen are optional.

3. On the Security Related System Parameters screen, set the required `ACCESS SECURITY GATEWAY PARAMETERS` fields to **y**.
4. When you have completed all entries on these screens, press **Enter** to save your changes.

Logging in via Access Security Gateway (session establishment)

Use the following procedure to log in to the system via the ASG interface:

NOTE:
The numbers shown as challenges and responses in the procedures below are for example purposes only. They will not be the numbers you actually use or see on your ASG Key.

1. Connect to the system administration/maintenance port.

   The system responds with the login prompt.

2. At the prompt, type your valid login ID and press **Return**.

   The system verifies the login ID and transmits the challenge in the form of a 7-digit number (for example, **5551234**).

3. Turn on your ASG key, press the button labeled **Red** to enter authentication mode, type your PIN, and press **Enter**.

   The ASG key responds with a challenge prompt.

4. On the ASG key, at the challenge prompt, type the 7-digit challenge number you see on your PC (leave out the "-", for example, **5552739**) and press **Enter**.

   The ASG key generates a response number (for example, **999-6713**).

5. On the PC, at the `Response` prompt, type the response number generated by the ASG key (leave out the "-", for example, **9996713**) and press **Return**.

   The system verifies the response. If correct, DEFINITY logs you on. If the response is incorrect, return to Step 1.

NOTE:
Three login/challenge/response attempts are permitted. If the user is not authenticated after the third response, the user sees the message `INVALID LOGIN` and the session will be terminated. If this happens, see the appropriate maintenance book for your system.

Maintaining login IDs

Temporarily disabling Access Security Gateway access for login

To temporarily disable ASG:

1. At the prompt, type **change login xxxx** (xxx = alphanumeric login ID) and press **Return** to log into the Login Administration screen.
2. On page 2 of the Login Administration screen, set the `Blocked` field to **y**.

   NOTE:
   Setting the `Blocked` field to **y** does not remove the login from the system, but temporarily disables the login.

3. Press **Return** to save your changes.

Restarting temporarily disabled ASG access for login

1. At the prompt, type **change login xxxx** (xxx = alphanumeric login ID) and press **Return** to log into the Login Administration screen.
2. On page 2 of the Login Administration screen, set the `Blocked` field to **n**.
3. Press **Return** to save your changes.

Maintaining the ASG history log

The ASG history log logs all session establishment and rejection events associated with users accessing the system administration and maintenance interface through ASG. This log emulates the information provided in the DEFINITY, MultiVantage™ Software, or Communication Manager history log, but also contains information on whether the session was accepted or rejected by ASG, and if rejected, the reason for the rejection.

This screen is accessible only if the `G3 Version` field on the System-Parameters Customer-Options screen is **V6** or greater and the `Access Security Gateway (ASG)` field on the screen is set to **y**.

Loss of an ASG key

Users who lose their ASG key must notify the system administrator immediately. The administrator, in turn, must do the following:

- Modify any logins associated with the lost ASG key. See the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506. for information on changing your PIN.
- If the login is no longer valid, at the prompt, type **remove login xxxx** (xxx = alphanumeric login ID) and press **Return** to remove the invalid login from the system.
- To keep the same login, change the secret key associated with the login to a new value.
- Using the new secret key value, re-key devices that generate responses and interact with the login.

Interactions of ASG

- Customer access INADS port

  If access to the INADS port is disabled on a system-wide basis, administering access to the SYSAM-RMT or INADS port through the ASG feature does not override the INADS port restriction. Administration does not prohibit assignment of ASG to the SYSAM-RMT or INADS port. However, in a configuration where this method of access is blocked, you will be denied access to the system through the SYSAM-RMT or INADS port even if you attempt to access the port using a valid ASG login ID.

  If access to the INADS port has been disabled on a login basis, administering access to the SYSAM-RMT or INADS port via the ASG feature will not override the INADS port restriction.

- Login administration

  The standard user interface for Communication Manager, MultiVantage™ Software, and DEFINITY ECS login administration has not been modified by ASG. Also, the standard login user interface is maintained in cases where ASG parameters have not been administered for the login.

- Security violation notification (SVN)

  ASG does not support an interface to the SVN feature. Session rejection events do not appear in the monitor security-violations login report and referral calls are not spawned in the event that the number of rejected ASG sessions exceeds the threshold/time interval criteria imposed by the SVN feature.

- Security measurements

  ASG session establishment or reject events do not increment the successful logins, invalid attempts, invalid IDs, forced disconnects, login security violations or trivial attempts counters maintained for the Security Violations Detail report. Additionally, login-specific information maintained by the Security Violations Summary report does not include ASG-related data.

Securing INTUITY AUDIX ports (Release 5.0 and later) with ASG

ASG also provides up-to-date authentication for the Intuity AUDIX system logins. For Intuity Release 5.0, ASG protection is available for remote dial-up logins only.

ASG protects Intuity AUDIX systems by challenging each potential dial-up session user. If an ASG login ID is established for a particular user (such as **sa**, which refers to a login for the "system administrator," or **vm**, which refers to the login of the "voice messaging administrator"), the ASG layer of protection is in place for anyone who attempts to log in as that user. If an ASG login ID is not established for a particular user, the user logs in to the system with the UNIX system password.

NOTE:
Information about ASG with Intuity and procedures for administering and using ASG can be found on the Intuity Messaging Solutions documentation CD. There, do a search within the index for "Access Security Gateway (ASG)."

In order to respond to the ASG challenge, the user must have a hand-held device called the ASG key. The ASG key must be set with an encryption key number that matches that of the user's ASG encryption key number in the Intuity AUDIX system. For more information about the ASG Key, see the *Administrator's Guide for Avaya™ Communication Manager*, 555-233-506.

Use the following procedures for logging in with ASG, maintaining login IDs, and setting and resolving violation warnings.

Logging in with ASG

When you begin a remote session with an Intuity AUDIX system that is ASG-activated, the system prompts you with a challenge. To log in to a system that has ASG activated for your login:

1. At the `login:` prompt, enter your login ID.

   The terminal screen displays the following message:

   ```
   Challenge: xxxxxxx
   Response:
   ```

2. Press **Enter** on the ASG key.

   The ASG key displays the following message:

   ```
   PIN:
   ```

3. On the ASG key, type your PIN and press **Enter**.

4. On the ASG key, type the challenge number that is displayed on the terminal screen, and press **Enter**.

   The ASG key displays the unique 7-digit response number that corresponds to the challenge number you entered. The challenge and response numbers are valid for this session only.

5. On the terminal screen, at the `Response:` prompt, enter the response number that is displayed on the ASG key.

NOTE:
If the authentication process is successful, the system displays the INTUITY Main Menu for the **sa** login or the AUDIX Command Prompt screen for the **vm** login. If the authentication process fails, the system makes an entry in the system history log and displays the message `INVALID LOGIN.`

Maintaining login IDs

Once you establish an ASG login for a specific Intuity AUDIX login user, sa or vm, anyone who attempts remote access to your system with the protected login is prompted for the challenge response number.

Adding an ASG login

You must be logged in as sa to add an ASG login for **sa** or **vm**. To add a new ASG login to your system:

1. At the INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration screen.

2. Complete the following fields:

   - `Login ID:`

     Type either **sa** or **vm**.

   - `Access Via ASG Blocked?`

     Set this field to **N**, which indicates that the login ID should have full access privileges.

   - `Authentication Type?`

     Type **PASSKEY**, which indicates that the user must have the ASG key to produce the unique response number during login.

     NOTE:
     If you type **PASSWORD** (rather than **PASSKEY**) in the `Authentication Type:` field, the system will use regular Intuity AUDIX password protection.

   - `System Generated Secret?`

     Set this field to **Y** for Yes or **N** for No. **Y** indicates that you want the system to create the secret key for this login ID. **N** indicates you will provide the secret key number in the `Secret Key:` field.

3. If you typed **N** in the `System Generated Secret?` field, complete the `Secret Key:` field.

   A secret key is a 20-digit string using only the digits 0 through 7 in any order.

4. Press **F2** (**Create**) to save the information.

   The system displays a confirmation message and provides the encryption key number that must match the ASG key when a user attempts to log in. The encryption key number must be entered into the ASG key as Key1 or Key2.

5. Press **Enter**, then press **F6** *(***Cancel***)* twice to return to the INTUITY Main Menu.

Blocking or reinstating access privileges for an ASG login

If a user will not need access to the system for a long period of time, you can block the ASG login ID's access temporarily. Perform the following tasks to block or reinstate access for an ASG login.

1. At the INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration screen.

2. Type the user's login ID in the `Login ID:` field.
3. Set the `Access Via ASG Blocked?` field to **Y** if you want to revoke the user's access to the system, or **N** if you want to reinstate the user's access to the system.
4. Press **F3** (**Change**) to save the changes.

   The system displays a confirmation message.

5. Press **Enter**, then press **F6** (**Cancel**) twice to return to the INTUITY Main Menu.

Changing the encryption key number for an ASG login

The encryption key number is used by the system and by the ASG key hand-held device to create challenge response pairs of numbers. If an encryption key number is lost or compromised, it must be changed in the system and in all associated ASG key hand-held devices.

To change the encryption number.

1. At the INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration screen.

2. Type the user's login ID in the `Login ID:` field.
3. Set the `System Generated Secret?` field to **Y** if you want to want the system to generate a unique Secret Key number, or **N** if you want to enter your own Secret Key number.
4. If the `System Generated Secret?` field is set to **N**, complete the `Secret Key:` field.

   A secret key is a 20-digit string, using only the digits 0 through 7 in any order.

5. Press **F3** (**Change)** to save the changes.

   The system displays a confirmation message and provides the challenge response number that the user will need to log in to the system.

6. Press **Enter**, then press **F6** (**Cancel**) twice to return to the INTUITY Main Menu.

Displaying ASG login information

If you need to check on the status of an ASG login, perform the following tasks to display the ASG Display screen.

1. At the INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration screen.

2. Type the user's login ID in the `Login ID:` field.

3. Press **F4** (**Display**) to display information about the ASG login ID.

   The system displays the ASG Display screen.

4. Press **Enter**, then press **F6** (**Cancel**) twice to return to the INTUITY Main Menu.

Disabling ASG authentication

If you want to discontinue ASG protection for a particular login, change the `Authentication Type` to **password**. To disable ASG authentication:

1. At the INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration screen.

2. Type the user's login ID in the `Login ID:` field.

3. Type **PASSWORD** in the `Authentication Type?` field.

4. Press **F3** (**Change**) to save the information.

   The system displays a confirmation message.

5. Press **Enter**, then press **F6** (**Cancel**) twice to return to the INTUITY Main Menu.

Setting and resolving violation warnings

ASG tracks the number of unsuccessful login attempts and the time between unsuccessful login attempts. If someone exceeds the allowed number of failed login attempts, a warning is added to the alarm log.

Setting notification limits

To set alarm parameters for ASG:

1. At the INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Violation Warning Administration.`

   The system displays the ASG Security Violation Warning Administration screen.

2. Type a new value in the `Number of failed login attempts:` field, if needed.

   This number can be from 1 to 99, and indicates the number of times that the user can incorrectly type the login information before the system places an entry in the alarm log and disallows further login attempts.

   NOTE:
   A lower number in this field protects the system more fully.

3. Type a new value in the `Failed login measurement window:` field, if needed.

   This number can be from 1 through 60, and indicates the maximum time, in minutes, that may elapse between failed login attempts, but still have the attempt count as one in a series.)

   NOTE:
   A higher value in this field protects the system more fully.

4. Press **F3** (**Save**) to save the changes.

   The system displays the following confirmation message:

   ```
   Assignment made
   Press Enter to continue.
   ```

5. Press **Enter**, then press **F6** (**Cancel**) twice to return to the INTUITY Main Menu.

Resolving ASG violation alarms

To resolve an ASG warning, follow these steps:

1. At the INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Violation Warning Administration.`

   The system displays the ASG Security Violation Warning Administration screen.

2. Set the `Resolve existing alarms?` field to **Y**.

   Y indicates that you want to resolve an active ASG alarm.

3. Press **F3** (**Save**) to save the changes.

   The system displays the following confirmation message:

   ```
   Assignment made
   Press Enter to continue.
   ```

3. Press **Enter**, then press **F6** (**Cancel**) twice to return to the INTUITY Main Menu.

Avaya support

Avaya provides RPSD keys to their maintenance centers to accommodate access to systems you secure with the RPSD lock.

With DEFINITY Release 7.2 and Intuity Release 5.0, the services area of Avaya has been modified to accommodate the ASG feature. However, note that, unlike the RPSD lock feature which requires access through a hardware RPSD key at the services site, negotiating the system through ASG is accomplished through a software interface to the INADS “connect” tool. Other desktop and laptop tools are also available to Avaya engineers and technicians to access the Avaya system via ASG.

HackerTracker

HackerTracker alerts you to abnormal calling activities. You can program the software to continually monitor all incoming calls and watch for hallmarks of hacker activity. Call detail activity is marked against a set of pre-established threshold criteria, and if these thresholds are exceeded, alarms and alerts are sent to designated security system administrators. HackerTracker is designed to work in conjunction with Avaya’s Call Accounting System (CAS Plus Version 3).

For more information, call **1 800 521-7872**.

Security Tune-Up Service

The Security Tune-Up Service is a fee-based, consultative service designed to provide an expedient, on-line review of your system security as it relates to toll fraud. This service is provided for Communication Manager, MultiVantage™ Software, DEFINITY ECS, DEFINITY communications systems G1, G2, and G3, the DIMENSION PBX System, System 75, System 85; and the AUDIX, the AUDIX Voice Power, the DEFINITY AUDIX, and the INTUITY AUDIX Voice Messaging Systems.

Customer support engineers specializing in security will remotely access your system, analyze the potential risks in the system, and optionally implement agreed-upon changes to secure the system.

For more information, call **1 800 643-2353.**

Toll fraud contact list

Contact:	For:
Your Avaya account executive or design specialists	General questions related to toll fraud
Avaya Toll Fraud Intervention Hotline **800 643-2353**	All systems and products and their adjuncts. Immediate crisis intervention if you suspect that your company is experiencing toll fraud.
United States Secret Service (listed under Federal Government in your local telephone directory)	To file a legal complaint in the event of international or interstate toll fraud

Product security checklists

17

NOTE:
Unless specifically stated otherwise, references in this document to "G3Vx and later" include the specified DEFINITY G3 (and more recent) versions, DEFINITY ECS, MultiVantage™ Software, and Communication Manager.

This chapter contains the following security checklists:

- General security procedures (page 17-2)
- AUDIX Voice Mail System (page 17-4)
- AUDIX Voice Power System (page 17-6)
- BasicWorks (page 17-8)
- CONVERSANT Voice Information System (page 17-12)
- DEFINITY G1 (page 17-14), G2 (page 17-20), and G3 (page 17-14)
- DEFINITY AUDIX System (page 17-4)
- DIMENSION PBX System and Communication Manager, MultiVantage™ Software, and DEFINITY ECS (page 17-24)
- INTUITY AUDIX Voice Messaging System (page 17-4)
- MERLIN II Communications System (page 17-27)
- MERLIN LEGEND Communications System (page 17-29)
- MERLIN MAIL Voice Messaging System (page 17-32)
- MERLIN MAIL-ML Voice Messaging System (page 17-34)
- MERLIN MAIL R3 Voice Messaging System (page 17-36)
- MERLIN Plus Communications System (page 17-39)
- Messaging 2000 Voice Mail System (page 17-40)
- Multimedia Communications Exchange Server (page 17-45)
- Multipoint Conferencing Unit (MCU)/Conference Reservation and Control System (CRCS) (page 17-46)
- PARTNER II Communications System (page 17-56)

- PARTNER MAIL System (page 17-61)
- PARTNER MAIL VS System (page 17-61)
- PARTNER Plus Communications System (page 17-56)
- System 25 (page 17-63)
- System 75 (page 17-14)
- System 85 (page 17-20)
- PassageWay Telephony Services (page 17-66)

General security procedures

Customer: _____

Location: _____

System & Version: _____

Date Installed: _____

Table 17-1. General security procedures checklist

	Y/N[1]	Note	N/A
Physical Security Switch room and wiring closets locked			
All equipment documentation secured			
Attendant console secured at night; headset unplugged			
Local and Remote administration equipment secured			
Remote Port Security Devices installed			
Telephone logs and print reports secured			

Continued on next page

Table 17-1. General security procedures checklist — *Continued*

	Y/N[1]	Note	N/A
Adjunct (CAS, AUDIX Voice Mail System, CMS, ISII, G3MA ...) remote administration terminals secured			
Customer Education System manager/administrator has copy of *Avaya™ Toll Fraud and Security Handbook* (this document)			
System security policy established and distributed			
System security policy reviewed periodically			
Security policy included in new-hire orientation			
Employees know how to detect potential toll fraud			
Employees know where to report suspected toll fraud			
Authorization codes not sequential			
Remote access phone number not published			
Barrier codes and passwords are chosen to be difficult to guess			
Barrier codes, passwords (including voice mail), and authorization codes removed/changed when employees terminated			
Authorization codes, account codes, and passwords not written down or translated on auto-dial buttons			
Logins and passwords are not written down			
All customer passwords changed on regular basis			

Continued on next page

Table 17-1. General security procedures checklist — *Continued*

	Y/N[1]	Note	N/A
HackerTracker thresholds established			
Social engineering explained			
Customer is aware of network-based toll fraud surveillance offerings such as netPROTECT			
Customer knows how to subscribe to ACCESS security shared folder			

1. If "NO" (N), provide Note reference number and explain.

AUDIX, DEFINITY AUDIX and INTUITY AUDIX voice messaging systems

Also see the general security checklist on page 17-2, and the security checklist for the host communications system.

Customer: _____

PBX Type: _____

Location: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-2. AUDIX, DEFINITY AUDIX and INTUITY AUDIX voice messaging systems security checklist

	Y/N[1]	Note	N/A
System Administration Administration password changed from default			
User passwords 7 to 15 characters			
Forced password change for new subscribers			
System Features Only active subscribers translated			
Call transfer out of voice mail system not allowed			
If transfer allowed, Enhanced Call Transfer enabled			
If transfer allowed and basic transfer enabled, transfer restricted to subscribers (DEFINITY AUDIX and INTUITY AUDIX voice messaging systems only)			
If transfer allowed, number restrictions administered (DEFINITY AUDIX Voice Messaging System 3.2 only)			
*T not allowed on auto attendants			
Retries before lockout < 6			
Retries before disconnect < 4			
Busy lamp on modem port			
Voice processing ports restricted from toll calls by host PBX, for example, restricted COR			
Outcalling not used			

Continued on next page

Table 17-2. AUDIX, DEFINITY AUDIX and INTUITY AUDIX voice messaging systems security checklist

	Y/N[1]	Note	N/A
Number of digits on outcalling minimized, and/or outcalling destination restricted by host PBX			
Voice processing ports COR-to-COR restricted from dialing remote access barrier codes (when host communications system is System 75, Communication Manager, MultiVantage™ Software, DEFINITY ECS, or DEFINITY G1 or G3)			
Product Monitoring Administration log and activity log checked daily			

1. If “NO” (N), provide Note reference number and explain.

AUDIX Voice Power System

Also see the general security checklist on page 17-2, the security checklist for the host communications system.

Customer: _____

PBX Type: _____

Location: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-3. AUDIX Voice Power System security checklist

	Y/N[1]	Note	N/A
System Administration Administrative login name changed from default			
All UNIX login passwords changed from default			
System Features Only active subscribers translated			
Call transfer not allowed			
If call transfer enabled, transfer to subscriber enabled			
Passwords changed from default for all subscribers			
Retries before lockout < 6			
Retries before disconnect < 4			
Outcalling inactive			
Number of digits on outcalling minimized, or outcalling destination restricted			
Invalid automated attendant menu options directed to operator or security			
Voice processing ports on host PBX system restricted from toll calls			
Voice processing ports restricted from dialing remote access extension			
Product Monitoring Administration log and activity log checked daily			
End-User Education Passwords changed from default for new subscribers			
Administrator instructed to change administration login password regularly			

1. If “NO” (N), provide Note reference number and explain.

BasicWorks

Also see the general security checklist on page 17-2.

Customer: _____

System & Version: _____

Location: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-4. BasicWorks security checklist

	Y/N[1]	Note	N/A
System Administration Customer advised of all logins under their control. Passwords changed from factory defaults.			
Passwords are customer-entered, maximum length, and unique alphanumeric words.			
NETCON access restricted by COR-to-COR restrictions			
NETCON channels secured			
Non-DID extensions used for NETCON ports			
Unused NETCON channels removed			
Login Security Violation Notification feature active ■ Logins automatically disabled after security violation ■ Login security violations monitored 24 hours per day			
Login permissions customized			
Unused logins removed (“remove login” command or disabled [passwords VOIDed])			

Continued on next page

Table 17-4. BasicWorks security checklist — *Continued*

	Y/N[1]	Note	N/A
Unique customer logins used			
Password aging activated			
Logins temporarily disabled when not needed (“disable/enable” commands)			
Customer access to INADS port disabled ■ Adjunct connectivity (TroubleTracker, Monitor I, SNMP, and G3MA) to access the switch through the INADS port established			
Remote Access Remote access permanently disabled			
Remote access administered ■ Remote access number is unpublished ■ Non-DID remote access number used ■ Barrier codes are random 7-digit sequences ■ Barrier codes in own restricted COR ■ Voice processing ports COR-to-COR restricted from dialing remote access barrier codes ■ Remote Access Security Violation Notification feature active — Remote access security violations monitored 24 hours per day — Remote access automatically disabled following detection of a security violation ■ Barrier code aging used ■ Remote access temporarily disabled when not needed (“disable/enable” commands)			
Logoff notification enabled for remote access			
PBX Features **Trunking** Prohibit trunk-to-trunk transfer on public access trunks			
Tie trunk groups are COR-to-COR restricted			

Continued on next page

Table 17-4. BasicWorks security checklist — *Continued*

	Y/N[1]	Note	N/A
Trunk groups have dial access = n			
COR-to-COR restrictions on dial-accessed trunks			
Automatic circuit assurance (ACA) on trunks groups			
SMDR/CDR activated on all trunk groups			
Attendant control of trunk groups with TAC = y			
Routing ARS/WCR used for call routing ■ 1+809 and 0+809 area code blocked ■ 900 and 976 calls blocked ■ 976 “look-alikes” blocked ■ Block access to Alliance teleconference service (0700) ■ 011/LD calls limited by FRLs ■ 011/LD calls limited by Time-of-Day routing ■ 011/LD calls limited by 6-digit or digit analysis ■ Alternate FRLs used (G3r)			
Facility Test Call/Data Origination Facility test code changed from default, if used ■ Facility test code translated only when needed ■ Facility test code limited to system admin/mtce COR ■ Logoff notification enabled for facility test call			
Data origination feature code not translated			
Miscellaneous Console permissions restricted/limited			
Individual and group-controlled restrictions used			
Authorization codes used			
Operator calls restricted			
Switch-hook flash denied on FAX machines, modems, etc.			

Continued on next page

Table 17-4. BasicWorks security checklist — *Continued*

	Y/N[1]	Note	N/A
COR-to-COR restrictions used on all CORs			
Ports for adjuncts in own restricted COR			
Restrict call forwarding off-net = y			
Digit conversion of unauthorized calls to console or security			
Three-way COR check on transfer/conference			
Authorization Code Security Violation Notification feature active			
Product Monitoring Traffic measurements reports monitored daily			
SMDR/CMS reports monitored daily			
Recent change history log reviewed daily			

1. If “NO” (N), provide Note reference number and explain.

CONVERSANT Voice Information System

Also see the general security checklist on page 17-2, and the security checklist for the host communications system.

Customer: _____

PBX Type: _____

Location: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-5. CONVERSANT Voice Information System security checklist

	Y/N[1]	Note	N/A
System Administration Administrative login name changed from default			
All UNIX login passwords changed from default			
Busy lamp on modem port			
Modem dial-up password administered			
System Features Customized scripts do not allow transfers			
Customized scripts limit transfers to specific extensions			

Continued on next page

Table 17-5. CONVERSANT Voice Information System security checklist — *Continued*

	Y/N[1]	Note	N/A
Host PBX Analog ports in CONVERSANT Voice Information System hunt group restricted from toll calls by host PBX, for example, restricted COR			
Analog ports in CONVERSANT Voice Information System hunt group COR-to-COR restricted from dialing remote access barrier codes (when host communications system is System 75, Communication Manager, MultiVantage™ Software, DEFINITY ECS, or DEFINITY G1 or G3)			
Product Monitoring System reports checked daily			

1. If “NO” (N), provide Note reference number and explain.

Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY G1 and G3, and System 75

Also see the general security checklist on page 17-2, and the security checklist for any attached voice mail systems or other adjuncts.

Customer: _____

Location: _____

System & Version: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-6. Communication Manager, MultiVantage™ Software, DEFINITY ECS, G1, and G3, and System 75 security checklist

	Y/N[1]	Note	N/A
System Administration Customer advised of all logins under their control			
Passwords changed from factory defaults			
Passwords are customer entered, maximum length, unique, nonsense alphanumeric words			
NETCON access restricted by COR-to-COR			
NETCON channels secured			
Non-DID extensions used for NETCON ports			
Unused NETCON channels removed			

Continued on next page

Table 17-6. Communication Manager, MultiVantage™ Software, DEFINITY ECS, G1, and G3, and System 75 security checklist — *Continued*

	Y/N[1]	Note	N/A
Login Security Violation Notification feature active			
Logins automatically disabled after security violations (G3V3 and later)			
Login permissions customized (G3V2)			
Unused logins removed (remove login command, (G3V3 and later) or disabled (passwords VOIDed)			
UNIQUE customer logins used (G3V3 and later)			
Password aging activated (G3V3 and later)			
Logins temporarily disabled when not needed (disable/enable commands) (G3V3 and later)			
If customer access to INADS port enabled, adjunct connectivity (TroubleTracker, Monitor I, SNMP and G3MA) to access the switch through the INADS port established (G3V4)			
Remote Access Remote access permanently disabled if not used (G3V2 and North American Dial Plan loads)			
Remote access administered			
Remote access number is unpublished			
Non-DID remote access number used			
Barrier codes are random 7-digit sequences			
Barrier codes in own restricted COR			
Seven-digit authorization codes used			

Continued on next page

Table 17-6. Communication Manager, MultiVantage™ Software, DEFINITY ECS, G1, and G3, and System 75 security checklist — *Continued*

	Y/N[1]	Note	N/A
Second dial tone omitted between barrier and authorization codes			
Authorization code timeout to attendant			
Voice processing ports COR-to-COR restricted from dialing remote access barrier codes			
Remote Access Security Violation Notification feature active			
Remote access security violations monitored 24 hours per day			
Login security violations monitored 24 hours per day			
Remote access automatically disabled following detection of a security violation (G3V3 and later)			
Barrier code aging used (G3V3 and later)			
Remote access temporarily disabled when not needed (disable/enable commands) (G3V3 and later)			
Logoff notification enabled (G3V4)			
PBX Features **Trunking** Prohibit trunk-to-trunk transfer on public access trunks			
Tie trunk groups are COR-to-COR restricted			
Trunk groups have dial access = n			
COR-to-COR restrictions on dial-accessed trunks			
ACA on trunk groups			
SMDR/CDR activated on all trunk groups			
Trunks measured by BCMS/CMS			

Continued on next page

Table 17-6. Communication Manager, MultiVantage™ Software, DEFINITY ECS, G1, and G3, and System 75 security checklist — *Continued*

	Y/N[1]	Note	N/A
Trunk-to-trunk transfer only allowed with DCS or CAS (G3V3 and later)			
`COS Trunk-to-Trunk Restriction Override` = **n** (Communication Manager, MultiVantage™ Software, DEFINITY ECS R5)			
Personal station access (PSA) (Communication Manager, MultiVantage™ Software, DEFINITY ECS R5) COS assignment limited to stations with need to access PSA			
8-digit security codes assigned to stations using PSA			
Station Security Code Security Violation Notification feature active ■ Station security code security violations monitored 24 hours per day			
Extended user administration of redirected calls (Communication Manager, MultiVantage™ Software, DEFINITY ECS R5) 8-digit security codes assigned to stations using extended user			
Telecommuting access extension not administered			
Administration of FACs for redirected calls ■ Extend Call Forward All Activate ■ Extended Call Forward Busy/Don't Answer Activate ■ Extended Call Forward Cancel ■ Change Coverage			

Continued on next page

Table 17-6. Communication Manager, MultiVantage™ Software, DEFINITY ECS, G1, and G3, and System 75 security checklist — *Continued*

	Y/N[1]	Note	N/A
Station Security Code Security Violation Notification feature active ■ Station security code security violations monitored 24 hours per day			
Routing ARS/WCR used for call routing			
1+809 and 0+809 area code blocked			
900, 976 calls blocked			
976 look-alikes blocked			
Block access to Alliance teleconference service (0700)			
011/LD calls limited by FRLs			
011/LD calls limited by Time-of-Day routing			
011/LD calls limited by 6-digit or digit analysis			
Alternate FRLs used (G3r)			
Facility Test Call/Data Origination Facility test code changed from default, if used			
Facility test code translated only when needed			
Facility test code limited to system admin/mtc COR			
Data origination feature code not translated			
Logoff notification enabled (G3V4)			
Miscellaneous Console permissions restricted/limited			
Operator calls restricted			

Continued on next page

Table 17-6. Communication Manager, MultiVantage™ Software, DEFINITY ECS, G1, and G3, and System 75 security checklist — *Continued*

	Y/N[1]	Note	N/A
Switch-hook flash denied on FAX machines, modems, etc.			
COR-to-COR restrictions used on all CORs			
Ports for adjuncts in own restricted COR			
VDNs have own restricted CORs (G3)			
`Restrict call forwarding off-net` = **y** (G3)			
Digit conversion of unauthorized calls to console or security (G3)			
Three-way COR check on transfer/conference (G3V3 and later)			
Authorization Code Security Violation Notification feature active (G3V3 and later)			
Product Monitoring Traffic measurement reports monitored daily			
SMDR/CMS reports monitored daily			
Recent change history log reviewed daily (G1/G3)			

1. If “NO” (N), provide Note reference number and explain.

DEFINITY G2 and System 85

Also see the general security checklist on page 17-2, and the security checklist for any attached voice mail systems or other adjuncts.

Customer: _____

Location: _____

System & Version: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-7. DEFINITY G2 and System 85 security checklist

	Y/N[1]	Note	N/A
System Administration Logins and Procedures Security code changed from factory default			
PBX Features Trunk groups have dial access disabled			
COS/miscellaneous trunk restrictions on dial-accessed trunks			
Disable trunk verification access code			
ACA on trunk groups			
Alternate FRLs used			
Individual and group controlled restrictions used			
Attendant control of trunk group activated for any trunk groups with TACs			

Continued on next page

Table 17-7. DEFINITY G2 and System 85 security checklist — *Continued*

	Y/N[1]	Note	N/A
VDNs have their own restricted COSs			
Ports for adjuncts in own restricted COS			
Authorization codes used			
Authorization codes not sequential			
900, 976 calls blocked			
Operator calls restricted			
011/LD calls restricted			
011/LD calls limited by Time-of-Day Routing			
1+809 and 0+809 area code blocked			
Digit conversion of unauthorized calls to console or security			
SMDR/CDR activated on all trunk groups			
Trunks measured by BCMS/CMS			
ARS/WCR used for call routing			
Remote Access Remote access disabled (no trunk groups translated as remote access)			
Remote access number is unpublished			
Seven-digit authorization codes used with remote access			
Authorization code timeout to attendant			
Barrier code is a random four-digit sequence			
SMDR/CAS/CDR reports monitored daily, including authorization code violations			

Continued on next page

Table 17-7. DEFINITY G2 and System 85 security checklist — *Continued*

	Y/N[1]	Note	N/A
Traffic measurement reports, including remote access history reviewed daily			
Customer Education Security code changed on a scheduled basis and coordinated with Denver maintenance center			
Blocking 976 look-alikes			
DID/DNIS number range does not overlap facility access codes			
Remote call forwarding not active			
Remote call forwarding used only offnet with groundstart trunks			
Positive disconnect verified with loop start trunks			
Remote Access Remote activated only if required			
Use non-DID number for remote access			
Barrier codes are maximum allowable digits, random number sequence			
Barrier codes are not sequential			
AVP/VMS Do not register ARS or FACS as subscribers			
Provide small mailboxes (AVP) and no voice mail coverage on “utility” stations (that is, non-voice such as FAX endpoints)			
Administration login password changed on regular basis			
`Transfer to Subscribers Only` = **y** (AVP)			

Continued on next page

Table 17-7. DEFINITY G2 and System 85 security checklist — *Continued*

	Y/N[1]	Note	N/A
Change password from default for new subscribers			
Voice ports outward restricted if outcalling not used			
Use of outcalling denied or minimized			
Invalid automated attendant menu options directed to operator			
Disable remote maintenance access when not in use			

1. If “NO” (N), provide Note reference number and explain.

DIMENSION PBX System

Also see the general security checklist on page 17-2, and the security checklist for any attached voice mail systems or other adjuncts.

Customer: _____

FP & Issue: _____

Location: _____

System Upgrade: _____

Major Addition: _____

Table 17-8. DIMENSION PBX System security checklist

	Y/N[1]	Note	N/A
System Administration Security code changed from factory default			
PBX Features Trunk-to-trunk transfer disabled			
Trunk groups have dial access disabled			
COS/miscellaneous trunk restrictions on dial-accessed trunks			
Disable trunk verification access code			
ACA on trunk groups			
Alternate FRLs used			
Individual and group controlled restrictions used			
Attendant control of trunk group activated for any trunk groups with TACS			
Ports for adjuncts in own restricted COS			

Continued on next page

Table 17-8. DIMENSION PBX System security checklist — *Continued*

	Y/N[1]	Note	N/A
Authorization codes used			
Authorization codes not sequential			
900, 976 calls blocked			
Operator calls restricted			
011/LD calls restricted			
011/LD calls limited by Time-of-Day Routing			
1+809 and 0+809 area code blocked			
Digit conversion of unauthorized calls to console or security			
SMDR activated on all trunk groups			
Trunks measured by BCMS/CMS			
Call forwarding off-net disabled			
ARS used for call routing			
Remote Access Remote access disabled (no trunk groups translated as remote access)			
Remote access number is unpublished			
7-digit authorization codes used with remote access			
Authorization code timeout to attendant			
Remote access COS is restricted			
Barrier code is a random 4-digit sequence			

Continued on next page

Table 17-8. DIMENSION PBX System security checklist — *Continued*

	Y/N[1]	Note	N/A
Product Monitoring SMDR reports monitored daily, including authorization code violations			
Traffic measurement reports, including remote access history reviewed daily			
Customer Education Security code changed on a scheduled basis and coordinated with Denver Maintenance Center			
Blocking 976 look-alikes			

1. If “NO” (N), provide Note reference number and explain.

MERLIN II Communications System

Also see the general security checklist on page 17-2, and the security checklist for any attached voice mail systems or other adjuncts.

Customer: _____

Location: _____

PBX Type: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-9. MERLIN II Communications System security checklist

	Y/N[1]	Note	N/A
System Features 900, 976 calls blocked			
Operator calls restricted			
011/LD calls limited by FRLs			
Remote Access (DISA) Remote access (DISA) not administered			
Use of non-DID/DNIS remote access number			
Voice Mail[2] Ports used for voice mail are toll restricted unless outcalling enabled			

Continued on next page

Table 17-9. MERLIN II Communications System security checklist — *Continued*

	Y/N[1]	Note	N/A
If outcalling enabled: ■ All voice mail ports except last one toll restricted ■ Last port for voice mail restricted to areas appropriate for outcalling			
Product Monitoring SMDR reports monitored daily			
Customer Education Blocking 976 look-alikes			

1. If “NO” (N), provide Note reference number and explain.
2. See also AVP or MERLIN MAIL Voice Messaging System checklists, as appropriate.

MERLIN LEGEND Communications System

Also see the general security checklist on page 17-2, and the security checklist for any attached voice mail systems or other adjuncts.

Customer: _____

Location: _____

System Version: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-10. MERLIN LEGEND Communications System security checklist

	Y/N[1]	Note	N/A
System Administration Password changed from factory default			
System Features Allow, Disallow List for all Ports 900, 976 calls blocked			
Operator calls restricted			
ARS FRLs established for internal dialing (0), local network calling (1), etc.			
Extension Remote call forwarding not active			
Remote call forward used offnet only with trunks that provide reliable disconnect (for example, ground-start)			

Continued on next page

Table 17-10. MERLIN LEGEND Communications System security checklist — *Continued*

	Y/N[1]	Note	N/A
ARS activated			
Trunk groups dial access = n			
FRLs assigned to limit network access based on business needs			
Remote Access Remote access inactive			
Use of non-DID/DNIS Remote Access number			
Barrier codes are random maximum-length, difficult-to-guess sequences			
Each barrier code's FRL is appropriate			
Assign allowed/disallowed lists when appropriate			
Different barrier code assigned to each user			
Voice Mail[2] Ports use for voice mail outward restricted (FRL) unless outcalling is used ■ If outcalling is used, all voice mail ports are outward restricted except those used for outcalling, which are restricted areas appropriate for outcalling by FRL ■ If outcalling to specific non-local areas is required, special allowed list has been created for those areas and assigned to the outcalling port(s)			

Continued on next page

Table 17-10. MERLIN LEGEND Communications System security checklist — *Continued*

	Y/N[1]	Note	N/A
Disallow list created containing 0, 011, 10, 700, 800, 1800, 809, 1809, 411, 1411, 900, and 9999			
Access denied to pooled facility codes 70, and 890-899			
Product Monitoring SMDR/HackerTracker reports monitored daily			

1. If “NO” (N), provide Note reference number and explain.
2. See also AVP or MERLIN MAIL Voice Messaging System checklists, as appropriate.

MERLIN MAIL Voice Messaging System

Also see the general security checklist on page 17-2, and the security checklist for the host communications system.

Customer: _____

Location: _____

PBX Type: _____

New Install: _____

System Upgrade: _____

Port Additions: _____

Table 17-11. MERLIN MAIL Voice Messaging System security checklist

	Y/N[1]	Note	N/A
System Administration System administrator mailbox changed from default			
System administrator mailbox password changed to a maximum-length, difficult-to-guess value			
System Features Mailboxes created only for active subscribers			
Outcalling privileges not assigned or assigned only to those requiring them			
MERLIN LEGEND Communications System voice mail port(s) outward restricted (FRL 0) if no outcalling			

Continued on next page

Table 17-11. MERLIN MAIL Voice Messaging System security checklist — *Continued*

	Y/N[1]	Note	N/A
MERLIN LEGEND Communications System voice mail port(s) used for outcalling restricted via allow list to specific areas if outcalling is needed. All other MERLIN LEGEND Communications System voice mail ports outward restricted.			
Disallow list created containing 0, 011, 10, 700, 800, 1800, 809, 1809, 411, 1411, 900, and 9999. All MERLIN LEGEND Communications System voice mail ports assigned to this list. (When MERLIN LEGEND Communications System is host system.)			
Remote call forwarding used only with trunks that provide reliable disconnect (such as ground-start). (When MERLIN LEGEND Communications System is host system.)			
Automated Attendant No pooled facility access codes translated on menus			
No ARS codes translated on menus			
Remote call forwarding used offnet only with trunks that provide reliable disconnect (for example, ground-start)			
End User Education Passwords changed from default for new subscribers			
Passwords are difficult to guess			
Passwords are changed quarterly			

1. If “NO” (N), provide Note reference number and explain.

MERLIN MAIL-ML Voice Messaging System

Also see the general security checklist on page 17-2, and the security checklist for the host communications system.

Customer: _____

Location: _____

PBX Type: _____

New Install: _____

System Upgrade: _____

Port Additions: _____

Table 17-12. MERLIN MAIL-ML Voice Messaging System security checklist

	Y/N[1]	Note	N/A
System Administration System administrator mailbox changed from default			
System administrator mailbox password changed to a maximum-length, difficult-to-guess value			
System Features Mailboxes created only for active subscribers			
Outcalling privileges not assigned or assigned only to those requiring them			
MERLIN LEGEND Communications System voice mail port(s) outward restricted (FRL 0) if no outcalling			

Continued on next page

Table 17-12. MERLIN MAIL-ML Voice Messaging System security checklist — *Continued*

	Y/N[1]	Note	N/A
MERLIN LEGEND Communications System voice mail port(s) used for outcalling restricted via allowed list to specific areas if outcalling is needed. All other MERLIN LEGEND Communications System voice mail ports outward restricted.			
On MERLIN LEGEND Communications System, create disallow list containing 0, 011, 10, 700, 800, 1800, 809, 1809, 411, 1411, 900, and 9999. All MERLIN LEGEND Communications System voice mail ports assigned to this list.			
Remote call forwarding used only with trunks that provide reliable disconnect (such as ground-start)			
Automated Attendant No pooled facility access codes translated on menus			
No ARS codes translated on menus			
Remote call forwarding used offnet only with trunks that provide reliable disconnect (for example, ground-start)			
End User Education Passwords changed from default for new subscribers			
Passwords are difficult to guess			
Passwords are changed quarterly			

1. If “NO” (N), provide Note reference number and explain.

MERLIN MAIL R3 Voice Messaging System

Also see the general security checklist on page 17-2, and the security checklist for the host communications system.

Customer: _____

Location: _____

PBX Type: _____

New Install: _____

System Upgrade: _____

Port Additions: _____

Table 17-13. MERLIN MAIL R3 Voice Messaging System security checklist

	Y/N[1]	Note	N/A
System Administration System administrator mailbox changed from default			
System administrator mailbox password changed to a maximum-length, difficult-to-guess value			
System administration menu access password changed to a maximum-length, difficult-to-guess value			
Forced password change for new subscribers			
User password > 6 characters long			
System Features Mailboxes created only for active subscribers			

Continued on next page

Table 17-13. MERLIN MAIL R3 Voice Messaging System security checklist — *Continued*

	Y/N[1]	Note	N/A
Transfer restricted to subscribers only			
Login attempts before warning message < 6			
Login attempts before mailbox lockout < 6			
Outcalling privileges not assigned or assigned only to those requiring them			
MERLIN LEGEND Communications System voice mail port(s) outward restricted (FRL 0) if no outcalling			
MERLIN LEGEND Communications System voice mail port(s) used for outcalling restricted via allow list to specific areas if outcalling is needed. All other MERLIN LEGEND Communications System voice mail ports outward restricted.			
On MERLIN LEGEND Communications System, create disallow list containing 0, 011, 10, 700, 800, 1800, 809, 1809, 411, 1411, 900, and 9999. All MERLIN LEGEND Communications System voice mail ports assigned to this list.			
Remote call forwarding used only with trunks that provide reliable disconnect (such as ground-start)			

Continued on next page

Table 17-13. MERLIN MAIL R3 Voice Messaging System security checklist — *Continued*

	Y/N[1]	Note	N/A
Automated Attendant No pooled facility access codes translated on menus			
No ARS codes translated on menus			
Remote call forwarding used offnet only with trunks that provide reliable disconnect (for example, ground-start)			
End User Education Passwords changed from default for new subscribers			
Passwords are difficult to guess			
Passwords are changed quarterly			

1. If “NO” (N), provide Note reference number and explain.

MERLIN Plus Communications System

Also see the general security checklist on page 17-2, and the security checklist for any attached adjuncts.

Customer: _____

Location: _____

PBX Type: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-14. MERLIN Plus Communications System security checklist

	Y/N[1]	Note	N/A
System Features 900, 976 calls blocked			
Operator calls restricted			
011/LD calls limited by FRLs			
Restrict remote call forwarding (MERLIN Plus Communications System R2 only) to those with need			
Implement Automatic Timeout feature for remote call forwarding (MERLIN Plus Communications System R2 only)			
Product Monitoring SMDR reports monitored daily			

1. If “NO” (N), provide Note reference number and explain.

Messaging 2000 Voice Mail System

Also see the general security checklist on page 17-2.

Customer: _____

PBX Type: _____

Location: _____

New Install: _____

System Upgrade: _____

Port Additions: _____

Table 17-15. Messaging 2000 Voice Mail System security checklist

	Y/N[1]	Note	N/A
System Administration Passwords [Required] Set the `Minimum Length of Password` parameter on the Subscriber tab in System Setup at least 1 digit higher than the number of digits system mailboxes.			
[Required] Set the `Days Before Forced Password Change` parameter on the Subscriber tab in System Setup to require subscribers to regularly change their mailbox passwords. The recommended setting is a value from 182 to 365.			
[Required] Use at least 6-digit **level 2 and level 3** supervisor passwords to prevent unauthorized system manager access.			
[Required] All remote access logins to the system must be administered to require the use of a secondary password.			

Continued on next page

Table 17-15. Messaging 2000 Voice Mail System security checklist — *Continued*

	Y/N[1]	Note	N/A
[Recommended] Use the randomly-generated method of assigning passwords to new mailboxes.			
[Recommended] Regularly monitor the Uninitialized Mailbox report to determine if subscribers have changed their mailboxes passwords. Remind subscribers that have not initialized their mailboxes that they should change their passwords immediately to prevent unauthorized access to their mailboxes.			
[Recommended] Activate the `Enable Password Security` parameter on the Subscriber tab in System Setup to require subscribers to press the "#" key after they finish entering their passwords.			
[Recommended] Write down **level 2** and **level 3** passwords and keep them in a secure place.			
[Recommended] Notify the local service provider of any changes to **level 2** or **level 3** supervisor passwords in case remote maintenance is required.			
Login Attempts [Required] Enable the `Failed Login Notification` parameter in subscribers' COSs and the `Failed Login Notify` option on the Subscriber Settings dialog box so the system notifies subscribers when one or more unsuccessful login attempts are made to their mailboxes.			

Continued on next page

Table 17-15. Messaging 2000 Voice Mail System security checklist — *Continued*

	Y/N[1]	Note	N/A
[Required] Set the `Consecutive Login Failures Before Lock-Out` parameter on the Subscriber tab in System Setup to specify how many unsuccessful login attempts are allowed before mailboxes are locked.			
[Required] Enable the `Mailbox Lock-Out` option in subscribers' COSs and the `Mailbox Lock-Out` option on the Subscriber Settings dialog box to lock subscriber mailboxes after the number of unsuccessful login attempts specified in the `Consecutive Login Failures Before Lock-Out` parameter have occurred.			
[Recommended] Regularly monitor the Login Failure report to determine if a high number of unsuccessful login attempts are occurring on a mailbox or if the login attempts are occurring after business hours.			
Miscellaneous [Required] Set the Auto Logoff feature to a low value to ensure that the M2000 system returns to security level 1 after a short period of inactivity.			
[Recommended] When Quick Assist is run in recover mode from the Quick Assist icon in the product folder, specify a `Mailbox to Receive Unattached Messages` on the Recover Files dialog box.			

Continued on next page

Table 17-15. Messaging 2000 Voice Mail System security checklist — *Continued*

	Y/N[1]	Note	N/A
[Recommended] When Quick Assist is run in recover mode from the \CVR prompt in an OS/2 window, or run automatically as part of system maintenance, include the -M*n* parameter to specify a mailbox to receive unattached messages.			
[Recommended] Use the `Require Password to Proceed to Next Level` option to secure v-trees that provide sensitive information such as pricing data and customer data.			
Toll Fraud [Required] Disable the `Transfer Invalid Mailboxes During Hours` and `Transfer Invalid Mailboxes After Hours` parameters on the Invalid Mailbox tab in System Setup.			
Physical Security [Required] Store the M2000 system PC in a secure area.			
[Required] The modem connection to the system should be “disabled” when it is not required for use by bonafide personnel. This connection should be enabled only by the system administrator on an “as needed” basis.			

Continued on next page

Table 17-15. Messaging 2000 Voice Mail System security checklist — *Continued*

	Y/N[1]	Note	N/A
End-User Education [Required] The end-user must periodically/frequently change all secondary passwords. After changing the secondary passwords, the end-user should notify the appropriate Avaya support organization(s) that the passwords have been changed.			
[Recommended] Require that subscribers record their name prompts so that the system voices the mailbox owner's name to callers sending messages to M2000 system mailboxes.			
MERLIN Legend Security [Required] Contact the Avaya system representative to determine what security features are available for the Merlin Legend communication system and how to implement them. Follow the guidelines given in the Merlin Legend security checklist. Before implementing any security features on the phone system, contact an Avaya technical support representative to ensure that the features you want to implement will not disrupt M2000 system performance in any way.			

1. If "NO" (N), provide Note reference number and explain.

Multimedia Communications Exchange Server

Also see the general security checklist on page page 17-2.

Customer: _____

System & Version: _____

Location: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-16. Multimedia Communications Exchange Server security checklist

	Y/N[1]	Note	N/A
System Administration Root password changed from default			
Administration login(s) password secured			
Remote Maintenance Access Remote Maintenance (RMB) installed			
RMB telephone number is unpublished			
System Features Administered licensed number of users			
Audit log advised to be checked daily			

1. If “NO” (N), provide Note reference number and explain.

Multipoint Conferencing Unit /Conference Reservation and Control System

Also see the general security checklist on page 17-2.

Customer: _____

Location: _____

MSM SW Version and Install Date: _____

ESM SW Version and Install Date: _____

CRCS SW Version and Install Date: _____

CRCS is Single-User or Multi-User? _____

Table 17-17. MCU/CRCS security checklist

	Y/N[1]	Note	N/A
Physical Security			
MCU room and wiring closets locked			
All equipment documentation secured			
CRCS secured at night			
MCU local and remote administration equipment secured			
Remote port security devices (RPSD) installed			
Call logs and printed reports secured			

Continued on next page

Table 17-17. MCU/CRCS security checklist — *Continued*

	Y/N[1]	Note	N/A
Customer Education System manager/administrator has copy of *Avaya™ Toll Fraud and Security Handbook* (this document)			
System security policy established and distributed			
System security policy reviewed periodically			
Security policy included in new-hire orientation			
Employees know how to detect potential toll fraud			
Employees know where to report suspected toll fraud			
Authorization codes not sequential			
Remote access phone number(s) not published			
Barrier codes and passwords are chosen to be difficult to guess			
Barrier codes, passwords (including ESM and CRCS) and authorization codes are removed/changed when employees are terminated			
Authorization codes, account codes, and passwords are not written down or translated on auto-dial buttons			
HackerTracker thresholds established			
Social engineering explained			

1. If “NO” (N), provide Note reference number and explain

MCU Product Checksheets Attached: (Check all that apply)
(__) Multimedia Server Module (MSM)
(__) Expansion Services Module (ESM)
(__) Conference Reservation and Control System (CRCS)

ESM security checklist

NOTE:
See the appropriate security checklist for the host MSM.

Customer: _____

ESM Type: _____

Location: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-18. ESM security checklist

	Y/N[1]	Note	N/A
System Administration Root login changed from default			
All other UNIX login passwords changed (INADS)			
Remote Maintenance Access Remote maintenance board (RMB) installed (if NO, skip to "Using External Modem...") ■ RMB (INADS) telephone number unpublished ■ Level 1 and Level 2 passwords protected ■ Level 1 and Level 2 passwords changed from default			
Using external modem off COM2 rather than RMB ■ Busy lamp on modem port ■ Modem dial-up password administered			
System Features Administered UNIX license number of system			
Periodic reboot advised to be enabled			
Host MSM (See checklist for the host MSM)			

1. If "NO" (N), provide Note reference number and explain.

CRCS Security Checklist

Customer: _____

CRCS Type: _____

Location: _____

New Install: _____

System Upgrade: _____

Port Additions: _____

Table 17-19. CRCS security checklist

	Y/N[1]	Note	N/A
System Administration Is CRCS type single-user (SU) or multi-user (MU)?			
Is the proper serial number assigned to the system?			
System administrator password changed to a maximum-length, difficult-to-guess value			
Client administrator(s) passwords changed (MU only) to a maximum length, difficult to guess value			
Forced password change for new clients (MU only)			
System Features Login attempts before warning message < 6 (R3 only)			
Outcalling privileges not assigned, or assigned only to those requiring them			

Continued on next page

Table 17-19. CRCS security checklist — *Continued*

	Y/N[1]	Note	N/A
End User Education Passwords changed for new subscribers			
Passwords are difficult to guess			
Passwords are changed quarterly			

1. If “NO” (N), provide Note reference number and explain.

MSM security checklist

See the appropriate security checklist for the attached ESM or CRCS.

Customer: _____

System & Version: _____

Location: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-20. MSM security checklist

	Y/N[1]	Note	N/A
System Administration Customer advised of all logins under their control. Passwords changed from factory defaults.			
Passwords are customer-entered, maximum length, unique alphanumeric words.			
NETCON access restricted by COR-to-COR restrictions.			
NETCON channels secured			
Non-DID extensions used for NETCON ports			
Unused NETCON channels removed			
Login Security Violation Notification feature active ■ Logins automatically disabled after security violation ■ Login security violations monitored 24 hours per day			
Login permissions customized			
Unused logins removed (“remove login” command or disabled [passwords VOIDed])			
Unique customer logins used			
Password aging activated			
Logins temporarily disabled when not needed (“disable/enable” commands)			
Customer access to INADS port disabled			
Remote Access Remote access permanently disabled if not used (G3V2 and North American Dial Plan loads)			

Continued on next page

Table 17-20. MSM security checklist — *Continued*

	Y/N[1]	Note	N/A
Remote access administered ■ Remote access number is unpublished ■ Non-DID remote access number used ■ Barrier codes are random 7-digit sequences ■ Barrier codes in own restricted COR ■ 7-digit authorization codes used ■ Second dial tone omitted between barrier and authorization codes ■ Authorization code time-out to attendant ■ Voice processing ports COR-to-COR restricted from dialing remote access barrier codes ■ Remote Access Security Violation Notification feature active — Remote access security violations monitored 24 hours per day — Remote access automatically disabled following detection of a security violation (G3V3) ■ Barrier code aging used (G3V3) ■ Remote access temporarily disabled when not needed (“disable/enable” commands)			
Logoff notification enabled for remote access			
Networking Features **Trunking** Prohibit trunk-to-trunk transfer on public access trunks			
Tie trunk groups are COR-to-COR restricted			

Continued on next page

Table 17-20. MSM security checklist — *Continued*

	Y/N[1]	Note	N/A
Trunk groups have dial access = n			
COR-to-COR restrictions on dial-accessed trunks			
ACA on trunks groups			
SMDR/CDR activated on all trunk groups			
Attendant control of trunk groups with TAC = y			
Routing ARS/WCR used for call routing ■ 1+809 and 0+809 area code blocked ■ 900 and 976 calls blocked ■ 976 “look-alikes” blocked ■ Block access to Alliance teleconference service (0700) ■ 011/LD calls limited by FRLs ■ 011/LD calls limited by Time-of-Day routing ■ 011/LD calls limited by 6-digit or digit analysis ■ Alternate FRLs used (G3r)			
Facility Test Call/Data Origination Facility test code changed from default, if used ■ Facility test code translated only when needed ■ Facility test code limited to system admin/mtce COR ■ Logoff notification enabled for facility test call (G3V4)			
Data origination feature code not translated			

Continued on next page

Table 17-20. MSM security checklist — *Continued*

	Y/N[1]	Note	N/A
Miscellaneous Console permissions restricted/limited			
Individual and group-controlled restrictions used			
Authorization codes used			
COR-to-COR restrictions used on all CORs			
Ports for adjuncts in own restricted COR			
Restrict call forwarding off-net = y (G3)			
Authorization Code Security Violation Notification feature active			
Product Monitoring Traffic measurements reports monitored daily			
SMDR/CMS reports monitored daily			
Recent change history log reviewed daily (G1/G3)			

1. If “NO” (N), provide Note reference number and explain.

PARTNER, PARTNER II, and PARTNER Plus communications systems, and PARTNER Advanced Communications System (ACS)

Also see the general security checklist on page page 17-2.

Customer: _____

Location: _____

Product Type: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-21. PARTNER, PARTNER II, and PARTNER Plus communication systems and PARTNER ACS security checklist

	Y/N[1]	Note	N/A
Physical Security Switch room and wiring closets locked			
All equipment documentation secured			
Attendant console secured at night; headset unplugged			
Local and remote administration equipment secured			
Telephone logs and printed reports secured			
Adjunct (CAT, SMDR, Printer, etc.) terminals secured			

Continued on next page

Table 17-21. PARTNER, PARTNER II, and PARTNER Plus communication systems and PARTNER ACS security checklist — *Continued*

	Y/N[1]	Note	N/A
Customer Education System manager/administrator has copy of *Avaya™ Toll Fraud and Security Handbook* (this document)			
System security policy established and distributed			
System security policy reviewed periodically			
Security policy included in new-hire orientation			
Employees know how to detect potential toll fraud			
Employees know where to report suspected toll fraud			
Account codes not sequential			
Remote access phone number not published			
Barrier codes and passwords are chosen to be difficult to guess			
Barrier codes, passwords (including voice mail), and account codes are removed/changed when employees are terminated			
Account codes and logins not written down or translated on auto-dial buttons			
Logins and passwords are not written down			
All customer passwords are changed on a regular basis			
HackerTracker thresholds established			
Social engineering explained			

Continued on next page

Table 17-21. PARTNER, PARTNER II, and PARTNER Plus communication systems and PARTNER ACS security checklist — *Continued*

	Y/N[1]	Note	N/A
Customer is aware of network-based toll fraud surveillance offerings such as netPROTECT			
Customer knows how to subscribe to ACCESS security shared folder			
System Features Forced account codes with verification used (PARTNER Plus Communications System 3.1 and later, and PARTNER II Communications System Release 3.1 and later, and PARTNER ACS Release 1 and later)			
900, 976 type calls blocked[2]			
976 look-alikes blocked[2]			
Operator calls restricted[2]			
011/LD calls restricted[2]			
1+809 and 0+809 area code blocked[2]			
Block access to Alliance teleconference service (0700)[2]			
Station lock used to secure terminals in public areas (PARTNER Plus Release 4.1 and later, PARTNER II Release 4.1 and later, PARTNER ACS Release 1 and later			
Remote Access (for PARTNER ACS Release 3 only) Remote access password is changed periodically			

Continued on next page

Table 17-21. PARTNER, PARTNER II, and PARTNER Plus communication systems and PARTNER ACS security checklist — *Continued*

	Y/N[1]	Note	N/A
System administrator is the only person responsible for the security of the remote access password			
Remote access password consists of random alpha numeric characters that can be entered only locally, onsite via dial pad administration			
Remote access password disabled when not in service			
Voice Mail (for PARTNER Plus Release 3.1 and later, PARTNER II Release 3.1 and later, and PARTNER ACS Release 1 and later) Ports used for voice mail outward restricted (FRL 0) unless outcalling is used ■ If outcalling is used, all voice mail ports are outward restricted except those used for outcalling, which are restricted to areas appropriate for outcalling by FRL ■ If outcalling to specific non-local areas is required, special allow list has been created for those areas and assigned to the outcallng port(s)			
Disallow list created containing *, 11, 0, 011, 10, 411, 1411, 700, 800, 1800, 809, 1809, 900, and 9999.,. All voice mail ports are assigned to this disallow list.			

Continued on next page

Table 17-21. PARTNER, PARTNER II, and PARTNER Plus communication systems and PARTNER ACS security checklist — *Continued*

	Y/N[1]	Note	N/A
Product Monitoring (for PARTNER Plus, PARTNER II, and PARTNER ACS only) SMDR/Call Accounting reports monitored daily			
HackerTracker reports monitored daily			
Automated Attendant Administer range of valid extensions			
Administer maximum digits to match dial plan			
Change default system password			
Adjuncts Remote Administration Unit (RAU) unattended mode disabled, or RAU password enabled for unattended mode			
RAU password consists of random numbers			
RAU password is changed regularly			

1. If “NO” (N), provide Note reference number and explain.
2. Use line access restrictions, outgoing call restrictions, allowed and disallowed lists features.

PARTNER MAIL, PARTNER MAIL VS, and PARTNER Voice Mail (PVM) systems

See also the general security checklist on page 17-2 and the security checklist for the host communications system.

Customer: _____

Location: _____

PBX Type: _____

New Install: _____

System Upgrade: _____

Port Additions: _____

Table 17-22. PARTNER MAIL, PARTNER MAIL VS, and PARTNER Voice Mail (PVM) systems security checklist

	Y/N[1]	Note	N/A
System Administration (for PARTNER Mail, PARTNER MAIL VS, and PARTNER Voice Mail) Passwords and mailboxes removed/changed when employees are terminated			
Mailboxes for unused extensions deleted			
Administration login password changed from default			
Administration login password changed regularly			
Outcalling privileges not assigned or assigned only to those requiring them			

Continued on next page

Table 17-22. PARTNER MAIL, PARTNER MAIL VS, and PARTNER Voice Mail (PVM) systems security checklist — *Continued*

	Y/N[1]	Note	N/A
(for PARTNER MAIL System only) System mailboxes (90 to 98 and 9999) assigned COS 7 to 9 to prevent transfer out of mailbox			
(for PARTNER MAIL Release 3 only) System administrator mailbox changed from default			
System administrator mailbox password changed to a maximum-length value that is difficult-to-guess			
System administrator menu access password changed to a maximum-length value that is difficult-to-guess			
Forced password change for new value			
User password more than 5 characters long			
System Features (for PARTNER MAIL Release 3 only) Mailboxes created only for active subscribers			
Transfer restricted to subscribers only			
Login attempts before mailbox lockout < 6			
Login attempts before warning message < 6			
Outcalling privileges not assigned or assigned only to those requiring them			

1. If “NO” (N), provide Note reference number and explain.

System 25

Also see the general security checklist on page 17-2, and the security checklist for any attached voice mail systems or other adjuncts.

Customer: _____

Location: _____

PBX Type: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 17-23. System 25 security checklist

	Y/N[1]	Note	N/A
System Administration Passwords changed from default			
Trunk-to-trunk transfer=n. (Warning: applies to loop start trunks only)			
Trunk groups have dial access disabled (DAC=n)			
Toll restrictions applied to stations and trunks as appropriate			
900, 976 calls blocked			
Operator calls restricted			
011/LD calls limited by FRLs			
DID/DNIS number range does not overlap facility access codes			
Remote call forwarding not active			
Remote call forwarding used only offnet with groundstart trunks			

Continued on next page

Table 17-23. System 25 security checklist — *Continued*

	Y/N[1]	Note	N/A
Positive disconnect verified with loop start trunks			
Remote Access Remote activated only if required			
Use non-DID number for remote access			
Barrier codes are maximum allowable digits, random number sequence, non-sequential			
AVP/VMS Do not register ARS or FACS as subscribers			
Provide small mailboxes (AVP) and no voice mail coverage on “utility” stations (that is, non-voice such as FAX endpoints)			
Admin login password changed on regular basis			
Transfer to Subscribers Only = y			
Change password from default for new subscribers			
Voice ports outward restricted if outcalling not used			
Use of outcalling denied or minimized			
Invalid automated attendant menu options directed to operator			

Continued on next page

Table 17-23. System 25 security checklist — *Continued*

	Y/N[1]	Note	N/A
Disable remote maintenance access when not in use			
Product Monitoring SMDR/CAS reports monitored daily, administration log and activity log checked daily (AVP)			
End-User Education Only trusted personnel transferred to remote maintenance port			

1. If “NO” (N), provide Note reference number and explain.

PassageWay Telephony Services

Also see the general security checklist on page 17-2.

Customer: _____

Location: _____

PassageWay Install Date: _____

Table 17-24. PassageWay Telephony Services security checklist

	Y/N[1]	Note	N/A
General Telephony server is in a secure location (locked room).			
Backups of the telephony server machine are made at regular intervals.			
Virus detection is run on the telephony server machine at regular intervals. If infected files are detected, they are cleaned or removed, or restored from system backups.			
Product Installation When using TCP/IP for Computer Telephone Integration (CTI) links, the CTI link between the telephony server and the PBX (for example, DEFINITY ECS) is installed on a private LAN.			
Routing is not enabled between two network cards.			

Continued on next page

Table 17-24. PassageWay Telephony Services security checklist — *Continued*

	Y/N[1]	Note	N/A
System Administration Guidelines followed for logins/passwords for user accounts. (See PassageWay customer documentation.)			
Customer educated about standard Avaya password recommendations (For example, at least 7 characters and forced password change for new subscribers. See PassageWay customer documentation.)			
Default administrator login for Tserver changed at installation.			
Separate Tserver accounts administered for each user. (Login and password added on OS, and login id added to Tserver) for each user. (Shared logins are not allowed.)			
Unused Tserver and system accounts are disabled or removed.			
When using btrieve, enabled the Log Changes to SDB feature.			
Customers entered their passwords as accounts were created.			
Individuals given control of only their devices during Tserver administration. (Avoid using any device or exception list.)			
Enabled Communication Manager, MultiVantage™ Software, or DEFINITY ECS CDR (or comparable capability of other Avaya switch) to track call history.			

Continued on next page

Table 17-24. PassageWay Telephony Services security checklist — *Continued*

	Y/N[1]	Note	N/A
For NetWare only: Used the NetWare Administrator feature (NetWare 4.10 and 4.11) or SYSCON utility (NetWare 3.12) to set the appropriate login and password restrictions (For example, require users to have passwords with a minimum length of 7 characters, enable password aging, and so forth.)			
Used the NetWare Administrator feature (NetWare 4.10 and 4.11) or SYSCON utility (NetWare 3.12) to enable the Intruder Detection feature and to lock accounts after several invalid login attempts have been made.			
Enabled the Restrict Users to Home Worktop feature in the telephony services security database.			
For Windows NT only: Disabled the Extended Worktop Access feature in the Telephony Services security database.			
Use the Account Policy dialog box of the Windows NT user manager to configure the following security features: ■ Minimum password length ■ Minimum and maximum password age ■ Password uniqueness ■ Account lockout for invalid logon attempts			
Took full advantage of Windows NT event log (for example, for monitoring failed login attempts)			

Continued on next page

Table 17-24. PassageWay Telephony Services security checklist — *Continued*

	Y/N[1]	Note	N/A
Access Control To ensure protection of sensitive system files used by Tserver, only System Administrator has access to Tserver, Security Database, and log files.			
For Windows NT only: Make file system NTFS instead of FAT.			
Remote Access When using pcANYWHERE (or another tool for remote access of customer PCs), customer has been advised of the following precautions: ■ Do not publish phone number for modem. ■ Use return call option with an Avaya phone number. (Do not set up pcANYWHERE without the callback option.)			
■ When on the PC, pcANYWHERE is not started except as required. ■ For added security, unplug phone jack from modem when pcANYWHERE is not in use. ■ Change password after services leaves and after remote access.			

Continued on next page

Table 17-24. PassageWay Telephony Services security checklist — *Continued*

	Y/N[1]	Note	N/A
■ Configure the following security options: — Require login names for callers — Make passwords case-sensitive — Log failed connection attempts — Maximum login attempts per call — Time to enter complete login — Disconnect if inactive			
■ Configure pcANYWHERE to log remote control and on-line sessions. (Set the `Save Session Statistics in Activity Log File` checkbox in the Other Session Parameters group box.)			

1. If “NO” (N), provide Note reference number and explain

Large business communications systems security tools by release

18

The following tables contain page references for the available security features for System 75, System 85, DEFINITY G1, G2, G3, DEFINITY ECS, MultiVantage™ Software, and Communication Manager. Information is listed by release.

NOTE:
MultiVantage™ Software and Communication Manager and bundled into the **ECS R5 & later** column.

Table 18-1. Large Business communications systems security tools by release

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
3-way COR check	"Restriction override (3-way COR check)" on page 5-17						x	x	x	x
AAR/ARS Analysis	"AAR/ARS analysis" on page 5-20	x	x	x	x	x	x	x	x	x
Administrable Logins	"Forced password aging and administrable logins" on page 5-52							x	x	x
Administration Security	"Administration / maintenance access" on page 4-4	x	x	x	x	x	x	x	x	x

Continued on next page

Table 18-1. Large Business communications systems security tools by release — *Continued*

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
Alternate Facility Restriction Levels	"Remote access" on page 4-2 "Class of restriction" on page 5-14 "Alternate facility restriction levels" on page 5-19 "Provide individualized calling privileges using FRLs" on page 5-31		x		x	x	x	x	x	x
ARS Dial Tone	"ARS dial tone" on page 5-20	x	x	x	x	x	x	x	x	x
Attendant-Controlled Voice Terminals	"Attendant - controlled voice terminals" on page 5-21		x		x					
Authorization Codes	(See Index)	R1V3	x	x	x	x	x	x	x	x
Authorization Code Security Violation Notification	"Security violation notification (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3)" on page 5-59							x	x	x
Automatic Circuit Assurance	"Automatic circuit assurance" on page 5-56 "Automatic circuit assurance" on page 8-11	x	x	x	x	x	x	x	x	x

Continued on next page

Table 18-1. Large Business communications systems security tools by release — *Continued*

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
Barrier Code	"Remote access" on page 4-2 "Security tips" on page 5-2 "Barrier codes" on page 5-5 "Restrict who can use remote access and track its usage" on page 5-29 "Protecting the Remote Access feature" on page 6-12	x	x	x	x	x	x	x	x	x
Barrier Code Aging	"Remote access barrier code aging/access limits (DEFINITY G3V3 and Later)" on page 5-67							x	x	x
BCMS Measurement	"BCMS measurements (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G1 and G3)" on page 5-58			x		x	x	x	x	x

Continued on next page

Table 18-1. Large Business communications systems security tools by release — *Continued*

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
Call Detail Recording (SMDR)	"Call detail recording/station message detail recording" on page 5-53 "Call detail recording and / station message detail recording" on page 7-13 "Call detail recording / station message detail recording" on page 8-9	x	x	x	x	x	x	x	x	x
Call Forward On/Off Net	"Class of service" on page 5-17						x	x	x	x
Call Prompting/ ASAI	"Protecting vectors that contain call prompting" on page 5-11		x		x	x	x	x	x	x
Call Vectoring	"Call vectoring (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3)" on page 5-10 "Prevent after-hours calling using time of day routing or alternate FRLs" on page 5-33		x		x	x	x	x	x	x
Central Office Restrictions	"Central office restrictions" on page 5-22	x	x	x	x	x	x	x	x	x
Class of Restrictions	(See Index)	x		x		x	x	x	x	x

Continued on next page

Table 18-1. Large Business communications systems security tools by release — *Continued*

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
Class of Service	"Class of service" on page 5-17 "Class of service" on page 7-7 "Class of service" on page 8-4	x	x	x	x	x	x	x	x	x
CMS Measurements	"CMS measurements" on page 5-58	x	x	x	x	x	x	x	x	x
COR Descriptions	"Class of restriction" on page 5-14							x	x	x
Digit Conversion	"Digit conversion" on page 5-25 "Block international calling" on page 5-34 "Limit international calling" on page 5-35 "Restrict calls to specified area codes" on page 5-37		x	x	x	G3i	x	x	x	x
Enhanced Call Transfer	"Basic call transfer" on page 7-23 "Disallow outside calls" on page 8-16	R1V3 Issue 2.0	R2V4	Issue 5.0	x	x	x	x	x	x
Extended User Administration of Redirected Calls	"Extended user administration of redirected calls" on page 5-27									x

Continued on next page

Table 18-1. Large Business communications systems security tools by release — *Continued*

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
Facility Restriction Levels	"Class of restriction" on page 5-14 "Facility restriction level" on page 5-19 "Facility restriction levels" on page 7-6 "Facility restriction levels" on page 8-2	x	x	x	x	x	x	x	x	x
Feature Access Code Administration	"Known toll fraud activity" on page 2-4 "Feature access code administration" on page 5-9	x	x	x	x	x	x	x	x	x
Forced Entry of Account Code	"Forced entry of account code" on page 5-24 "Require account codes" on page 5-47	x	x	x	x	x	x	x	x	x
Forced Password Aging	"Forced password aging and administrable logins" on page 5-52							x	x	x
Free Call List	"Free call list" on page 5-20		x		x					
Fully Restricted Service	"Calling party and called party restrictions" on page 5-15 "Fully restrict service" on page 5-31	x	x	x	x	x	x	x	x	x
INADS Port Access Restrictions	"Adding customer logins and assigning initial password" on page 13-13								x	x

Continued on next page

Table 18-1. Large Business communications systems security tools by release — *Continued*

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
List Call Forward Command	"Class of service" on page 5-17								x	x
Login ID Kill After "N" Attempts	"Administering the Login ID Kill After N Attempts feature" on page 13-7							x	x	x
Logoff Notification - Facility Test Call	"Adding customer logins and assigning initial password" on page 13-13								x	x
Logoff Notification - Remote Access	"Adding customer logins and assigning initial password" on page 13-13								x	x
Malicious Call Trace	"Malicious call trace" on page 5-68		R2V4		x	G3r	x	x	x	x
Monitor Command	"Monitor trunks" on page 5-46			x		x	x	x	x	x
Monitor Security Violations Reports	"Administering the security violations reports" on page 13-18						x	x	x	x
Night Service	"Night service" on page 5-10	x	x	x	x	x	x	x	x	x
Permanently Disable Remote Access	"Administering barrier code aging" on page 13-11	R1V3n		G1V4n		x	x	x	x	x
Personal Station Access (PSA)	"Personal station access" on page 5-25									x
Recall Signaling	"Recall signaling (switchhook flash)" on page 5-21	x		x		x	x	x	x	x
Recent Change History Report	"Recent Change History report (Communication Manager, MultiVantage Software, DEFINITY ECS, and DEFINITY G1 and G3)" on page 5-68			x		x	x	x	x	x

Continued on next page

Table 18-1. Large Business communications systems security tools by release — *Continued*

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
Remote Access Authorization Code Dial Tone	"Remote access dial tone" on page 5-10	R1V3		x		x	x	x	x	x
Remote Access Kill After "N" Attempts	"Administering the Remote Access Kill After N Attempts feature" on page 13-6							x	x	x
Remote User Administration of Call Coverage	"Remote user administration of call coverage" on page 5-27									x
Restrict Changes to Administration Objects	"Require passwords" on page 5-28 "Forced password aging and administrable logins" on page 5-52						x	x	x	x
Restricting Incoming Tie Trunks	"Restricting incoming tie trunks" on page 5-22		x		x					
Restrictions; Individual and Group-Controlled	"Restrictions — individual and group-controlled (Communication Manager, MultiVantage Software, DEFINITY ECS, DEFINITY G1, G3, and System 75)" on page 5-21	x		x		x	x	x	x	x
Security Violations Measurement Report	"Security Violations Measurement reports" on page 5-62	x	x	x	x	x	x	x	x	x

Continued on next page

Table 18-1. Large Business communications systems security tools by release — *Continued*

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
Security Violation Notification Feature	"Security violation notification (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3)" on page 5-59					x	x	x	x	x
Service Observing	"Service observing" on page 5-69	x	x	x	x	x	x	x	x	x
Station Restrictions	"Station restrictions" on page 5-20	x	x	x	x	x	x	x	x	x
Status Remote Access	"Adding customer logins and assigning initial password" on page 13-13								x	x
SVN Referral Call With Announcements	"Security violation notification (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G3)" on page 5-59							x	x	x
Terminal Translation Initialization	"Use terminal translation initialization" on page 5-46					G3r	x	x	x	x
Toll Analysis	"Toll analysis (G3 only)" on page 5-19 "Toll analysis" on page 7-7 "Toll analysis" on page 8-5					x	x	x	x	x

Continued on next page

Table 18-1. Large Business communications systems security tools by release — *Continued*

Feature	See Section/Page	S75	S85	G1	G2	G3V1	G3V2	G3V3	G3V4	ECS R5 & later
Traffic Measurements and Performance	"Traffic measurements and performance" on page 5-55 "SAT, Manager I, and G3-MT reporting" on page 7-14 "SAT, Manager I, and G3-MT reporting" on page 8-10	x	x	x	x	x	x	x	x	x
Trunk Administration	"Trunk administration" on page 5-9	x	x	x	x	x	x	x	x	x
Trunk-to-Trunk Transfer	"Disable transfer outgoing trunk to outgoing trunk" on page 5-44	x	x	x	x	x	x	x	x	x
Trunk-to-Trunk Transfer (all trunks)	"Disallow trunk-to-trunk transfer" on page 5-43							x	x	x
Void Customer Passwords	"Require passwords" on page 5-28	R1V2 R1V3		x		x	x	x	x	x
World Class Routing	"Known toll fraud activity" on page 2-4 "World class routing (Communication Manager, MultiVantage Software, DEFINITY ECS and DEFINITY G2.2 and G3)" on page 5-24 "Use world class routing restrictions" on page 5-49				G2.2	all except G3iV1	x	x	x	x

Non-supported products

19

Below are listed the products Avaya no longer supports as of the given dates.

As of December 31, 2002

As of December 31, 2002, Avaya will no longer support these products:

- AVP w/ Y2k Software Update
- AUDIX R1 Prior to V8
- AUDIX R1 V8:2 w/ Y2k Update, QPPCN from V8
- AVP Y2k Patch Only
- Auto Attendant Software

As of December 31, 2001

As of December 31, 2001, Avaya will no longer support these products:

- AP16 CMS
- Integrated Solutions III (IS-III) on System 25/DEFINITY
- Merlin Legend CMS

As of December 31, 2000

As of December 31, 2000, Avaya no longer supports these products:

- Integrated Solutions II (IS-II)
- Integrated Solutions III (IS-III) on Legend

As of September 30, 2000

As of September 30, 2000, Avaya no longer supports these products:

- INTUITY Lodging
- R1.1, QPPCN from R1.0
- INTUITY Interchange (pre 5.1)
- INTUITY High Capacity Option (pre 4.4)
- Fax Attendant
- Fax Attendant w/ Y2k Software Update
- Auto Attendant Software w/ Y2k Software Update

As of December 31, 1999

As of December 31, 1999, Avaya no longer supports these products:

- CMS R2 3B2
- CMS R3V1, V2, V4
- CentreVu Supervisor V1
- CONVERSANT V3.0
- CONVERSANT V3.1.1, 4.0, 4.0i
- CONVERSANT V3.1.1 INTRO
- CONVERSANT V2.1
- DEFINITY AUDIX pre 3.1
- INTUITY AUDIX 3.3 (IP55), QPPCN from IA 3.2 and prior
- INTUITY AUDIX 3.3 (IP55), QPPCN from R3.3 non-IP55
- INTUITY AUDIX 3.3 (IP55)
- INTUITY AUDIX 3.3 International (PTS Load)
- INTUITY CONVERSANT V5.0
- INTUITY CONVERSANT V6.0
- INTUITY VS on Merlin Legend, QPPCN to R3.3 (IP55) or 4.4
- INTUITY AUDIX 4.0-4.2

Links to additional security information

20

About IP and network security

As IP and network technology advances, so do ways to abuse the technology. This appendix provides links to various references you can use to enhance your own knowledge of security issues.

Avaya products to enhance security

Avaya offers a security gateway that can protect your VoIP environment to provide for a 24x7 architecture. Combining VPN access and H.323 stateful firewall delivers the best overall security blanket to run anywhere in the world. More information is available at http://www.avaya.com:

- Hover over/click **Products and Services**
- Click **VPN and Security**

White papers

- Security and the Avaya™ S8700 Media Server
- Security and the Avaya™ S8300 Media Server
- Security in Converged Networks

Books and articles

- *Hacking Exposed: Linux (Second Edition*)
  Brian Hatch, James Lee
  ISBN: 0072225645
- *Writing Secure Code (Second Edition)*
  Michael Howard, David C. LeBlanc
  ISBN: 0735717228

- *RedHat Linux 8 Bible*
  Publisher: John Wiley & Sons
  ISBN: 0764549685
- *Anti-Hacker Tool Kit*
  Keith J. Jones, Bradley C. Johnson, Mike Shema
  ISBN: 0072222824
- *Hacking Exposed: Network Security Secrets and Solutions* (Fourth Edition)
  Stuart McClure, Joel Scambray, George Kurtz
  ISBN: 0072227427
- *Real World Linux Security* (Second Edition)
  Bob Toxen
  ISBN: 0130464562
- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*
  Bruce Schneier, Phil Sutherland (Ed)
  ISBN: 0471128457

Web sites

- Avaya Security Advisories web site

  http://support.avaya.com/japple/css/japple?PAGE=avaya.css.OpenPage&temp.template.name=SecurityAdvisory
- The Unofficial 802.11 Security Web Page

  http://www.drizzle.com/~aboba/IEEE/
- SANS Information Security Reading Room

  http://www.sans.org/rr/
- Center for Internet Security

  http://www.cisecurity.org/
- Internet Storm Center

  http://isc.incidents.org/
- Security Focus

  http://www.securityfocus.com/

Glossary

A

AAR
Automatic Alternate Routing

ACA
Automatic Circuit Assurance

ACD
Automatic Call Distribution

ADAP
AUDIX Data Acquisition Package

AFRL
Alternate Facility Restriction Level

AMIS
Audio Messaging Interface Specification

ANI
Automatic Number Identification

APLT
Advanced Private Line Termination

ARS
Automatic Route Selection, replaced by WCR in DEFINITY G2.2

AUDIX
Audio Information Exchange

AVP
AUDIX Voice Power

Access
The act of entering into a PBX system.

Account Code
A number (1 to 15 digits) that can be required when originating toll calls or WCR network calls.

Adjunct
Equipment that connects to a PBX port and interacts with the PBX system to provide a service, such as voice mail, automated attendant, and call traffic reporting.

Administer
Access or change the parameters associated with the services or features of the PBX system.

Alternate Facility Restriction Level
Sets time-dependent limits on access to routing patterns.

AMIS Analog Networking
An AUDIX Voice Mail System feature that connects the AUDIX Voice Mail System to other voice mail systems to exchange messages. Call Delivery is a service of AMIS Analog Networking.

ARS dial tone
The dial tone callers hear after they enter the ARS feature access code.

Attendant
The operator of the console.

Attendant Console
An electronic call-handling position with push-button control. Used by attendants to answer and place calls and to manage and monitor some of the PBX operations.

AUDIX Voice Mail System
An Avaya adjunct that provides voice mail and automated attendant services.

Authorization Code
A security code used with Remote Access to prevent unauthorized access or egress. A dialed code that can raise the Facility Restriction Level or Class of Restriction (COR) of the trunk used to place an outgoing call. An authorization code can also be used in preference to or in combination with a barrier code to protect against unauthorized use of Remote Access trunks.

Automated Attendant
Adjunct equipment that performs the services of an attendant, such as directing calls to individuals or departments.

Automatic Circuit Assurance
Detects short and long holding times and visually notifies a designated station when corresponding thresholds are exceeded.

B

BCMS
Basic Call Management System

Barrier Code
A security code used with the Remote Access feature to help prevent unauthorized access.

Basic Call Transfer
A type of transfer where the AUDIX Voice Mail System validates that the number of digits entered matches the length of extensions in the dial plan, and then transfers the call to the switch before disconnecting.

BCMS Measurements
Reports traffic patterns for measured trunk groups.

C

CAS
Centralized Attendant Service, Call Accounting System

CDR
Call Detail Recording

Call Forwarding
A set of features that allow calls destined for an extension to be redirected to another extension, designated during activation.

Call Forwarding All Calls (Follow Me)
A feature that allows calls destined for an extension to be redirected to another extension, designated during activation, regardless of the busy or idle state of the called extension. Intended to redirect calls to the called party when he or she is away from his or her desk.

Call Forwarding (Off Net)
A function of the Call Forwarding Follow Me feature that allows a user to forward all calls to a telephone in the public network.

Call Forward Off/On-Net
A function of the Call Forwarding Follow Me feature that allows a user to Call Forward outside the switch (Off-Net), or inside AND outside the switch to non-toll locations (Off/On-Net).

CMS
Call Management System

CO
Central Office

COR
Class of Restriction

COS
Class of Service

CSM
Centralized System Management

Call Detail Recording
Records call information when specified trunk groups are used for the call.

Called Party Restrictions
The calling privileges or restrictions that can be placed on the receiving station or trunk.

Calling Party Restrictions
The calling privileges or restrictions that can be placed on the originating station or trunk.

Call Management System
An adjunct processor that collects data from an ACD and generates reports to be stored or displayed regarding status of agents, splits, and trunks.

Call Vector
A set of commands to be performed for an incoming or internal call. See *Call Vectoring*.

Call Vectoring
Directs incoming and internal calls to various destinations: on- or off-premises destinations, a hunt group or split, or a specific call treatment, such as an announcement, forced disconnect, forced busy, or delay treatment. Calls access these destinations, or vectors, through Vector Directory Numbers (VDNs).

Central Office
The location housing the telephone switching equipment that provides local telephone service and access to toll facilities for long-distance calls.

Class of Restriction
A number (0 through 63) that specifies the calling privileges and limitations assigned to stations, Remote Access users, and trunk groups. For DEFINITY G3rV1, G3i-Global, and G3V2 and later, CORs have been increased to 96; thus, the number is 0 through 95.

Class of Service
For DEFINITY G2 and System 85, specifies the calling privileges and limitations assigned to the station. For DEFINITY ECS, DEFINITY G1, G3, and System 75, a number (0 through 15) that specifies if users can activate Automatic Callback, Call Forwarding, Console Permissions, Data Privacy, and Priority Calling features. For G3V2 and later, also specifies additional COR feature restrictions.

CMS Measurements
Measures traffic patterns and time on calls to compare them with preset traffic counts and time limit thresholds.

Coverage Path
The order in which calls are redirected to alternate answering positions.

Customer Premises Equipment-Based System
A customer's PBX, voice mail, or voice processing system.

D

DAC
Dial Access Code (see *Trunk Access Code*)

DCS
Distributed Communications System

DDD
Direct Distance Dialing

DID
Direct Inward Dialing

DISA
Direct Inward System Access

Digit Conversion
A process used to convert specific dialed numbers into other dialed numbers.

Direct Inward Dialing
Allows an incoming call from the public network (not FX or WATS) to reach a specific telephone without attendant assistance. DID calls to DID-restricted telephone lines are routed to an attendant or recorded announcement, depending on the option selected.

E

EPSCS
Enhanced Private Switched Communications Service

ETN
Electronic Tandem Network

Enhanced Call Transfer
An AUDIX Voice Mail System feature that provides security by interacting with the PBX system to validate that the number entered by an AUDIX Voice Mail System caller is a valid extension number in the dial plan.

Enhanced Private Switched Communications Service
A private telecommunications network that provides advanced voice and data telecommunications services to companies with many locations.

Electronic Tandem Network
A tandem tie trunk network that has automatic call routing capabilities based on the number dialed and the most preferred route available at the time the call is placed. Each switch in the network is assigned a unique private network office code (RNX), and each voice terminal is assigned a unique extension number.

Extended User Administration of Redirected Calls
Feature that allows station users to select one of two previously administered call coverage paths assigned to them (for example, a work location coverage path or a remote work location coverage path) from any on-site extension or from a remote location (for example, home). Also provided is the ability to activate, change, or deactivate Call Forward Add or Call Forward Busy/Don't Answer from any on-site extension or from a remote location.

F

FAC
Feature Access Code; Facility Access Code

FEAC
Forced Entry of Account Code

FNPA
Foreign Numbering-Plan Area

FRL
Facility Restriction Level

FX
Foreign Exchange

Facility Access Code
The code required to access outgoing facilities (trunks).

Facility Restriction Level
Identifies where AAR/ARS/WCR calls can be made and what facilities can be used. FRLs range from 0 to 7 with the lower numbers being the most restrictive. In an ETN environment, it is passed along with the call as a Traveling Class Mark.

Facility Test Call
Allows a local voice terminal user or an INADS voice terminal user to call a trunk, touch-tone receiver, time slot or system tone to see if the facility is working properly.

Feature
A specifically defined function or service provided by the PBX system.

Feature Access Code
A code used to access a feature, such as ARS, Data Origination, Priority Calling and Call Pickup.

Foreign Exchange
A Central Office other than the one providing local access to the public telephone network.

Foreign Numbering-Plan Area Code
An area code other than the local area code. The FNPAC must be dialed to call outside the local geographic area.

Fully Restricted
A feature that denies outgoing calls, including dial access to trunks, and allows no incoming calls from Public Network trunks.

G

G3-MA
Generic 3 Management Application

G3-MT
Generic 3 Management Terminal

H

Hacker
A criminal who attempts to penetrate PBX systems to gain unauthorized access to their features.

I

ICC
Interexchange Carrier Code

INADS
Initialization and Administration System

INPA
Improved Numbering Plan Address

IXC
Interexchange Carrier

Intercept Tone
An alternating high and low tone; indicates a dialing error or denial of the service requested.

Invalid Attempt
A single invalid Remote Access (barrier code), authorization code, or login access attempt.

L

LEC
Local Exchange Carrier

M

Manual Terminating Restriction
Prevents the station from receiving calls other than those originated by the attendant.

MERLIN Attendant
An Avaya adjunct that provides voice mail and automated attendant services for use with the MERLIN LEGEND Communications System and MERLIN II Communications System R3.

Message Indicator Lamp
The light on a voice terminal that is activated by the attendant or a voice mail adjunct when there is a message for the user.

Miscellaneous Restrictions
Restricts certain CORs from calling other CORs.

Miscellaneous Trunk Restrictions
Restricts certain stations from calling certain trunk groups.

N

NETCON
Network Control (port) data channel

NMS
Network Management System

NPA
Numbering Plan Area

NSAC
National Service Assistance Center

Night Service
Provides different coverage paths for stations after business hours.

O

OTTOTT
Outgoing Trunk to Outgoing Trunk Transfer

Outcalling
An AUDIX Voice Mail System feature that alerts designated subscribers when a voice mail message is delivered to their voice mailbox.

Outgoing Trunk to Outgoing Trunk Transfer
Allows a controlling party, such as a station user or attendant, to initiate two or more outgoing trunk calls and then transfer the trunks together. The transfer removes the controlling party from the connection and conferences the outgoing trunks. Alternatively, the controlling party can establish a conference call with the outgoing trunks and then drop out of the conference, leaving only the outgoing trunks on the conference connection.

Outward Restricted
Restricts the station from placing outgoing calls over specified trunks.

P

PARTNER Attendant
An Avaya adjunct that provides voice mail and automated attendant services for use with the PARTNER II Communications System.

PBX
Private Branch Exchange

PC
Personal Computer

Personal Station Access (PSA)
A feature that allows multiple users to work at the same voice terminal location at different times. PSA provides capabilities that are similar to TTI, but for a single station.

PGN
Partitioned Group Number

PNA
Private Network Access

Private Network
A network used exclusively for handling the telecommunications needs of a particular customer.

Private Network Office Code (RNX)
The first three digits of a 7-digit private network number. These codes are numbered 220 through 999, excluding any codes that have 0 or 1 as the second digit.

Public Network
The network that can be openly accessed by all customers for local or long-distance calling.

R

RAU
Remote Administration Unit

RNX
Route Number Index (See *Private Network Office Code*)

RHNPA
Remote Home Numbering Plan Area

RPSD
Remote Port Security Device

Random Number Generators
Devices frequently used by hackers to decipher passwords and access codes.

Redirect
A feature that sends an incoming call to another station for coverage.

Referral Call
An internally-generated call that terminates to a designated destination and indicates an event such as a security violation.

Remote Access
A feature that provides remote callers access to most of the PBX features.

Remote Access Dial Tone
A special dial tone for the Remote Access feature that can be used after the caller enters the barrier code.

Remote Home Numbering Plan Area Code
A foreign numbering-plan area code that is treated as a home area code by the Automatic Route Selection (ARS) feature. Calls can be allowed or denied based on the area code and the dialed Central Office (CO) code rather than just the area code. If the call is allowed, the ARS pattern used for the call is determined by these six digits.

Remote Port Security Device
An Avaya product that helps protect administration and maintenance ports from unauthorized access.

Remote User Administration of Call Coverage
A feature that allows calls that are forwarded off of the network to be tracked for busy or no-answer conditions and to be brought back for further call coverage processing in such cases.

S

SAT
System Access Terminal

SDN
Software Defined Network

SMDR
Station Message Detail Recording

SPM
System Programming and Maintenance

SVN
Security Violations Notification

Security Violation
An event that occurs when the number of invalid access attempts (login, Remote Access, or authorization code) exceeds the customer-administered threshold of the number of invalid access attempts permitted within a specified time interval.

Security Violations Measurement Report
Monitors Remote Access and administration ports for invalid login attempts and attempts to enter invalid barrier codes.

Security Violations Notification Feature
Detects attempts to enter barrier codes or authorization codes, as well as attempts to log in to Remote Access or administration ports. Alerts a designated station of threshold violations.

Service Observing
The monitoring of actual calls in progress for security purposes.

Station Message Detail Recording
Creates call records for incoming and outgoing calls.

System Manager
A person responsible for specifying and administering features and services for the PBX system.

T

TAC
Trunk Access Code

TCM
Traveling Class Mark

TSC
Technical Service Center

TTI
Terminal Translation Initialization

Tandem Tie Trunk Network
A private network that interconnects several customer switching systems by dial repeating tie trunks. Access to the various systems is dictated by the codes that are individually dialed for each system.

Telecommunications Fraud
The unauthorized use of a company's telecommunications system. Also called any of the following: telephone abuse, toll fraud, phone fraud, call fraud.

Tie Trunk
A telecommunications channel that directly connects two private switching systems.

Toll Analysis
Specifies the routing of toll calls, including numbers to be assigned to the Restricted Call List and the Unrestricted Call List.

Toll Restriction
Prevents the user from making toll calls unless the number is specified on an Unrestricted Call List.

Trunk Group
Telecommunications channels assigned as a group for certain functions that can be used interchangeably between two communications systems or Central Offices.

Trunk Access Code
A digit assignment assigned during trunk administration that identifies the trunk.

U

UCL
Unrestricted Call List

UDP
Uniform Dial Plan

Uniform Dial Plan
A feature that allows a unique 4- or 5-digit number assignment for each terminal in a multi-switch configuration such as a distributed communications system (DCS) or main-satellite tributary configuration.

V

VDN
Vector Directory Number

VF
Virtual Facility

VNI
Virtual Nodepoint Identifier

Vector Directory Number
An extension that provides access to the Call Vectoring feature on the switch. Call vectoring allows a customer to specify the treatment of incoming calls based on the dialed number.

Virtual Facility
A call routing facility not defined by the physical facility (trunk) over which calls are routed.

Voice Terminal
A single-line or multi-appearance telephone.

W

War Dialer
Slang. A device used by hackers that randomly dials telephone numbers (generally 800 numbers) until a modem or dial tone is obtained.

WATS
Wide Area Telecommunications Service

WCR
World Class Routing

Wide Area Telecommunications Service
A service that allows calls to a certain area or areas for a flat-rate charge based on expected usage.

World Class Routing
For DEFINITY ECS and DEFINITY G2.2 and G3, provides flexible network numbering plans.

Index

Numerics

0 calls, 5-24, 5-55
00 calls, 5-24
01 calls, 5-35
  blocking, 11-15
010 calls, 5-35
011 calls, 5-35, 5-55
10xxx calls, 2-7, 5-24
10xxx01 calls, 5-35
10xxx11 calls, 5-35
2-way trunk groups, 5-16
3-way COR check, 5-17, 5-50
3-way-conferencing, 7-35
6-digit screening, 2-8
800 numbers, 2-7, 4-2, 5-3, 15-1
800 service, 7-55, 7-58
  trunks, 4-2
911 number, 5-15
950 numbers, 2-7
976-look-alike numbers, 2-8

A

AAR, see Automatic Alternate Routing
AAR/ARS
  analysis, 5-20
  Feature Access Code, 5-9
Abbreviated Dialing
  Feature Access Code, 5-9
abuse
  internal, 2-8, 4-8
access
  administration and maintenance, 4-4
Access Security Gateway feature
  loss of an ASG Key, 16-8
  restarting temporarily disabled ASG, 16-7
Access Security Gateway, interactions, 16-8
account code, 7-57, 7-59
  CDR, 5-18
  undefined, 5-54, 6-60, 6-63
ADAP, see AUDIX Data Acquisition Package
add/change login command, 13-7
adjunct
  changing default password, 4-4
  security, 4-6
administrable logins, 5-52
administration and maintenance access, 4-4
administration port, 5-55
Advanced Private Line Termination, 5-16
  Off-Net, 5-17
after-hours calling
  preventing, 5-33
  restricting, 5-19
alarm
  ACA, 5-56
  long holding time, 8-11
  sending to attendant, 5-57
alternate carrier access, 2-6
Alternate Facility Restriction Level, 5-19
  preventing after-hours calling, 5-33
AMIS Networking, 7-26
ANI, see Automatic Number Identification
area codes
  restricting calls, 8-6
ARS Measurement Selection, 5-56, 7-15, 8-11
ARS, see Automatic Route Selection
attendant
  call routing, 5-31, 5-50, 10-1
  CAS
    call routing, 5-31
  reporting suspicious calls, 4-8, 5-50
  sending alarms/reports, 8-12
  transferring, 5-31
attendant console, 5-70, 7-27, 8-13, 8-17
  Facility Restriction Level, 5-32
  physical security, 4-9
attendant control
  activating, 5-40
  Remote Access calls, 5-38
  specific extensions, 5-38
  trunk group access, 5-39
Audio Message Interchange Specification, 7-26
AUDIX Data Acquisition Package, 1-10, 7-19, 7-20, 8-13
AUDIX Voice Mail System
  Call Detail Recording, 7-19, 8-13
  disabling transfer out, 7-28
  logins, 7-22
  password
    changing, 14-1
    protecting, 7-22
  protecting the system, 7-16
  security checklist, 17-4
  security considerations, 7-23
  session termination values, 7-20
AUDIX Voice Power System, 7-39
  automated attendant, 7-4, 8-16, 8-17, 8-20, 8-22
  limiting outbound transfers, 7-32, 7-62
  Lodging, 7-4
  password
    changing, 14-2
    protecting, 7-39, 7-61
  protecting, 7-30, 7-39
  security checklists, 17-6
  security measures, 7-40, 7-62
  security tips, 7-31, 7-39, 7-61
  traffic reports, 7-30
  Transfer Only to System Subscribers, 7-32, 7-62

authorization code, 5-3, 5-19, 5-22, 5-29, 5-30, 7-57, 7-59
  invalid login attempts, 5-64
  maximum allowed, 5-9
  monitoring usage, 5-30
  Network Access Flag set, 5-9
  removing, 5-30
  Time-Out to Attendant, 5-36
  usage patterns, 6-13, 6-60
  used with barrier code, 5-7
  VDN, 5-9
Authorization Code Violations Status Report, 5-64, 5-66
auto dial button, 4-8
  programming passwords, 7-3
automated attendant, 2-1, 2-5, 4-3, 7-19, 7-25, 7-28, 7-32, 7-40
  adjunct equipment, 8-3
  AUDIX Voice Mail System, 8-16
  AUDIX Voice Power System, 8-17, 8-20, 8-22
  CONVERSANT Voice Information System, 8-18
  DEFINITY AUDIX Voice Messaging System, 8-18
  DEFINITY Communications System, 8-1
  INTUITY System, 8-18
  MERLIN MAIL R3 Voice Messaging System, 8-20
  MERLIN MAIL Voice Messaging System, 8-19, 8-20
  MERLIN MAIL-ML Voice Messaging System, 8-20
  nested, 8-14
  PARTNER MAIL System, 8-21, 8-22
  PARTNER MAIL VS System, 8-21, 8-22
  ports, 8-5
  restricting menu options, 8-5
  security tools, 8-2
  symptoms of abuse, 8-9
  System 75, 8-1
  System 85, 8-1
  toll fraud detection, 8-8
Automatic Alternate Routing, 5-25
  analysis, 5-20
  setting FRLs, 5-15
Automatic Call Restriction Reset, 6-60
Automatic Circuit Assurance, 5-56, 8-11
  referral calls, 5-57
Automatic Number Identification, 15-2
Automatic Route Selection, 5-20
Automatic Timeout, 6-60

B

barrier code, 5-3, 5-5, 5-29, 5-30, 5-36, 6-12, 6-14, 6-60, 6-63
  aging, 5-67, 13-11
  COR, 5-7, 5-14, 5-30
  COS, 5-7
  default expiration dates and upgrades, 5-67
  invalid entry, 5-62
Basic Call Transfer, 7-23, 7-43
BasicWorks
  security checklists, 17-8
BCMS Measurements, 5-58
beeper scam, 2-7
bridging to outbound call, 7-33, 7-34, 7-35
bulletin board, 2-6, 7-25
Busy Verification, 5-70, 7-16, 8-12
  button, 5-70
button
  act-tr-grp, 5-40
  Alternate Facility Restriction Level, 5-34
  asvn-call, 5-61
  auto dial, 4-8, 7-3
  Busy Verification, 5-70, 7-16, 8-13
  deact-tr-grp, 5-40
  Login SVN, 5-61
  lsvn-call, 5-61
  lsvn-halt, 13-3
  night service, 5-10
  Remote Access SVN, 5-61
  rsvn-call, 5-61
  rsvn-halt, 13-5
  trk-ac-alm, 5-42
  Verify, 5-70, 8-13

C

call
  ACA referral, 5-57
  allowing to specified numbers, 7-10, 8-6
  disallowing outbound, 7-26, 8-16
  FX, 7-9
  international, 5-34, 5-35
  monitoring, 5-56, 5-69, 8-11
  private network, 5-16, 7-9
  public network, 5-20
  Remote Access
    sending to attendant, 5-36
  Tandem Tie Trunk, 5-39
  toll, 8-5
  Transfer Out of AUDIX, 8-16
  trunk-to-trunk, 5-56, 8-11
  volume
    tracking, 5-55
  WATS, 7-9
Call Accounting System Plus, 5-54
Call Accounting System reports, 6-6, 6-13, 6-60, 6-63, 7-35, 7-37, 7-47, 7-56, 7-58, 7-60
call attempt
  invalid, 5-31, 5-54, 5-59, 6-60, 6-62, 6-63, 8-5, 8-6
Call Detail Recording, 2-4, 5-30, 7-13, 7-19, 8-13
  account code, 5-18
  outgoing voice, 7-21, 8-15
  required with FEAC, 5-24
  reviewing for abuse, 5-54
call diverters, 2-7
call flow through PBX system, 10-1
Call Forward Follow Me, 5-17, 7-7, 8-4
Call Forward Off/On-Net, 5-18

Call Forward Off-Net, 5-17, 7-7, 8-4
Call Forwarding, 2-8, 5-70
  Feature Access Code, 5-9
call list, 7-7, 8-5
  free, 5-20
  specifying, 5-19
  unrestricted, 5-19, 7-29
Call Management System
  helplines, 9-2
  log, 5-58
  Measurements, 5-58
  securing, 4-6
  security tips, 9-1
call pager, 7-29
  scam, 2-7
Call Prompting, 5-11
call sell operations, 2-2
Call Traffic Report, 7-14, 8-10, 8-13
Call Vectoring, 5-10, 5-11, 5-33
call volume increases, 5-55
calling
  out-of-hours, 6-6, 6-13, 6-59
  restricting by area, 7-8
calling cards, 2-3, 2-5, 2-7
CallMaster PC
  security tips, 9-3
CAS Plus, see Call Accounting System Plus
CDR, see Call Detail Recording
cellular phones, 7-3
Central Office restrictions, 5-22
Centralized Attendant Service, 5-31
Centralized System Management
  securing, 4-6
change remote-access command, 13-6
change station command, 5-70
change system-parameters features command, 13-7
change system-parameters features security command, 13-6
change system-parameters security command, 13-2, 13-4
circuit pack
  TN744 Call Classifier, 5-40, 5-41
  Tone Detector, 5-40, 5-41
Class of Restriction, 5-14, 5-31, 7-7, 8-3
  3-way calling, 5-17
  authorization code, 5-14
  barrier code, 5-14
  blocking access, 5-11
  Facility Access Trunk test option, 5-40
  maximum allowed, 5-14, 7-7, 8-3
  outward-restricted, 5-30
  Remote Access, 5-30
  VDN, 5-16
Class of Service, 5-17, 7-7, 8-4
clear measurements security-violations command, 5-52
CMS, see Call Management System
CO trunks, 4-2
code
  account, 7-57, 7-59
  authorization, 4-2, 5-3, 7-36, 7-46, 7-57, 7-59, 7-60
  barrier, 4-2, 5-3, 5-5
  restriction, 5-16
Code Restriction Level, 8-4
command
  add/change login, 13-7
  change remote-access, 13-6
  change station, 5-70
  change system-parameters features, 13-7
  change system-parameters features security, 13-6
  change system-parameters security, 13-2, 13-4
  clear measurements security-violations, 5-52
  disable remote-access, 13-7
  enable remote-access, 13-6
  list bcms trunk, 5-58
  list call forwarding, 5-70
  list data module, 4-7
  list history, 5-68
  list hunt group, 4-7
  list measurements, 5-56
  list performance, 5-56
  monitor, 5-46
  monitor security-violations, 5-59, 5-64
  status remote access, 5-12
  verify, 5-70
Committee of the Alliance for Telecommunications, 1-8
con games, 2-6, 2-8
Conference Reservation and Control System
  protecting the system, 9-4
  security checklists, 17-46
conferencing, 7-35
console
  attendant, 5-70, 7-27, 8-13
  key, 5-40
  permissions, 5-18
converged networks, 3-1
CONVERSANT Voice Information System
  automated attendant, 8-18
  password
    changing, 14-2
  remote maintenance board, 7-33
  security checklists, 17-12
  security tips, 7-35
COR-to-COR restrictions, 5-16, 5-49
  NETCON, 4-7
credit card calls, 2-3, 2-5, 2-7

D

DAC, see Dial Access Code
data channel, 4-3
Data Origination
  Feature Access Code, 5-9

Data Privacy
Feature Access Code, 5-9
Data Restriction
Feature Access Code, 5-9
DCS, see Distributed Communication System
default passwords
changing, 4-4
DEFINITY AUDIX Voice Messaging System
automated attendant, 8-18
logins, 7-22
password
changing, 14-4
protecting, 7-22
protecting the system, 7-16
security checklists, 17-4
security considerations, 7-23
DEFINITY Communications System
automated attendant, 8-1
detecting toll fraud, 5-50
restricting unauthorized outgoing calls, 5-13
security goals and tools, 4-10
security measures, 5-28
security tips, 5-2
security tools by release, 18-1
voice mail, 7-4
DEFINITY Communications System G1
password
changing, 14-5
security checklists, 17-14
DEFINITY Communications System G2
password
changing, 14-6
security checklists, 17-20
DEFINITY Communications System G3
password
changing, 14-5
security checklists, 17-14
DEFINITY ECS, see DEFINITY Enterprise Communications Server
DEFINITY Enterprise Communications Server
detecting toll fraud, 5-50
restricting unauthorized outgoing calls, 5-13
security checklists, 17-14
security measures, 5-28
security tips, 5-2
voice mail, 7-4
Dial Access Code, 5-41, 7-2
dial tone
AAR, 5-43
accessing, 2-5
ARS, 5-20, 5-43
authorization code, 5-8
barrier code, 5-7
Remote Access, 5-3
suppressing, 5-42
switch, 5-43
transferring, 2-5
DID Restriction, 8-4
digit conversion, 5-25, 5-35, 5-36
Digital Port Emulation Mode, 7-30
DIMENSION PBX System
security checklists, 17-24
direct dial access, 5-9, 5-20
Direct Distance Dialing, 2-1
Direct Inward Dialing, 15-1
Direct Inward System Access, 2-4, 2-5, 4-2, 15-2
MERLIN LEGEND Communications System, 6-6
DISA, see Direct Inward System Access
disable remote-access command, 13-7
disabling Remote Access, 12-3
disallowing outside calls, 7-26, 8-3, 8-16
Distributed Communication System, 5-44, 5-57
Trunk Turnaround, 5-44
dumpster diving, 2-6

E

Electronic Tandem Network, 5-20, 5-45
E-mail administration
Viruses, 7-19
employee
abuse, 2-8, 4-8, 9-9
education, 4-8
emulation programs
PC-based, 4-6
enable remote-access command, 13-6
Enhanced Automated Attendant, 7-19, 8-14
Enhanced Call Transfer, 7-24, 7-26, 7-30, 8-2, 8-16
coverage limitations, 7-24
EPSCS network, 5-17
equipment rooms
physical security, 4-9
Escape to Attendant, 7-24
ETN, see Electronic Tandem Network
Extended User Administration of Redirected Calls, 5-27

F

FAC, see Feature Access Code
Facility Restriction Level, 5-18, 5-19, 7-6, 8-2, 8-5
attendant console, 5-32
MERLIN LEGEND System, 6-10
overriding, 5-19
providing individualized calling privileges, 5-31
suggested value, 5-32
Facility Test Call, 5-42
access code, 5-41, 7-2
denying, 5-11
disabling, 5-40
FEAC, see Forced Entry of Account Code

Feature Access Code, 2-5
Abbreviated Dialing, 5-9
ARS/AAR, 5-9
Call Forwarding, 5-9
Data Origination, 5-9
Data Privacy, 5-9
Data Restriction, 5-9
Facility Test Calls, 5-9
firewalls, 3-2
FNPA, see Foreign Numbering Plan Area
Forced Entry of Account Code, 5-24, 5-47
Forced Password Aging, 5-52
Foreign Numbering Plan Area, 5-34, 5-35, 5-37
free call list, 5-20
AAR/ARS calls, 5-20
TAC calls, 5-20
FRL, see Facility Restriction Level
Fully Restricted Service, 5-16, 5-31
FX trunks, 4-2

G

G3-MA, see Generic 3 Management Application
G3-MT, see Generic 3 Management Terminal
Generic 3 Management Application, 4-6, 5-59
invalid login attempts, 5-64
Generic 3 Management Terminal, 5-55, 5-59, 7-14, 8-10

H

hackers, 2-2
800 numbers, 4-2
accessing automated attendant systems, 4-3
random number generators, 2-2, 4-2
Highest Extension, 8-19
holding time
long, 5-55, 5-56, 5-57, 8-11
short, 5-53, 5-54, 5-55, 5-56, 5-57, 6-63, 8-11, 15-1

I

INADS port, 5-51
individual and group-controlled restrictions, 5-21
individualized calling privileges
providing, 5-31
intercept tone, 5-25
call routing, 5-31
intercept treatment, 5-38
Interexchange Carrier, 2-7, 6-62
internal abusers, 2-8
international
calls, 5-34, 5-35
disallowing, 6-62
operator, 5-35
INTUITY AUDIX Voice Messaging System, 7-41
logins, 7-22
password
protecting, 7-22, 7-42
protecting, 7-41
protecting the system, 7-16
security checklists, 17-4
security considerations, 7-23
INTUITY System
automated attendant, 8-18
password
changing, 14-6
Inward Restriction, 8-4
IP
security, 3-1
IP telephony networks, 3-1
IXC, see Interexchange Carrier

L

LDN, see Listed Directory Number
LEC, see Local Exchange Carrier
list bcms trunk command, 5-58
list call forwarding command, 5-70
list data module command, 4-7
list history command, 5-68
list hunt group command, 4-7
list measurements command, 5-56
list performance command, 5-56
Listed Directory Number, 5-10, 7-27, 8-17
lobby
telephones, 5-38
Local Exchange Carrier, 2-7
log
Real-Time Exception, 5-58
Trunk Group Exceptions, 5-58
login
invalid attempts, 5-59
Login Violations Status Report, 5-64, 5-65
logins, 5-52
assigned during installation, 5-29
bcms, 5-28, 5-46
browse, 5-28, 5-46
cust, 5-28, 5-46
invalid attempts, 5-60, 5-62
NMS, 5-28
rcust, 5-28, 5-46
storing, 4-6
logoff screen, 5-12
looping, 2-3, 2-7
loop-start trunks, 6-15, 6-62
trunk to trunk transfers, 6-62
Lowest Extension, 8-19

M

maintenance access, 4-7
maintenance port, 4-9
  target of abuse, 2-4
Malicious Call Trace, 5-68
Manager I, 7-14
  reporting, 5-55, 8-10
Manager III/IV, 4-6
Manual Terminating Line Restriction, 8-4
Measurement Selection
  ARS, 5-56, 7-15, 8-11
measurements
  BCMS, 5-58
  CMS, 5-58
MERLIN Attendant, 8-19, 8-20
MERLIN II Communications System
  protecting DISA, 6-5
  security checklists, 17-27
  security goals and tools, 4-14
  security tips, 6-5
  voice mail, 7-35
MERLIN LEGEND Communications System
  allowed and disallowed lists, 6-9
  preventative measures, 6-8
  Remote Access, 6-12
  security checklists, 17-29
  security goals and tools, 4-14
  setting facility restriction levels, 6-10
  star codes, 6-9
  voice mail, 7-38
MERLIN LEGEND Mail Voice Messaging System, 7-45
  automated attendant
    protecting, 7-45
  password
    changing, 14-8
    protecting, 7-46
MERLIN MAIL R3 Voice Messaging System, 7-45
  automated attendant, 8-20
    protecting, 7-45
  password
    changing, 14-8
    protecting, 7-46
  security checklists, 17-36
  security tips, 7-46
MERLIN MAIL Voice Messaging System, 7-45
  automated attendant, 8-19, 8-20
    protecting, 7-45
  password
    changing, 14-7
    protecting, 7-36, 7-46
  ports, 7-35
  protecting, 7-35
  security checklists, 17-32
  security tips, 7-36, 7-46
MERLIN MAIL-ML Voice Messaging System, 7-45
  automated attendant, 8-20
    protecting, 7-45
  password
    changing, 14-7
    protecting, 7-46
  security checklists, 17-34
  security tips, 7-46
MERLIN Plus Communications System
  protecting Remote Call Forwarding, 6-60
  protecting Remote Line Access, 6-59
  Remote Line Access, 6-59
  security checklists, 17-39
  security goals and tools, 4-14
Message Delivery, 7-21, 7-26, 8-15
Miscellaneous Trunk Restrictions, 7-6, 7-7, 8-3, 8-4
modem
  flashing switch-hook, 4-3
  protecting ports, 4-3
monitor command, 5-46
Monitor I, 5-55, 7-14, 8-10, 8-11, 8-13
monitor security-violations command, 5-59, 5-64
Multimedia Communications Exchange Server
  security checklists, 17-40
Multipoint Conferencing Unit
  protecting the system, 9-4
  security checklists, 17-46

N

NETCON, see Network Control data channel
Network 3, 5-38, 7-11, 8-7
network access
  unauthorized, 2-1
Network Control data channel, 4-3, 4-7
Network Corporate Security, 7-4
Network I Toll Access Code, 5-18, 8-5
network, IP, 3-1
night
  service, 5-10
  shut-down procedure, 5-21
North American Dialing Plan, 5-36, 11-1
NSAC, see National Service Assistance Center
Numbering Plan
  area, 5-32, 11-10
  defining, 5-50

O

Observe Remotely feature, 5-70
Originating Line Screening, 6-62
Origination Restriction, 8-4
OTTOTT, see Outgoing Trunk to Outgoing Trunk Transfer

outcalling, 7-25, 7-40, 7-57, 7-59, 7-61
  limiting, 7-29, 7-44
Outgoing Trunk to Outgoing Trunk Transfer
  disabling, 5-44
Outward Restriction, 5-15, 5-17, 7-7, 8-4
overlapped sending, 5-49

P

Partitioned Group Number, 12-1
PARTNER Attendant, 8-21, 8-22
PARTNER II Communications System
  protecting the system, 6-61
  security checklists, 17-56
  security goals and tools, 4-19
  voice mail, 7-55
PARTNER MAIL System, 7-55, 7-58
  automated attendant, 8-21, 8-22
  outcalling, 7-57, 7-59
  password
    changing, 14-9
    protecting, 7-55, 7-58
  protecting, 7-55
  security checklist, 17-61
  security tips, 7-56, 7-58
PARTNER MAIL VS System, 7-55, 7-58
  automated attendant, 8-21, 8-22
  password
    changing, 14-9
    protecting, 7-55, 7-58
  protecting, 7-55
  security tips, 7-56, 7-58
PARTNER Plus Communications System
  protecting the system, 6-61
  security goals and tools, 4-19
  voice mail, 7-57
PassageWay Telephony Services
  security tips, 9-6
password
  security for administrator passwords, 7-17
passwords
  adjunct, 7-3
  aging, 5-52
  choosing, 4-5
  default, 2-4
  forced aging, 5-52
  general security measures, 4-9
  programs to crack, 2-2, 4-2
  protecting, 4-8
  storing, 4-6
PBX
  accessing, 2-5
  toll fraud, 4-1
peg counts, 5-55, 8-10
  high, 5-55
Personal Identification Number, 15-2
Personal Station Access, 5-25, 17-17
Personal Station Access (PSA), 5-25
PGN, see Partitioned Group Number
PNA, see Private Network Access
ports
  administration, 5-55, 5-62
  automated attendant, 8-3
  INADS, 5-51
  maintenance, 5-62
  MERLIN LEGEND Communications System, 6-7
  MERLIN MAIL Voice Messaging System, 7-35
  outward restricted, 7-8
  PARTNER MAIL System, 7-57
  PARTNER MAIL VS System, 7-57
  PBX, 7-6
  Remote Access, 5-59, 5-62
  security, 4-3, 4-6
  System Management, 5-59
  tip/ring, 6-62
  treated as station, 7-6
  usage data, 8-13
  used as station, 8-2
  voice, 7-29
  voice mail, 7-6
  Voice Mail Integrated, 6-7
private control networks, 3-2
Private Network Access, 5-25
product security checklists, 17-1

R

random number generators, 2-2, 4-2
recall signaling, 5-21
Recent Change History Report, 5-68
referral call
  SVN, 5-59
Remote Access, 2-1, 2-4, 2-5, 4-2
  800 numbers, 5-3
  attendant control of calls, 5-38
  Barrier Code Aging, 5-67
  DEFINITY Communications System, 4-2
  dial tone, 5-42
  dialing in
    800 service trunks, 4-2
    CO trunks, 4-2
    FX trunks, 4-2
  disabled during business hours, 5-38
  disabling, 5-3, 12-3
  invalid login attempts, 5-64
  kill, 13-6
  MERLIN II Communications System, 6-6
  MERLIN LEGEND Communications System, 6-12
  MERLIN Plus Communications System, 6-59
  permanently disabling, 13-13
  removing, 5-3
  setting up, 12-1

Remote Access, (continued)
Status Report, 5-64
status report, 5-64
System 25, 6-62
System 75, 5-2
System 85, 5-2
Violations Status Report, 5-65
Remote Administration Unit, 4-20, 6-61
Remote Call Forwarding, 6-15, 6-60
used with loop-start trunks, 6-15
Remote Home Numbering Plan Area, 5-37
Remote Line Access, 6-59
Remote Maintenance Board, 7-33
Remote Maintenance Device, 6-62
Remote Port Security Device, 16-1
remote service observing, 5-70
Remote System Administration
System 25, 6-63
Remote System Programming, 6-14
Remote User Administration of Call Coverage, 5-27
reports
Authorization Code Violations Status, 5-64
Call Accounting System, 6-6, 6-13, 6-60, 6-63, 7-35, 7-37, 7-47, 7-56, 7-58
call traffic, 7-14, 8-10, 8-13
distributed, 4-9
G3-MT, 5-55, 8-10
Manager I, 5-55, 8-10
Recent Change History, 5-68
Remote Access status, 5-64
SAT, 5-55, 8-10
securing, 4-9
Security Measurement, 5-52
Security Violations, 13-18
Security Violations Measurement, 5-60
Security Violations Status, 5-59
sending to attendant, 5-57
SMDR, 6-13, 6-60, 6-63, 7-13, 7-35, 7-37, 7-47, 7-56, 7-58, 7-60
traffic, 8-13
trunk group, 7-14, 8-10, 8-13
Restriction Override, 5-50
restrictions
calling party and called party, 5-15
individual and group-controlled, 5-21
originating station, 5-15
originating trunk, 5-15
switch translation, 7-30, 7-35
RHNPA, see Remote Home Numbering Plan Area
RMB, see Remote Maintenance Board
routing
patterns, 5-56
Time of Day, 5-24, 5-59
RPSD, see Remote Port Security Device

S

SAT, see System Administrator Tool
screening
6-digit, 2-8
securing the INADS port, 5-51
Security
administration and management, 3-3
administrator passwords, 7-17
firewall, 3-2
IP, 3-1
virus transmission via e-mail, 7-19
security checklist
AUDIX Voice Mail System, 17-4
security checklists
AUDIX Voice Power System, 17-6
BasicWorks, 17-8
Conference Reservation and Control System, 17-46
CONVERSANT Voice Information System, 17-12
DEFINITY AUDIX Voice Messaging System, 17-4
DEFINITY Communications System G1, 17-14
DEFINITY Communications System G2, 17-20
DEFINITY Communications System G3, 17-14
DEFINITY ECS, 17-14
DIMENSION PBX System, 17-24
INTUITY AUDIX Voice Messaging System, 17-4
MERLIN II Communications System, 17-27
MERLIN LEGEND Communications System, 17-29
MERLIN MAIL R3 Voice Messaging System, 17-36
MERLIN MAIL Voice Messaging System, 17-32
MERLIN MAIL-ML Voice Messaging System, 17-34
MERLIN Plus Communications System, 17-39
Multimedia Communications Exchange Server, 17-40
Multipoint Conferencing Unit, 17-46
System 75, 17-14
System 85, 17-20
Security Measurement reports, 5-52
security risks
port, 4-3
Security Tools for Outgoing Calls, 5-13
Security Tools for Remote Access, 5-4
Security Violation Notification feature, 5-59
referral call, 5-59
Security Violations
measurement report, 5-60, 5-62
report, 13-18
status report, 5-59
Security Violations Detail Report, 5-63
Security Violations Summary Report, 5-62
sending
overlapped, 5-49
service observing, 5-69, 5-70
shoulder surfing, 2-6
six-digit screening, 2-8

SMDR
reports, 6-6, 6-13, 6-60, 6-63, 7-35, 7-37, 7-47, 7-56, 7-58, 7-60
SMDR, see Station Message Detail Recording
social engineering, 2-6
SPM, see System Programming and Maintenance
Station Message Detail Recording, 2-4, 5-47, 7-13, 7-44, 8-9, 15-1
station restrictions, 5-20
Station Security Code Violations Report, 5-66
Station Security Violation Status Report, 5-64
Station-to-Trunk Restrictions, 7-6, 8-3
status remote access command, 5-12
SVN, see Security Violation Notification feature
switch
dial tone, 5-43
translation restrictions, 7-30, 7-35
switchhook flash
administering, 5-21
System 25
password
changing, 14-10
protecting Remote Access, 6-62
protecting the system, 6-62
security goals and tools, 4-14
voice mail, 7-60
System 75
automated attendant, 8-1
detecting toll fraud, 5-50
password
changing, 14-10
Remote Access, 5-3
restricting unauthorized outgoing calls, 5-13
security checklists, 17-14
security goals and tools, 4-10
security measures, 5-28
security tips, 5-2
voice mail, 7-4
System 85
automated attendant, 8-1
detecting toll fraud, 5-50
password
changing, 14-11
Remote Access, 5-3
restricting unauthorized outgoing calls, 5-13
security checklists, 17-20
security goals and tools, 4-10
security measures, 5-28
voice mail, 7-4
system administration
remote, 6-12
System Administrator Tool, 5-55, 7-14
reporting, 5-55, 8-10
system console
physical security, 4-9
system files
performing backups, 4-9
System Programming and Maintenance, 6-14
system tone test call, 5-41

T

TAC, see Trunk Access Code
Tandem Tie Trunk, 5-39
TCM, see Traveling Class Mark
telecommunications fraud
airports, 2-6
by employees, 2-8
definition, 2-1
effect, 2-2, 2-3
employees, 4-8
in lobby, 5-21
telephone number
nonpublished, 5-2
telephony server
control networks, 3-2
firewalls, 3-2
third-party software, 3-2
Tenant Services, 5-33, 7-11, 8-7
Terminal Translation Initialization, 5-46
Terminal-to-Terminal Only Calling Restriction, 8-4
Terminal-to-Terminal Restriction, 5-17, 7-7, 8-4
Termination Restriction, 8-5
test call
facility, 5-40
trunk, 5-40
third party calls, 7-3
third-party applications, 3-2
three-way-conferencing, 7-35
tie trunk, 5-45
disallowing outgoing calls, 5-45
incoming, 5-22
limiting access, 5-45
restricting, 5-22
tandem, 5-45, 5-49
Time of Day
plan, 5-33
routing, 5-24, 5-59
preventing after-hours calling, 5-33
time slot test call, 5-41
Time-Out to Attendant authorization code, 5-36
tip/ring port, 6-62
Title 18 Section 1029, 2-2
TN744 Call Classifier circuit pack, 5-40, 5-41
Toll Analysis, 5-19, 7-7, 8-5
table, 7-9, 7-11
toll fraud
contact list, 16-16
internal, 5-54
voice messaging, 7-2
Toll Restriction, 5-15, 5-17, 7-7, 7-35, 8-4, 8-5
Tone Detector circuit pack, 5-40, 5-41

traffic
abnormal patterns, 8-10
measurements, 5-55
monitoring flow, 5-56
reports, 7-19, 7-30, 8-13
Trans Talk 9000 Digital Wireless System
security tips, 9-9
Transfer Out of AUDIX, 7-25
disabling, 7-28
transfers
limiting, 8-5
Traveling Class Mark, 5-46, 5-49
Trouble Tracker, 4-6
trunk
800 service, 4-2
AAR, 5-8
administration, 5-9
ARS, 5-8, 5-47
CO, 4-2, 5-16, 5-17, 5-20, 8-4, 8-5
disabling direct access, 5-39
FX, 4-2, 5-16, 5-17, 8-4, 8-5
loop-start, 6-62
monitoring, 5-46
outgoing, 5-47
public network, 5-16
Remote Access, 4-2
tie, 5-15, 5-22
WATS, 5-17, 5-19, 5-23, 5-32, 5-43, 8-4, 8-5
WCR, 5-8, 5-47
Trunk Access Code, 2-5, 5-16, 5-35, 5-36, 5-45, 5-46, 5-49, 5-70, 7-2, 7-6, 7-26, 8-3, 8-16
obtaining outgoing trunk, 5-9
Trunk Group Report, 7-14, 8-10, 8-13
trunk groups
800, 5-3
attendant control, 5-40
CO, 4-2
outgoing, 5-11, 5-16
Remote Access, 4-2
two-way, 5-16
trunk override, 5-23
trunk test call, 5-40
Trunk Turnaround
Distributed Communication System, 5-44
Trunk Verification, 7-6, 8-3
Trunk-to-Trunk Transfer
disallowing, 5-43, 7-60
restriction override, 17-17
Trusted server
definition, 7-18
overview, 7-18
TTI, see Terminal Translation Initialization

U

UDP, see Uniform Dial Plan
Unattended Console Service, 5-10, 5-38
Unauthorized Call Control table, 7-10
unauthorized calls
preventing, 7-5
Uniform Dial Plan, 5-15
United States Criminal Code, 2-2
unrestricted call list, 5-19
usage
monitoring, 5-56

V

VDN, see Vector Directory Number
Vector Directory Number, 5-10, 5-11
authorization code, 5-9
COR, 5-11
Verify button, 5-70
Video Conference, see Multipoint Control Unit
Virtual Nodepoint Identifier, 7-10, 7-11, 8-6, 8-7
VMAAP
securing, 4-6
VNI, see Virtual Nodepoint Identifier
voice mail, 2-1, 2-5, 2-6, 2-8, 4-4
cellular phones, 7-3
DEFINITY Communications System, 7-4
DEFINITY ECS, 7-4
detecting toll fraud, 7-12
limiting, 7-8
MERLIN II Communications System, 7-35
MERLIN LEGEND Communications System, 7-38
PARTNER II Communications System, 7-55
PARTNER Plus Communications System, 7-57
protecting, 7-2
security risks, 4-4
System 25, 7-60
System 75, 7-4
System 85, 7-4
Voice Session Record, 7-19
voice mailboxes
deleting unused, 4-9
maximum invalid attempts allowed, 4-9
passwords, 4-8
unassigned, 4-4, 7-3
voice messaging systems
automated attendant, 4-3
transfer command, 4-4

voice processing systems, 4-4
voice session record, 7-19, 8-14
voice terminal
    Public Restriction, 5-16
    Termination Restriction, 5-16
voice terminal group
    attendant-controlled, 5-21
void
    disabling logins, 5-28

W

WCR, see World Class Routing
wild card characters, 5-49, 5-50
wiring closets
    physical security, 4-9
World Class Routing, 5-24, 5-33
    restricting, 5-49
    Toll Restriction, 5-18
    toll restriction, 8-5