AVAYA

Avaya Toll Fraud Security guide

555-025-600
Issue 1
February 2010

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 Web site: 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.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

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

- Within the United States, click the *Escalation Contacts* link. click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Contacts* link. click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and 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 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 its networked equipment. Also realize that, if such an intrusion must 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 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 must 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, or IEC 60950-1, 1st 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, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

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 used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

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

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

> **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.**

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.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover 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 G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of 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.

For all media gateways:

The REN is used to determine the quantity of devices that 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 must 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, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off 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
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	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

For all media gateways:

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

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.

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.

Installation and Repairs

Before installing this equipment, users must ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer must be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment must be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect 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).

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

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。

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 support Web site: http://www.avaya.com/support.

Contents

Chapter 1: Introduction 5

Overview 5

Reason for issue 5

Intended audience 6

How this guide is organized 6

Avaya's statement of direction 7

Avaya and customer security roles and responsibilities 8

Avaya roles and responsibilities 9

Customer roles and responsibilities 9

Toll Fraud action plan 10

Related resources 11

Product documentation 11

Avaya toll fraud hotline 11

Within the US and Canada 11

International 11

Sending us comments 12

Chapter 2: Toll fraud risk model 13

Who is the enemy? 13

Overview 13

Hackers and phreakers 13

Call sell operations 14

Drug dealers 15

What is in a loss? 15

Known toll fraud activity 16

PBX-based activity. 16

Telephone network-based activities 18

General Toll Fraud Security Risks 20

Remote access 20

Unauthorized call transfer. 21

Automated attendant 22

Other port security risks 22

Unauthorized system use 23

Voice messaging systems 23

What users should know 24

Physical security considerations 25

Automated attendant attacks 25

Find-Me, Call-Me, Notify-Me feature attacks 25

Unauthorized mailbox use 26

Tips to help prevent phone fraud . . . 26
Voice Messaging Security tips . . . 27

Chapter 3: Product policy controls. . . . 29
Avaya Aura^{TM} Communication Manager . . . 29
Communication Manager Security Features. . . . 37
Security tips for the Remote access feature . . . 38
Call routing. . . . 38
Command: status remote-access . . . 39
Logoff screen notification. . . . 40
Disable/remove the Remote Access feature . . . 40
Facility restriction levels . . . 40
Class of restriction . . . 43
Class of service . . . 45
Barrier codes. . . . 46
Authorization codes . . . 50
Restricting who can use remote dial access and track its usage . . . 52
Feature access code administration . . . 55
Station-to-trunk restrictions . . . 55
Trunk administration . . . 55
Remote access with Night service . . . 56
Remote access with Call vectoring. . . . 56
Protect vectors that contain call prompting . . . 56
Configuring COR and VDN to prohibit outgoing access . . . 57
Toll analysis . . . 57
AAR/ARS analysis . . . 57
ARS dial tone. . . . 58
Station restrictions . . . 58
Recall signaling (switchhook flash) . . . 58
Attendant-controlled voice terminals . . . 59
Central office restrictions . . . 59
Restrictions — individual and group-controlled. . . . 59
Carrier-based restrictions. . . . 60
Restrict incoming tie trunks . . . 60
Trunk-to-trunk transfer . . . 60
Forced entry of account code. . . . 61
AAR/ARS routing . . . 61
Using AAR/ARS routing restrictions . . . 61
Digit conversion . . . 62

Station Security Codes 62
EC500 Security Features 64
Blocking international calling. 64
Limiting international calling 68
Selecting authorization code time-out to attendant 68
Restricting calls to specified area codes 69
Allowing calling to specified numbers 69
Using attendant control of specific extensions 69
Disabling direct access to trunks. 70
Using attendant control of trunk group access 70
Disable facility test calls 71
Removing the Facility Test Calls Access Code 71
Suppressing remote access dial tone 72
Disallowing trunk-to-trunk transfer. 72
Disable transfer outgoing trunk to outgoing trunk 73
Configuring outgoing trunk to outgoing trunk transfer. 73
Disallowing outgoing calls from tie trunks 73
Limiting access to tie trunks 74
Configuring Forced Entry of Account Code 74
Assign COR restrictions to call center and other adjuncts 75
Disable distinctive audible alert for adjunct equipment 75
Remove data origination code 75
Change override restrictions on 3-way COR check 75
Enhanced call transfer 76

Automated attendant: Considerations for CM and Messaging 77
Security measures. 77
Protect voice mail automated attendant 78

Communication Manager Messaging 79

Call Management System 82
Security tips 82

Modular Messaging 83
Security tips 85

Avaya Aura^{TM} Session Manager 91
Security tips 91

Chapter 4: Toll fraud detection 93

Toll fraud warning signs. 93

Communication Manager 94
Detect toll fraud 94

Administering the SVN feature 102
Administering the authorization code component 106
Administering the station security code component 107
Security violations reports 108
Detecting adjunct-related fraud. 112
Detecting Toll Fraud with Communication Manager Messaging and Modular Messaging115
Voice session records. 115
Detecting automated attendant toll fraud with related CM functions 118
MM Report tool. 123
Call Management System 125
Detecting toll fraud 125
Appendix A: Security support services 127
Avaya support 127
Security Hardening Services 127
Toll fraud contact list 127

Chapter 1: Introduction

Overview

This guide describes the security risks and measures that can help prevent external telecommunications fraud that involves the following Avaya products:

IP Telephony components

- Avaya Aura^{TM} Communication Manager
- Avaya Aura^{TM} Session Manager

Messaging systems

- Avaya Aura™ Communication Manager Messaging
- Modular Messaging

Other Integrated products

- Avaya Aura ™ Application Enablement Services
- Call Management System (CMS)

Note:
This guide describes features of certain products and how they are related to toll fraud security. It does not fully describe the capabilities of each feature. For more information about the security features and their interactions with other system features, see the required product documentation. See Product documentation in this chapter for titles and document numbers.

Reason for issue

This issue, Issue 1, of the Avaya Toll Fraud Security Guide includes:

- Prior material from the obsolete Toll Fraud Security Handbook.
- Latest toll-fraud prevention information.
- New product coverage that includes the latest Avaya Aura^{TM} products.

Intended audience

Telecommunications managers, telephony administrators, and those with security responsibilities for communication networks will find this guide critical to understand and prevent toll fraud within their Avaya Unified Communications environments.

Note that although this guide covers toll fraud feature functionality applicable to Avaya product implementations worldwide, many of the examples given in this guide depend on specific attributes of the North American Numbering Plan. Readers configuring toll fraud prevention functionality outside North America are encouraged to consult with their local sales and services teams or Authorized Avaya Business Partner for specific examples and configuration advice tailored for their locale.

How this guide is organized

The Avaya Toll Fraud Security Guide has the following chapters:

Chapter 1: Introduction	Describes the scope, intended audience, and contents of this guide. Provides Avaya's Statement of Direction. Defines the roles and responsibilities for Avaya and the customers.
Chapter 2: Toll fraud risk model	Provides a risk model surrounding Toll Fraud.
Chapter 3: Product policy controls	Provides a summary of policy controls (toll fraud-related access control features) for each product.
Chapter 4: Toll fraud detection	Summarizes toll fraud detection techniques and related product features.
Appendix A: Security support services	Details special product and service offers and provides a toll fraud contact list.
Appendix B: Product security checklists	Lists the available security features and tips per product.
Appendix C: Links to additional security information	Provides links to additional information sources for security issues.

Avaya's statement of direction

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

A telecommunications system cannot be entirely free from the risk of unauthorized use. However, diligent attention to system management and security can reduce the 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. These customers know how to best customize the system to meet the unique needs and are in the best position to protect the system from unauthorized use. As the customer has ultimate control over the configuration and use of the purchased Avaya services and products, the customer bears responsibility for fraudulent use of these services and products.

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

- Avaya products and services offer a comprehensive range of options to help customers secure their communications systems in ways consistent with their telecommunications needs. Avaya products include industry standard encryption and data-integrity algorithms recognized by FIPS 140-2.
- Avaya is committed to develop and offer services that, for a fee, reduce or eliminate customer liability for toll fraud, provided the customer implements prescribed security requirements in their telecommunications systems.
- Avaya's product and service literature, marketing information and contractual documents address, wherever practical, the security features of our offerings and their limitations, and the customer responsibility for preventing fraudulent use of the Avaya products and services.
- Avaya sales and service people are highly knowledgeable and well informed people in the industry and can help customers manage their systems securely. In their continuing contact with customers, they strive to provide the latest information on how to do it most effectively.
- Avaya trains its sales, installation and maintenance, and technical support people to focus customers on the known toll fraud risks; to describe mechanisms that reduce those risks; to discuss the trade-off 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 provides education programs for internal and external customers to keep them aware of emerging technologies, trends, and options in the area of telecommunications fraud.

- As new fraudulent schemes develop, Avaya is dedicated to initiate efforts to impede these schemes, share the learning with the customers, and work with law enforcement officials to identify and prosecute fraudulent users whenever possible.

Avaya is committed to meet and exceed customers' expectations, and to provide 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 customers' communications services and products.

Avaya and 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, the customers, vendors, and their agents each have specific roles and responsibilities. Each organization must ensure that systems are designed, ordered, installed, and maintained in a secure manner.

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

Customers also have specific responsibilities to ensure the system they install is as secure as the requirements dictate. The following quote is from *A Cooperative Solution to the Fraud that Targets Telecom Systems*, a position paper that is 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 guide 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 roles and responsibilities

- Avaya, as a manufacturer, has the responsibility to **provide** the customer with securable technology, information resources (product documentation) to understand the capabilities of the technology, and configuration of the equipment when it is 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 agree on the required 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 Avaya serves to introduce risk to the customer's system. At the very least Avaya must ensure that the customer is as secure after Avaya's assistance as they were before it.

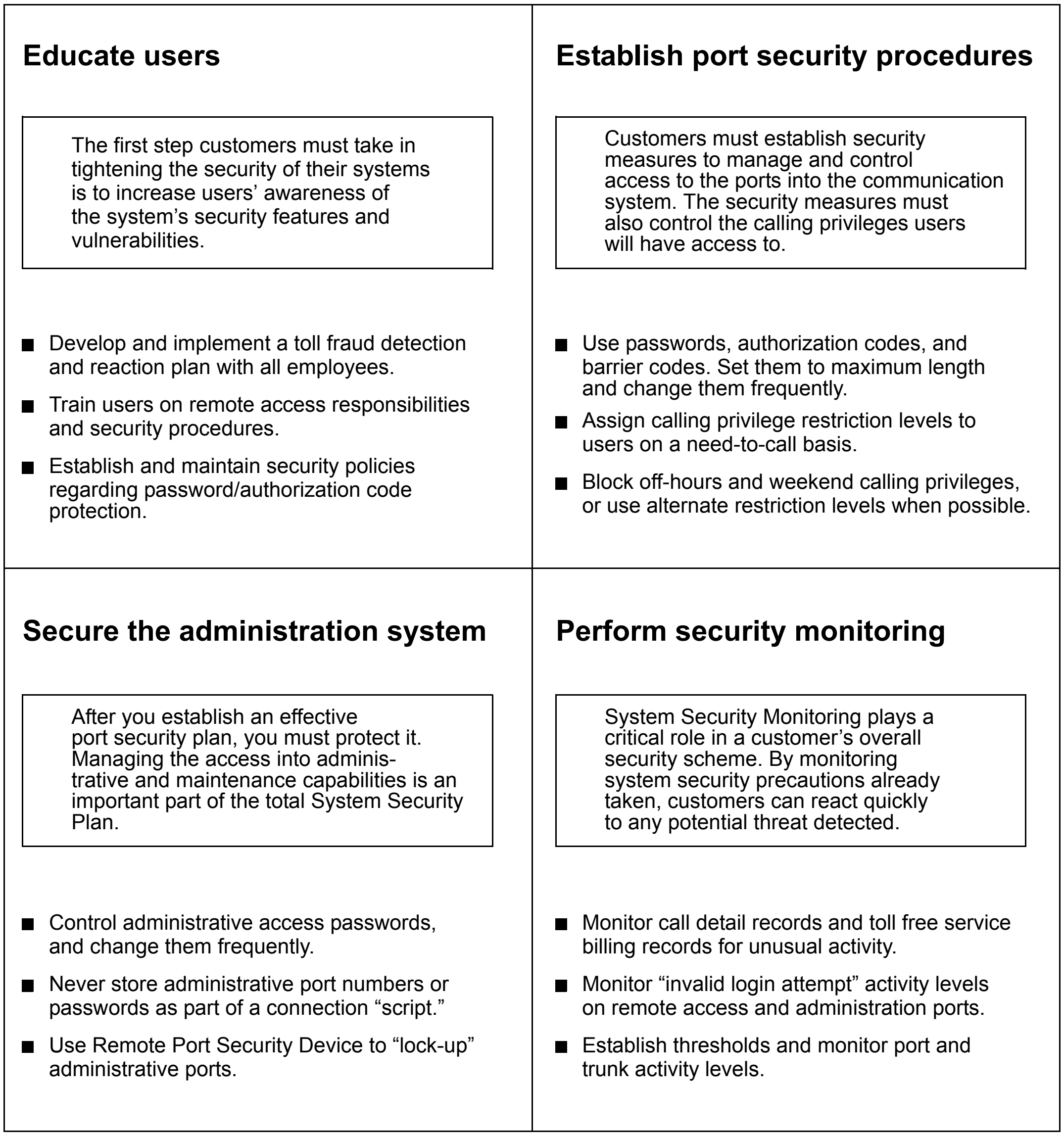
Customer roles and responsibilities

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, and so on.) 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 the business."

Toll Fraud action plan

Figure 1: Toll Fraud action plan



Educate users

The first step customers must take in tightening the security of their systems is to increase users' awareness of the system's security features and vulnerabilities.

- Develop and implement a toll fraud detection and reaction plan with all employees.
- Train users on remote access responsibilities and security procedures.
- Establish and maintain security policies regarding password/authorization code protection.

Establish port security procedures

Customers must establish security measures to manage and control access to the ports into the communication system. The security measures must also control the calling privileges users will have access to.

- Use passwords, authorization codes, and barrier codes. Set them to maximum length and change them frequently.
- Assign calling privilege restriction levels to users on a need-to-call basis.
- Block off-hours and weekend calling privileges, or use alternate restriction levels when possible.

Secure the administration system

After you establish an effective port security plan, you must protect it. Managing the access into administrative and maintenance capabilities is an important part of the total System Security Plan.

- Control administrative access passwords, and change them frequently.
- Never store administrative port numbers or passwords as part of a connection "script."
- Use Remote Port Security Device to "lock-up" administrative ports.

Perform security monitoring

System Security Monitoring plays a critical role in a customer's overall security scheme. By monitoring system security precautions already taken, customers can react quickly to any potential threat detected.

- Monitor call detail records and toll free service billing records for unusual activity.
- Monitor "invalid login attempt" activity levels on remote access and administration ports.
- Establish thresholds and monitor port and trunk activity levels.

Related resources

This section describes additional documentation and security resources.

Product documentation

The security risks and preventive measures in this guide relate specifically to toll fraud. The guide is designed to work with the documentation provided for the products. It is not intended as a replacement for the product documentation.

To access product documentation, please visit the Avaya Support Web site at http://www.avaya.com/support.

Avaya toll fraud hotline

For additional support contact numbers, see http://www.avaya.com/support. If you suspect that you are victimized by toll fraud, and need technical assistance or support, contact the Technical Service Center Toll Fraud Intervention Hotline.

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 a service agreement.

Within the US and Canada

Toll Fraud Intervention Hotline Call this number if you suspect you are being victimized by toll fraud or theft of service, call the appropriate Avaya service.	**1 800 643-2353**

International

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

Sending us comments

Avaya appreciates any comments or suggestions that you might have about this product documentation. Send your comments to the Avaya documentation team.

Avaya Toll Fraud Security Guide, 555-025-600.

Chapter 2: Toll fraud risk model

Who is the enemy?

Overview

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. With the added capabilities of voice mail and automated attendant services, customer premises equipment-based toll fraud expanded as new types of communication abuses became possible in the 1980s and 1990s. Since 2000, the rapid growth in Voice over IP (VoIP) and other Unified Communications (UC) technology has only increased the range of capabilities and potential targets that has to be protected

Today, security problems are not just limited to toll fraud. There have been sharp increases in reported incidents of attackers: 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 attackers can gain control over the setup of the system. Through these ports, attackers create security "holes" to allow unauthorized calling — a serious form of electronic vandalism and other unwanted activity.

A company's "information resources" are yet another target for modern criminals. They may attempt to infiltrate invading voice mailboxes or eavesdrop on cellular phone calls to obtain proprietary information about your products or your customers.

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 an attacker 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 advertise that they have broken your system and how they did it. They will also sell this information to a call sell operator. Some attackers 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 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 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 codesells for up to $3,000.00.

Drug dealers

Drug dealers want phone lines that are difficult to trace so they can conduct their illicit activities. For this reason, drug dealers are more likely to route their calls through two or more communications systems (**PBX**s) or voice mail systems before a call is completed. This is called “looping.” Law enforcement officers believe that drug dealers and other criminals attempting to obscure illegal activity taking place over long distance networks commit 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 attackers penetrate your system is the first step in learning what to do to protect your company. Be aware that attackers communicate very well, are extremely resourceful, and are persistent. The following is a list of known methods attackers use to break into systems.

PBX-based activity

- **Maintenance port**

  Maintenance ports are the most recent target of abuse. In this scenario, attackers 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 “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 attackers 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.

    Attackers 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) and hack your system all weekend, and turn it back on before Monday morning. This is especially disturbing to managers who are security conscious and check the CDR reports every morning looking for suspicious activity. They will not see records of the calls because CDR was turned off by the attackers. The administrator may notice the absence of CDR 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 an attacker accesses a mailbox to either take it over or simply access the information stored within it.

  In the first situation, an attacker dials either 9 or a TAC that allows the call to be transferred to the outgoing facilities. In the second situation, an attacker typically hacks the mail password and changes it along with the greeting. This gives the attacker 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 attacker 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 attacker enters the remaining digits of the phone number and the call is completed. You, the **PBX** owner, pay for it. This attacker 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.

  Attackers 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 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 an attacker is disconnected, he or she may call back repeatedly in an attempt to crack the code.

Telephone network-based activities

– **Shoulder surfing**

Network attackers use video cameras in airports supposedly to take pictures of their family, but they are actually taking pictures of people using their calling cards. Attackers 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 attackers 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 attacker takes full advantage.

For example, attackers 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 attacker asks for an outside line. Often, because operators do not know any better, they will connect the attacker to an outside line.

Another example of social engineering is an attacker 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 attacker more ammunition with which to crack your system.

– **Dumpster diving**

Attackers 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, attackers 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 **IXC**s (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 a toll-free access number outbound from the **PBX**. The toll-free 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 toll-free 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 attackers 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 attackers find a number they suspect is using a call diverter, they call the number. When the call is answered, the attacker claims to have misdialed or remains silent. When the caller hangs up, the call diverter sometimes gives the attacker a dial tone before the disconnect is completed. The attacker seizes the dial tone and uses it to place fraudulent long distance calls.

- **Beeper and pager scam**

  A scam directed at pagers and beepers is as follows. Many of the Local Exchange Carriers (**LEC**s) 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 can also easily apply to messages left on voice mail. The person can 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.They call one of these 976-look-alike numbers and stay on the line for a minute or two. Your company gets the bill for a $250 call that lasted only a couple of minutes.

- **Internal abuse**

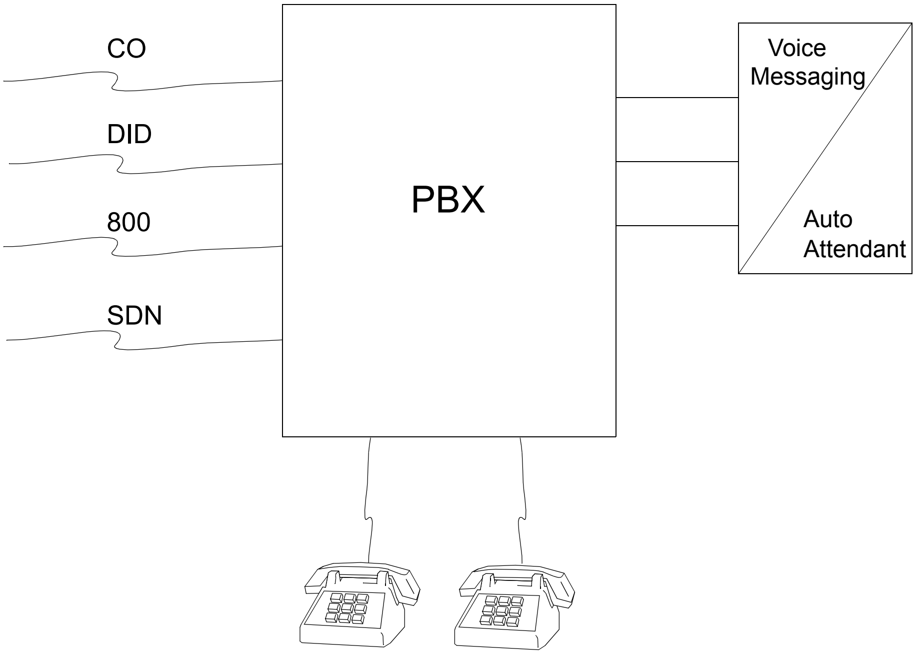
  Unfortunately, not all toll fraud is generated from "outsiders." Many times it can be traced to internal employees who either sell the information or abuse the system for their own gain.

- **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 toll-free 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.

General Toll Fraud Security Risks

Figure 2: Call transfer through the PBX



Remote access

Remote access, or direct inward system access (DISA), allows callers to call into the system 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.

Note:

In this guide, **Remote access** refers to DISA-type dial access only. It does not refer to the methods that commonly use this term: remote system administration, servicing activities, or Internet Protocol (IP) 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 toll-free 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.

When a remote access call is answered, the caller can be requested to enter a barrier code and an authorization code before calls are processed. When both maximum length barrier codes and authorization codes are required, attackers need to decipher up to 14 digits (a 7-digit barrier code and 4 to 13 digit authorization code) to gain access to the feature.

Attackers 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, attackers use random number generators and password cracking programs to find a combination of numbers that gives them access to an outside facility.

For these reasons, all switches in the network must be protected.

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

Unauthorized call transfer

Most equipment-related toll fraud loss occurs when attackers misuse the call transfer capabilities of voice mail systems. Attackers can dial a Trunk Access Code (TAC), Feature Access Code, Facility Access Code (FAC), or an extension number. Attackers attempt to make fraudulent long-distance calls directly or request a company employee to transfer them to a long-distance number.

Automated attendant

An automated attendant is the industry term for an electronic receptionist and is a service that connects to a PBX system that helps route calls to the appropriate extensions. Callers can select a defined destination from a menu of options. The destination can be a department, announcement, or an attendant. A destination can also be a user-defined destination, such as an extension number. Because the automated attendants provide the necessary signaling to the PBX when a call is being transferred, failure to configure appropriate restrictions on the routing destinations it can request can result in toll fraud. When attackers connect to an automated attendant system, they try to find a menu option that leads to an outside facility. Attackers may also attempt to enter a portion of the toll number to verify whether the automated attendant system passes the digits directly to the PBX, enter the remaining digits after the transfer has been made to an outside line.

Attackers 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 attacker 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 attacker 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 attacker 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 Automated attendant: Considerations for CM and Messaging 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 must 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. Other examples of adjunct access that need to be managed include call center, mobility, conferencing, and any other equipment that uses station or trunk access to interact with Communication Manager, Session Manager, or the PSTN.

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 a Voice Mail System if not protected by appropriate restrictions. Any features or endpoints that can be dialed, but are to be denied to incoming callers, must be placed in restriction groups that cannot be reached from the incoming facility or from endpoints that can 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 58.)

Unauthorized system use

Although maintenance ports cannot be used to place telephone calls, discovery of these ports and administrative credentials required to use them can allow an attacker to gain control over the system setup. Through maintenance ports, hackers try to create security holes that permit unauthorized calling. Typically attackers use devices that randomly dial numbers until a modem or dial tone is obtained, they attempt to discover a user ID and password that will allow them to enter your system. Select a good password with a combination of alphanumeric and special characters. A good password decreases the chances of password hacking.

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 attackers connect to the voice messaging system, they try to enter digits that connect them to an outside facility. For example, attackers enter a transfer command followed by an outgoing trunk access number for an outside trunk. Most attackers do not realize how they gained access to an outside facility; they only need to know the right combination of digits.

Sometimes attackers 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. Attackers can even use cellular phones to break into voice mailboxes. In addition, unauthorized access to voice messaging systems can allow attackers to access the switch and change administration data.

Toll fraud is possible when an incoming caller is allowed to make an outbound connection back to the PSTN. Once a mechanism for reaching an outside line is obtained, attackers can make calls to anywhere in the world. The following threats are typical of those associated with toll fraud via messaging systems:

- Unauthorized system use. Intruders breach your system to create a mailbox and use system resources. Avenues for access include:

- Use of personal computers, random number generators, and password cracking programs to break into customer premises equipment-based systems.
- Disclosure or discovery of remote modem access mechanism directly connected to the Modular Messaging server(s).
- Disclosure or discovery of IP network dial-up or VPN remote access mechanism or
- IP-based attacks that originate from inside your network (less common)

- Unauthorized call transfer. An intruder uses the transfer-to-extension feature by transferring to the first few digits of a trunk access code or other mechanism that provides the caller access to an outside line.
- Unauthorized mailbox use. May involve toll fraud or may be simple theft of messaging services. An intruder discovers how to use a particular mailbox, perhaps by:
    - Finding the password on a subscriber desk or in a wallet
    - Trying all the common variations of passwords
    - Buying the password from a computer attacker who breached the system security and logged in as an administrator

What users should know

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 attacker 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 must 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 must frequently change personal passwords and must not choose obvious passwords.
- 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.

Physical security considerations

You must always limit access to the system console. The following are some recommendations:

- Keep the attendant console 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.

Automated attendant attacks

Many automated attendant systems are vulnerable to toll fraud and are easy targets for toll attackers. 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**.

- 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.
- 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.
- Voice Mail Systems must use the Enhanced Call Transfer feature.

Find-Me, Call-Me, Notify-Me feature attacks

The Find-Me feature redirects unanswered calls to a list of telephone numbers specified by the subscriber. Find Me is a real-time feature that attempts to connect the caller to the subscriber in order to avoid creating a message.

The Call-Me feature calls subscribers at a designated telephone number or a telephone list when subscribers receive a message that meets certain specified criteria. Subscribers who can use the feature create condition rules that can trigger Call Me and call the telephone numbers. The Notify-Me feature operates similarly but is targeted at devices and does not initiate a phone call except when a pager is dialed.

An attacker with unrestricted access to either feature can create costly notification or outbound find-me calls or combine it with other attacks. Transfers performed as part of these operations are not usually prone to toll fraud because the transfer is supervised, but certain configurations and conditions can lead to unsupervised transfer conditions that can be exploited by an attacker.

Unauthorized mailbox use

When attackers gain control of a mailbox, they are either seeking to control the mailbox directly or use the information stored within the mailbox. Typically, the attacker hacks the voice mail password to change the password and greeting.

Tips to help prevent phone fraud

- **Protect system administration access**

  Set unique passwords for each system administration or maintenance account and consider the use of expiration policies to force regular password changes. Monitor access to maintenance ports (IP or dial-up).

- **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 authorization codes set for maximum length. Change the codes frequently.

- **Place protection on systems that prompt callers to input digits**

  Callers must be prevented from dialing unintended digit combinations at prompts.

  Auto attendants and call vectors must be restricted from allowing access to dial tone.

- **Use system software to intelligently control call routing**

  Create **ARS** or AAR patterns to control how each call is to be handled. If you have configured Uniform Dial Plan (UDP) for off-network calls, ensure you enable appropriate calling restriction features.

  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.

- **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.
- **Ensure operational processes for provisioning, de-provisioning, and user password management are secure**

  Always provision a password for user accounts and force a password change on first use. Consider adding password complexity, expiration, and lockout rules for user accounts. Establish well-controlled procedures for resetting user passwords. Delete unused voice mailboxes and ensure that mailboxes belonging to terminated employees are locked and deleted appropriately.

Voice Messaging Security tips

- Restrict transfers back to the host PBX by not allowing transfers, by using enhanced call transfer (AUDIX® / CM Messaging only), 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 attackers.)
- 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).
- Change adjunct default passwords immediately; never skip the password entry. Attackers 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.

Chapter 3: Product policy controls

Avaya Aura^{TM} Communication Manager

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

Table 1: Security goals

Security Goal	Method	Security Feature	Steps	Page #
Protect Remote Access feature	Limit access to authorized users	Barrier codes	Set to maximum length Set COR/COS Administer Barrier Code Aging Restrict who can use remote dial access Set up remote access example Suppress remote access dial tone	46 64 46 53 72
		Authorization codes	Configure remote access authorization codes Set to maximum length Set **FRL on COR** Suppress remote access dial tone	51 50 51
	Disable/ Remove Remote Access feature if not needed	Disable/ Remove Remote Access	Permanently Disable Remote Access	40
1 of 8				

Table 1: Security goals

Security Goal	Method	Security Feature	Steps	Page #
	Use **VDN**s to route calls	Call vectoring	Administer call vectoring Use **COR**s to restrict calling privileges of **VDN**s Protect Vectors that contain call prompting	57 56
	Limit times when Remote Access is available	Night service	Administer night service	56
2 of 8				

Table 1: Security goals

Security Goal	Method	Security Feature	Steps	Page #
Prevent unauthorized outgoing calls	Limit calling area	AAR/ARS Analysis	Set **FRL** Set **COR** Restricting calls to specified area codes Allow calling to specified numbers	57 69 69
		Digit conversion	Administer digit conversion	62
		Toll analysis	Identify toll areas to be restricted	57
		Facility Restriction Levels (FRLs)	Limit access to AAR/ARS route patterns by setting to lowest possible value	40
	Restrict phones from making outbound calls	Attendant-controlled voice terminals	Place phones in attendant-controlled group Using attendant control of trunk group access	59 69 70
		Authorization code time-out	Select authorization code time-out to attendant	68
		Recall signaling	Administer switchhook flash to **n**	58
3 of 8				

Table 1: Security goals

Security Goal	Method	Security Feature	Steps	Page #
Prevent unauthorized outgoing calls (continued)	Screening calls	Central office restrictions		59
		Carrier-based restrictions		60
	Restricitng Terminals	Restrictions - individual and group-controlled	Activate and deactivate individual or group based terminals Use terminal translation initialization	59
	Limit outgoing calls	Facility Restriction Levels (FRLs)	Restrict tie trunk usage Deny access to AAR/ARS	74
		Authorization codes	Set to maximum length Set **FRL on COR**	50
		Access to trunk	Disable direct access to trunk Monitor trunk	70 74
		AAR/ARS restrictions	Restrict AAR/ ARS from unauthorized use	61
4 of 8				

Table 1: Security goals

Security Goal	Method	Security Feature	Steps	Page #
Prevent unauthorized outgoing calls (continued)	Limit calling permissions	Class of Service (COS)	Set COS restrictions	45
		Class of Restriction (COR)	Set **FRL** Set calling party restrictions or outward restrictions Set COR to COR restrictions	44
	Require account code before calls	Forced entry of account code	Set account code length Configure forced entry of account code	61 74
	Create time-dependent limits on access to route patterns	Alternate **FRL**	Set lowest value possible	42
	Suppress dial tone after AAR/ARS feature access code	Suppress dial tone	Turn off AAR/ARS dial tone	58
	Screen all AAR/ARS calls	AAR/ARS	Administer all capabilities	57
	Block international calls	**ARS** Digit Analysis	Deny permission to international numbers	64
			Blocking international calls Call Blocking example	64 65
5 of 8				

Table 1: Security goals

Security Goal	Method	Security Feature	Steps	Page #
Prevent unauthorized outgoing calls (continued)	Limit international calls	**ARS** Digit Analysis	Deny permission to international numbers Limiting international calling	68 68
	Disallow/ disable Trunk-to-trunk transfer	Outgoing trunk to outgoing trunk transfer (**OTTOTT**) feature	Disable OTTOTT	72 73
		Trunk-to-trunk transfer	Disallow trunk-to-trunk transfer	72
		Limiting access to tie trunks	Assign COR-to-**COR** restrictions	74
	Set Station security codes (SSC)	Station security codes	SSC input	62
	Carefully assign feature access codes	Feature access codes	Feature access code administration	55
	Enable EC500 security functionality	Calling Number Verification	Restrict incoming EC500 calls to calling numbers that are "Network Provided" or "User Provided Verified and Passed"	64
		Protect remote EC500 features with Station Security Codes	Assign Station Security Codes	62
6 of 8				

Table 1: Security goals

Security Goal	Method	Security Feature	Steps	Page #
		Idle Appearance Select Feature Named Extension (FNE)	Don't enable Idle Appearance Select FNE	64
	Restrict Trunk Access Codes	Trunk Access Codes	Limit direct dial and facility test access to Trunk Access Codes	55
Prevent exit from voice messaging system	Disable distinctive audible alert for adjunct equipment	Distinctive audible alert (stutter tone)	Administer analog station settings to disable distinctive audible alert	75
	Remove or change data origination code	Data Origination	Remove or change data origination code	75
	Prevent messaging system transfer to dial tone (supported messaging systems only)	Station restrictions	Turn off transfer feature	58
		Enhanced Transfer	Set Transfer Type= “Enhanced”	40
		Basic transfer	Set Transfer Restriction= “Subscribers”[1]	76
7 of 8				

Table 1: Security goals

Security Goal	Method	Security Feature	Steps	Page #
Prevent unauthorized calling from automated attendant service				
	Limit exit to outgoing trunks	Enhanced call transfer		40
		Facility Restriction Levels (FRLs)	Set lowest possible value	40
		Station-to-trunk restrictions		55
		Class of restriction		43
		Class of service		45
	Restrict outgoing toll calls	Toll Analysis	Identify toll areas to be restricted	57
8 of 8				

1.

Communication Manager Security Features

Note:
This document provides high-level guidance on how to leverage toll fraud security features in CM. For complete details and full descriptions of these features, refer to *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Security tips for the Remote access feature

- Evaluate the necessity for remote access. If this feature is not vital to your organization, consider deactivating this 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 attackers scan telephone directories for local numbers and toll-free 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 so that no dial-tone prompt is supplied for entry of the authorization code. No dial tone after a remote access call is connected discourages most attackers 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 a toll-free number. For example, if all your authorized users are on the east coast, do not provide trunks that allow calling in from San Francisco.
- Specify maximum length barrier codes and authorization codes. Codes may be specified up to 14 digits (a 7-digit barrier code and a 4 to 13 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 an attacker 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.

Call routing

Call routing call flow

The following is the basic call flow through Communication Manager:

- 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 transferred 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 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 that is 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 9. 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

Command: status remote-access

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

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.

Disable/remove the Remote Access feature

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, it requires Avaya maintenance personnel intervention to reactivate the feature.

For Communication Manager, the Remote Access feature can be permanently removed. Permanent removal protects against unauthorized remote access usage even if criminals break into the maintenance port.

1. Enter **change remote-access** to display the Remote Access screen.
2. Ensure the `Remote Access Extension` field is blank.
3. Enter **y** in the `Permanently Disable` field.
4. Log off. (You must log off to enable the change.)
5. Log back in and enter **display remote-access** to verify the changes. If you get an error message or you cannot display the screen, you know it worked.

The Remote Access feature is disabled after you log off from the switch.

Facility restriction levels

FRLs provide eight different levels of restrictions for AAR/ARS calls. **FRL**s are used in combination with calling permissions and routing patterns and preferences to determine where calls can be made. **FRL**s 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 feature to determine call access to an outgoing trunk group. Outgoing call routing is determined by a comparison of the **FRL**s in the AAR/ARS routing pattern to the **FRL** associated with the COR 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. Ensure that the **FRL**s 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 calls. Therefore, the **FRL** level does not matter since **FRL**s are not checked. However, if you enable access to public network destinations through Universal Dial Plan (UDP) configuration, you must ensure FRLs and other restrictions are specified for the destinations that you want to restrict.

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.

Note:
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 Facility Restriction Levels (FRLs)

FRLs are used to allow or deny calls when AAR/ARS 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 assigned an FRL of 7 is allowed to complete a call on any route pattern. A COR assigned an FRL of 2 can only access route patterns assigned an FRL of 0, 1, 2, or 3. A low FRL must be assigned to analog stations used for voice mail, remote access barrier codes, VDNs, and tie-lines from other systems. Refer to Table 2 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.

FRLs 1 through 7 include the capabilities of the lower **FRL**s.

Assigning Facility Restriction Levels:

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

Preventing 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.

Use the following procedure to regulate the after-hours calling:

1. Use **change ars analysis partition x** to define an **ARS** analysis table to be used for after-hours calling.
2. Use **change time-of-day y** to select and define a time of day plan.
3. 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.

Facility restriction level for unauthorized outgoing calls

Facility restriction levels (FRLs) provide up to eight levels of restrictions (0 through 7) for users of AAR/ARS. **FRL**s 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 **FRL**s are the most restrictive for stations; **FRL** 0 can be implemented to provide no outside access.

Note:
ARS/ARS route patterns must never be assigned an FRL of 0 (zero).

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

Authorization codes provide users with an **FRL** value high enough to give them the required calling privileges. 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 access codes are dialed.

Alternate facility restriction levels

This feature is used with or without authorization codes to replace originating **FRL** values with an alternate set of values when enabled. Only the class of Restriction (COR) FRL is affected alternate do not modify AAR/ARS pattern preference FRLs). This allows **FRL**s to be set to a lower value outside normal business hours so more restrictions are placed on after-hours calling.

Note:
The associated button would typically is assigned to the attendant console to activate alternate FRLs.

Class of restriction

The class of restriction (**COR**) places calling permissions and restrictions on both the calling party and the called extension. Up to 996 **COR**s can be defined in the system.

For complete details and full descriptions of COR features and configuration, refer to *Feature Description and Implementation for Avaya Aura*^{TM} *Communication Manager,* 555-245-205.

Each COR may be assigned a unique name through the Class of Restriction screen. **COR**s 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 **COR**s.

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 **FRL**s for use by 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 can dial 9 or a TAC and be routed out of the system to the network.

To help maximize system security, follow these steps:

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

Calling party and called party restrictions

The default value of the `Calling Party Restriction` field on the COR screen 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 through AAR/ARS or **TAC**s. Calls can be placed to internal stations, to tie trunks via **TAC**s, 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. You can specify if the restriction applies to all toll calls or only **TAC** toll calls over CO/FX trunks.

  Note:
  Toll calls and private network calls are defined on the Toll Analysis screen. Failure to properly define toll calls on the toll analysis screen can create exposures to toll fraud.

- Fully Restricted: denies outgoing calls, including dial access to trunks. Allows no incoming calls via public network trunks.

COR-to-COR restrictions/calling permission

If it is not practical to block dial access on an outgoing or two-way trunk, then COR-to-COR restrictions must be used to prevent direct access to the trunk groups.

Additional COR options are related to toll fraud prevention

- APLT: allows callers to dial public network numbers over the EPSCS private network.
- FRL: establishes the user’s access to AAR/ARS routes
- CDR Account Code: requires the entry of an account code before an AAR/ARS call is processed or before completing a TAC call to a toll destination.

  Note:
  Account code entries are not validated.

Restriction override (3-way COR check)

The Restriction Override feature determines whether or not there is a 3-way **COR** check made on conference and transfer calls.

The default value of the `Restriction Override` field on the COR screen 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 **COR**s of all other parties on the conference and 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 **COR**s 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

Class of Service (COS) is used to control the availability of certain features for a given extension. COR and COS do not overlap in the access or restrictions they control. The following COS-configurable features should be assigned only to users with legitimate need for the associated feature-functionality:

The following **COS** options are related to toll fraud prevention:

- 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). A default is in place that limits 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.

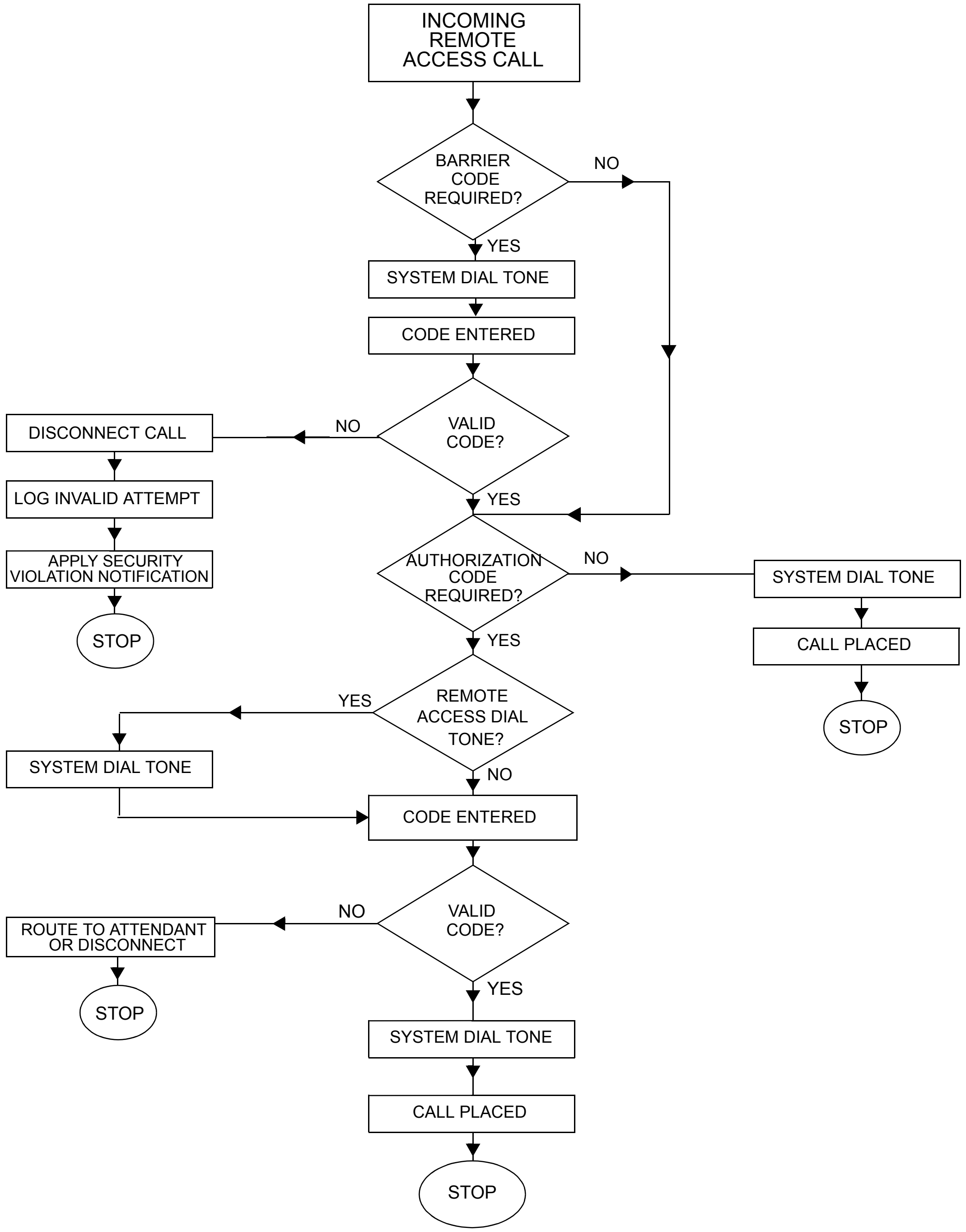
  Note:
  The **list call-forwarding** command displays all stations with Call Forwarding On/Off Net Call Forwarding and Busy/Don't Answer (BY/DA). This display includes the initiating station and destination address.

- Extended User Administration of Redirected Calls feature: The COS screen contains two fields: `Extended Forwarding All` and `Extended Forwarding B/DA`. The default for both fields is **n**.
- Class of Service (COS) is used to control the availability of certain features for a given extension. COR and COS do not overlap in the access or restrictions they control.
- Enhanced Call Forwarding (CM 4.0 and later) enables incoming calls to be forwarded to different destinations depending on whether the incoming calls are from internal or external sources, and is shown on the COS form as "Call Forwarding Enhanced" - The default for this field is **n**.

Barrier codes

Figure 3 illustrates how barrier codes and authorization codes can provide added security for remote access calls. Refer to this flowchart for more information on barrier codes and authorization codes.

Figure 3: Remote access call path



For Communication Manager, 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 must enter a valid barrier code before they can access the system.

Note:
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 must be set to `console permission =` **n**.

The Remote Access Barrier Code Aging feature provides a means of limiting the validity time of the remote access barrier codes, and 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 on page 109, and Administering barrier code aging on page 318.

Remote Access Notification provides automatic reporting when remote access is in use. For more information, see Adding customer logins and assigning initial password on page 321.

Administering 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.
   - `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 13-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 13-digit number in this field for maximum security.

- `Class of Restriction (COR)`

  Enter the **COR** (**0** through **995**) 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 define only the level of service required, provides 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 define only the level of service required, provides 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. The default is the following day’s date. Valid entries are a date greater than the current date or a blank. 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 required.

- `No. of Calls`

  This field specifies the number of remote access calls that can be placed using the associated barrier code. The default is **1**. Valid entries are **1** to **9999**, or **blank**. 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 incriminated 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.

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 **FRL**s to allow access to restricted AAR/ARS facilities. They can be recorded on CDR/CAS to check against abuse. The **`list`** command can be used to display all administered authorization codes.

Note:
For all systems, once established, the number of digits (4 to 13) 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. If the number of digits is increased, trailing zeros are added - we recommend customers establish new random codes for the full new length. Decreasing length is not recommended and will force all codes to be replaced.

For Communication Manager, 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 must be assigned unique authorization codes from 4 to 13 digits (use all 13 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 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), tCDRhen the authorization code COR must have an appropriately low **FRL**.

Note:

Authorization codes are also recorded by the PBX's call detail recording feature (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.

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 calls for outgoing calls [see Facility restriction levels on page 40]. Up to 90,000 authorization codes can be issued to the Communication Manager users. However, it is best to keep the number of authorized users to a minimum.

Configuring Authorization codes to maximize the system security

1. When assigning authorization codes, give the users the lowest possible **FRL** needed for their calling requirements.
2. Be sure to remove any unused authorization codes from the system, including those assigned to employees who have changed assignments or left the company.
3. Assign each authorization code the minimum level of calling permissions required.
4. Make authorization codes nonconsecutive (random).
5. Administer each authorization code to the maximum length allowed by the system (13 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.

Remote access dial tone

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.

Restricting who can use remote dial 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.

1. Use **change system-parameters CDR** to display the CDR System Parameters screen.
   - If the software has been purchased, enter **y** in the `Authorization Code Enabled` field.
   - Enter **13 (or preferred length below 13)** 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.
2. Use **change remote-access** to display the Remote Access Status screen.
   - Enter the appropriate extension number in the `Remote Access Extension` field.
   - Enter **7 (or preferred length below 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.
3. Enter up to 10 barrier codes (use all seven digits) and assign each a **COR** and **COS** that allow only necessary calls. The **COR** must be restricted so that even if an attacker deciphers the barrier code, a valid authorization code is still needed to make a call.

   Note:
   Use the Remote Access feature 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 on page 109.
4. When assigning authorization codes used only to upgrade **FRL**s, 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.
5. Consider using a special partition group for the remote access **COR**, and administer the AAR/ARS tables only for those external locations that 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.

6. Monitor authorization code usage with **CDR**. See Monitor trunks on page 95 for further details.

Setting up remote access example

Use this 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 **13** (or preferred length below 13) in the `Barrier Code Length` field.
3. Enter **n** in the `Authorization Code Required` field.
4. Enter **7** (or preferred length below 7) digits and enter it into the first `Barrier Code` field.
5. Select a unique **COR** (**0** through **995**) 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, 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. A group number may be required when setting COS - for more details refer *Administering Avaya Aura^{TM} Communication Manager*, 03-300509.

   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, 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.

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 Disabling direct access to trunks on page 70.

    Note:
    Repeat Steps 14 and 15 for all the trunk groups in the system so that all outgoing calls route via ARS/AAR.

16. 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. 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.

18. 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.

19. Assign authorization codes for your remote access users that provide the lowest possible **FRL** to match each user’s calling requirements.

Table 2: Suggested values for FRLs

FRL	Suggested Value
0	No outgoing (off-switch) calls permitted.
1	Allow local calls only; deny 0+ and toll-free calls.
2	Allow local calls, 0+, and toll-free 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.

Feature access code administration

Certain feature access codes may facilitate egress from the system and must be used with care. These include: Data Origination, Data Privacy, Data Restriction, Abbreviated Dialing, ARS/AAR, Call Forwarding, and Facility Test Calls. In addition, be careful of how FACs are administered for redirected calls: Extend Call Forward All Activate, Extended Call Forward Busy/Don't Answer Activate, Extended Call Forward Cancel, and Change Coverage.

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 of voice mail to an outside facility using trunk access codes.

Note:

Allowing **TAC** access to tie trunks on the 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.

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 **TAC**s to obtain an outgoing trunk.

Remote access with 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.

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.

Remote access with Call vectoring

Administering access to the Remote Access feature through the use of Vector Directory Numbers (**VDN**s) 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.

Protect vectors that contain call prompting

Attackers 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 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 **VDN**s, “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***.

Configuring COR and VDN to prohibit outgoing access

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 60.

1. Assign a Calling Party Restriction of “Outward” and deny Facility Test Call capability.
2. 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.)
3. Block access to specific **COR**s assigned to outgoing trunk groups by using the Calling Permissions section of the Class of Restriction screen.

Use of Call Vectoring with Prompting for remote access allows the system 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 attackers to detect a remote access port.

Note:
Avaya strongly recommends, for both security and performance reasons, that the Ethernet connectivity between the CM and any SPI-enabled hosts with which it will communicate be a separate LAN segment. Otherwise, an unscrupulous person can gain unauthorized access to the CM vectoring functions in order to commit toll fraud and tamper with the real-time aspects of CTI applications.

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

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 **AAR** calls.

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 route to **ARS**. If Uniform Dial Plan (UDP) is used to route public network calls, apply appropriate restrictions to public UDP routes as well.

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-to-COR restrictions do not apply to AAR/ARS calls, use **FRL**s to limit the calling area [see Facility restriction levels on page 40 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 attackers 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 **TAC**s is necessary for certain users to allow direct dial access to specific facilities, use the appropriate restrictions. If all trunk groups have their own unique COR, restrict the station CORs from accessing the trunk group CORs. For those stations and all trunk-originated calls, always use AAR/ARS 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, attackers 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.

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.

Restrictions — individual and group-controlled

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 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.

Carrier-based restrictions

Some carriers offer additional services that screen long distance calls, such as 0 + calls and 101xxxx+ calls. Contact your carrier for details.

Restrict incoming tie trunks

You can deny access to PSTN calls when the caller is on an incoming tie trunk. For all the switches, you can force the caller to enter an authorization code. In addition, the COR of the incoming tie trunk can 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.

Trunk-to-trunk transfer

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

Note:

Attackers 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.

Communication Manager 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.

Three options are available:

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

Note:

Starting with Communication Manager ECS Release 5, trunk-to-trunk transfer is automatically restricted via administration. The `Restriction Override` field in the Class of Restriction screen is set to **none** by default.

For information on how to disallow this feature, refer to the procedure provided in Disallowing trunk-to-trunk transfer on page 72.

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.

An entry of an account number (1 to 15 digits) can be required for the originating station COR, toll calls, or AAR/ARS 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 an attacker must crack to gain access to an outside line.

AAR/ARS routing

Specific digit strings are assigned to either allow or deny calls. The 900 look-alike numbers can be routed for interception. The toll-free numbers for ICX carriers can be blocked. This still allows normal toll-free 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 AAR/ARS to shut down toll routes during out-of-business hours by using Time-of-Day routing.

Using AAR/ARS routing restrictions

Use the following steps to restrict AAR/ARS from unauthorized use:

1. Miscellaneous restrictions (COR-to-**COR** restrictions) are not observed during AAR/ARS call processing. The **FRL** value is used instead.
2. Use **change COR** to display the Class of Restriction screen.
3. 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.

4. Use tandem tie trunks for routing private network calls.
5. Use **change toll** to display the Toll screen. Identify what calls are allowed or disallowed.
6. Use **change ars analysis** to display the **ARS** Toll Analysis screen. Limit long distance and international calls by **ARS** calls.
7. Use **change route-pattern** to assign the appropriate **FRL** for public network trunks in the routing pattern.
8. Use **change ars analysis** to administer **ARS** Analysis Tables with at least 3- or 4-digit strings.
9. 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.
10. Use wildcard characters with care.
11. 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 must be disallowed. See Disabling direct access to trunks on page 70.

Digit conversion

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

- The conversion can be to “blank” (intercept tone), or to a Route Number Index (**RNX**) private network number.
- 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 to associate stations with extensions, and to prevent other users from accessing specific functions that require extension validation associated with a user's station.

Examples where SSCs are used include:

- IP station registration
- Softphone registration

- Personal station access
- Other extension mobility features including certain EC500 features, station lock activation, and deactivation.
- Several other features that use the station security code as an additional authentication check. For example, remote user administration of call coverage.

Because the station security code is numeric, it is important to protect it by assigning a code that isn't related to the extension number or easy to guess. Codes can contain up to 8 numbers, with an administrable minimum length. Users can use an administrable feature access code to change an SSC. As a security best practice, Avaya recommends that customers must periodically change the SSC for each administered extension.

The Security Violations Status report shows the 16 most recent invalid attempts of SSC usage for station registration. 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.

After the user enters the extension and station security code at the appropriate time, a “no response” feedback is usually provided for both success or failure entry. This makes it difficult for an automated attack to detect a success entry. 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.

Most SSC-enabled 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 transactions, access the Feature-Related System Parameters screen by entering the `change logging-levels` command and be sure that **y** is entered for `Log CTA/PSA/TTI Transactions?` to enable logging for those transactions. If Log CTA/PSA/TTI is associated with a terminal or soft client, anyone using the terminal has all the privileges and capabilities of that station.

Refer to the following registration related documents for security report information:

- *Avaya Aura™ Communication Manager Reports*, 555-233-505
- *Administering Avaya Aura™ Communication Manager*, 03-300509

EC500 Security Features

When Extension to Cellular is administered and active, a call to a configured user's CM office extension is simultaneously extended to a configured destination such as a cellular phone. When EC500 is enabled for a given CM extension, incoming EC500 calls extended across the PSTN are treated as calls that originate from the associated internal extension. In such instances policy controls such as trunk-to-trunk transfer restrictions are not applied. However, all calling restrictions associated with that CM extension are applied to the EC500 and One-X Server functionality.

If Self Administration Feature Access Code for EC500 (SAFE) is enabled, users can configure the EC500 destination number (subject to all applicable dial restrictions for their CM extension). SAFE and other inbound EC500 functions require a Station Security Code (SSC) if not performed on the local or EC500 extension assigned to the user. Remote access from the assigned EC500 extension can be validated through the ISDN ANI (automatic number identification) feature. To prevent spoofing of the ANI data, Avaya recommends that customers retain the default setting for EC500 Calling Number Verification (default is y) so that unverified "user-provided" ANI data is not trusted. If this setting is changed and EC500 is enabled, it may become possible for an attacker with knowledge of assigned cellular destinations to use that information to make unauthorized calls as an EC500 user.

Warning: Within North America, no legal requirement exists for carriers to correctly validate and screen "user-provided" ANI data. Once a carrier has marked that data as verified, other carriers accept it, and in some cases this can allow spoofed ANI data to appear to be trustworthy. Even with EC500 Calling Number Verification set to y this transitive trust problem remain an issue for customers in North America for the forseeable future.

Because of a potential for toll fraud in conjunction with ANI spoofing, Avaya recommends that customers avoid enabling one EC500 off-PBX-telephone Feature Named Extension (FNE) that can become a target for abuse: Idle Appearance Select. This FNE enables an EC500 extension (typically a user's cell phone) to receive a dial tone from CM as the office extension.

For a complete description of EC500 functionality and security feature configuration options for EC500 and one-X Server, refer to the **Extension to Cellular chapter** in Avaya Aura™ Communication Manager Feature Description and Implementation, 555-245-205.

Blocking 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.

Use the following procedure to block international calls:

1. Enter **change ars analysis** partition to display the **ARS** Analysis screen.
2. 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

Note:

As a reminder, not all international calls follow this pattern. For example, Canada uses standard area codes, as do other Caribbean countries that are part of the North American Numbering Plan.

Call Blocking Example

This section contains a sample **ARS** Digit Analysis Table. In the example, international and operator-assisted numbers are allowed, but 0700 calls are denied, as well as certain destinations which tend to have high toll fraud rates.

Use the following procedure to block calls:

1. To access the section of the **ARS** Digit Analysis Table to be changed, use **Enter digits between 0-9 "x," or 'X', ['location'(1-250 or 'all')], ['min' (1-28)]**.
2. 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: Enter route pattern (1-999), partition-route-table index (p1-p2000), RHNPA index (r1-r250), deny, or node.

d. `Call Type` field: Enter the specific call type (see examples in table below):

ARS DIGIT ANALYSIS TABLE

Partitioned Group Number: 1

Dialed	Total		Route	Call
String	**Min**	**Max**	**Pat**	**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
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

1 of 3

ARS DIGIT ANALYSIS TABLE (continued)

Partitioned Group Number: 1

Dialed	**Total**		**Route**	**Call**
String	**Min**	**Max**	**Pat**	**Type**
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
101xxxx0700	16	16		op
101xxxx1	16	16	1	fnpa

2 of 3

ARS DIGIT ANALYSIS TABLE (continued)

Partitioned Group Number: 1

Dialed	Total		Route	Call
String	Min	Max	Pat	Type
101xxxx1809	16	16		fnpa
180	11	11	1	fnpa
1809	11	11		fnpa

3 of 3

Limiting international calling

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

1. Enter **change ars analysis** to display the **ARS** Analysis screen.
2. 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**.
3. Disable TAC/DAC dialing (see Disabling direct access to trunks on page 70).
4. 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.

Selecting authorization code time-out to attendant

1. Attendent Time Out Flag indicates that a call is not to be routed to the attendent if a caller does not dial an authorization code within 10 seconds or dials an invalid authorization code.
2. Select the Timeout to Attendant feature when you administer authorization codes.
3. Use the System-Parameters features screen to request authorization code timeout.

Restricting 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. Certain destinations such as 1+809 and 0+809 (Dominican Republic), 900/976 services and look-alikes, and Alliance teleconference service (0700) are common toll-fraud destinations that must be restricted if your business doesn't require regular access to them.

1. Enter **change ars analysis** to display the **ARS** Analysis screen.
2. Specify the telephone numbers in the `Dial String` field that you do not want dialed. Enter **den** (for **deny**) in the routing pattern, or use a pattern that contains a high **FRL**.

   Note:
   In addition to blocking area codes, you can block specific destinations using this method. For instance, you may want to block toll-free access numbers for long-distance services which can also be a source of abuse.
3. Disable **TAC** dialing (see Disabling direct access to trunks on page 70).

Allowing calling to specified numbers

A reverse strategy to preventing calls is to allow outbound calls only to certain numbers specifying the area codes or telephone numbers of calls you allow.

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

Using 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.

1. Enter **change feature-access-codes** to display the **FAC** screen.
2. In the `User-Control Restrict Activation/Deactivation` fields, enter a valid **FAC**.
3. Enter **change system-parameters feature** to display the Feature-Related System Parameters screen.
4. Specify the type of intercept treatment (**announcement, attendant, extension**, or **tone**) the controlled stations will receive.

5. Enter **change COS** to display the Class of Service screen.
6. Enter **y** in the `Console Permissions` field.
7. Enter **change station** or **change attendant** to assign the **COS** to the station handling the controlled restrictions.

Disabling direct access to trunks

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

1. For each trunk group in the system:
   a. Enter **change trunk group n** (where *n* is the trunk group number) to display the Trunk Group screen.
   b. Enter **n** in the `Dial Access` field.
2. To allow individual stations to use **DAC**s, but deny **DAC** access to others, use the following procedure.
   a. Place the trunk group in a separate **COR**.
   b. Use COR-to-**COR** restrictions to deny stations with specified CORs from directly accessing the trunk group.

Using 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 screen the calls.

Up to 12 trunk groups can be controlled.

1. 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.
2. Enter the corresponding trunk access code in the `Direct Trunk Group Select Button Assignment` field.
3. 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, these trunks will be skipped in the routing pattern.

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 within media gateways..
- 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. 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, this 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.

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.

Removing the Facility Test Calls Access Code

1. Enter **change feature-access-codes** to display the FAC screen.
2. Leave the Facility Test Calls Access Code field **blank**.
3. To allow stations with a specified COR to perform the test, but deny the ability to others:
   a. Use **change cor** to display the Class of Restriction screen.
   b. Enter **y** in the `Facility Access Trunk Test` field.
   c. Use **change station** to assign the **COR** with the **FAC** test permission to the appropriate station.
   d. Assign all other stations to a **COR** with the `Facility Access Trunk Test` field set to **n**.

   e. To monitor its use, assign a trunk access alarm button to a voice terminal.

4. To help secure the Facility Test Call feature from unauthorized use, follow these steps:
   a. Remove the access code when not in use.
   b. Change the code frequently if used (else disable by leaving it blank).
   c. Protect records of the code.
   d. Use **COR**s to restrict which users can use the access code.
   e. 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.

The sign off feature can be used to alert the administrator that the code is administered.

Suppressing remote access dial tone

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.

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

Disallowing 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**, the trunks are disconnected as soon as the station hangs up.

1. Use **change system-parameters** to display the Features-Related System Parameters screen.
2. Enter the following in the `Trunk-to-Trunk Transfer` field, as appropriate:
   a. Enter **a** (all) to allow all trunk-to-trunk transfers.
   b. Enter **r** (restricted) to restrict all public trunks.
   c. 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**) feature allows a controlling party, such as a station user or attendant, to initiate two or more outgoing trunk calls and 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 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.

Configuring outgoing trunk to outgoing trunk transfer

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

Disallowing 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 calls.

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

Limiting access to tie trunks

If you need to make outgoing calls using tie trunks, you can limit access to the trunks using the following procedures.

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

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

Configuring Forced Entry of Account Code

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 outgoing trunk group or for access to AAR/ARS calls. 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).

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

Note:
CDR and account codes are only required for toll calls.

7. Use **change toll** to display the Toll Analysis screen.
8. Enter dialed strings that require **FEAC**, and enter **x** in the `Toll` and `CDR FEAC` fields.

Assign COR restrictions to call center and other adjuncts

With many adjuncts, an auto-available split assigned to the adjunct equipment (for example, Contact Center Applications, Application Enablement Services, Voice Mail, or **VRU**) must have the **COR** restrictions assigned to stations, trunks, and sometimes other entities such as or other equivalent extension. Where multiple CORs apply, such as when both the agent login ID and the extension **COR**s must have the needed restrictions, the COR of the login ID takes precedence.

Disable distinctive audible alert for adjunct equipment

The Distinctive Audible Alert feature on an analog telephone 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 must have the Distinctive Audible Alert feature (a field on the Analog Station screen) set to **no** (the default is **yes)**.

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 attackers to compromise a system.

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, the code must be changed.

Change override restrictions on 3-way COR check

Restriction Override is used with the 3-way **COR** check on transfer and conference calls. The default check is **none**.

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:

- 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, 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 a Voice Mail System subscriber (either local or remote) whose extension number is in the dial plan.

- 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.

- 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 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 unless "Coverage After Forwarding?" is set to "y" on Communication Manager or "Maximum Number of Call Forwarding Hops" is set to a number greater than 1.

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. Contact your Avaya Sales Representative for additional details and availability.

Automated attendant: Considerations for CM and Messaging

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 attackers may keep trying to get through.

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.

- 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.

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 country codes, and even to specific telephone numbers.

- 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.

Allow calling to specified numbers

A reverse strategy to preventing calls is to allow outbound calls only to certain numbers, specifying the area code or telephone number of calls you allow.

- 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.

Protect voice mail automated attendant

Disallowing outside calls

Voice Mail Systems integrated with Communication Manager provide a feature called Enhanced Call Transfer that only transfers voice mail calls to valid extension numbers. With this feature, when an automated attendant caller enters an extension as a menu choice, the 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 attackers can choose a menu option that allows an extension number, and enter a **TAC** to get an outside line.

Another advantage of this feature is that when a toll attacker tries to enter an unauthorized number, the voice mail system error message notifies the attacker that this automated attendant system is secure.

1. On the voice mail 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 switch, use **change listed-directory-numbers** to add a valid extension for your attendant.
5. After you activate Enhanced Call Transfer, dial into your voice mail system automated attendant.
6. Press the menu choice to transfer to an extension.
7. Enter an invalid extension number followed by **#**.

   The failed announcement must play, followed by a prompt for another extension number.
8. Enter a valid extension number followed by **#**.

   You might 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, dial back in on the number assigned to the automated attendant. A station to station connection will not test correctly.

Avaya Aura^{TM} Communication Manager Messaging

Enhanced call transfer

With the Enhanced Call Transfer feature:

- The voice mail system uses a digital control link message to initiate the transfer
- 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:

- 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, 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 a Voice Mail System subscriber (either local or remote) whose extension number is in the dial plan.
- If the verification is successful, the voice mail system sends a transfer control link message verification is unsuccessful, the voice mail system plays an error message to the caller and prompts for another try.
- The switch verifies that the digits entered match a valid station number in the dial plan.
  - If the switch verification 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 the switch verification 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 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 unless "Coverage After Forwarding?" is set to "y" on Communication Manager or "Maximum Number of Call Forwarding Hops" is set to a number greater than 1.

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. Contact your Avaya Sales Representative for additional details and availability.

Transfer out of the system

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:
Transfers are permitted only to numbers administered in the **transfer-dialplan** screen. Refer to your voice messaging 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, and 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 can also 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 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 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.

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 extension. However, if you do not need to transfer out, consider eliminating this feature (see Transfer out of the system on page 80 for details).

Use the Feature-Related System Parameters screen, entering **none** in the `Transfer Type` field.

Note:
If the automated attendant system uses transfer to an extension, you cannot use this security measure.

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.

- Use **change cor** to display the Class of Restriction screen, and create an outward restricted **COR** by entering **outward** in the `Calling Party Restriction` field. The COR must carry an FRL of 0. Outward calling party restrictions and calling permissions must be blocked from all trunk CORs.
- Assign the outward restricted **COR** to the voice mail system voice ports.

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:
For outcalling 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 CM outgoing call restrictions on the voice mail system voice ports.

Call Management System

Call Management System is a reporting system for call centers that provides real time and historical data about the status and performance of a customer's call. This data includes information about agents, trunks, trunk groups, splits/skills, busy hours, forecasts, and so on.

In addition to the reporting data passing from CM to the CMS system, vector modifications can be sent from the CMS system to CM. Unauthorized vector modifications or abuse of CMS access lines can make toll fraud possible in certain circumstances. It is important to secure access to the CMS system and its links to CM.

Note:

Avaya recommends, for both security and performance reasons, that the Ethernet connectivity between the CMS and CM must be a separate LAN segment. Otherwise, an unscrupulous person can gain unauthorized access to Vector/VDN functions to commit toll fraud and tamper with the real-time aspects of CTI applications

Security tips

The following considerations are for the **CMS** administrator.

- When setting up the ports, modems must be defined in UNIX (using the FACE administration tool) for inbound access only.
- If station lines are used for the modems, the **COR** must be set to disallow outbound dialing capabilities.
- Switchhook flash and distinctive audible alert must be set to **no** on the Station screens.
- Remote users must not have access to UNIX via the **CMS** application. Restrict access by means of the User Permissions feature of **CMS**.
- Assign a static or reserved address to the CMS server and ensure the SPI link configuration within CM is restricted to that IP address

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 quick reference information listed under the Call Management System (CMS) product documentation heading on http://www.avaya.com/support.

For switch restrictions, see the CM section in this chapter. You can also refer to the CM administration manuals.

Modular Messaging

Review your Modular messaging configuration regularly to block potential avenues for toll fraud that enable calls from outside the enterprise to be transferred to another outbound trunk.

⚠ **WARNING:**
Toll fraud is a theft of long-distance service. When toll fraud occurs, your organization is responsible for the charges incurred. For more information about how to prevent toll fraud, call the Avaya Customer Care Center at **1-800-643-2352** and Avaya Support at **1-800-242- 2121**.

Because opportunities for toll fraud can potentially exist across many different messaging system functions, it is essential for customers to keep each and every potential avenue for fraud locked down appropriately. In general, the settings listed below default to the most secure option initially and must be changed during configuration. Within each of the sections below, you will find guidance and recommendations for protecting that function from toll-fraud exploit.

The following table lists the security goals for each Modular messaging system, and provides an overview of the methods and steps that are offered through the switches to minimize the risk of unauthorized use of the system.

Table 3: MM Security goals

Security Goal	Method	Security Feature	Steps	Page #
Prevent unauthorized calling	Block transfers to invalid mailboxes	Block invalid mailbox transfer	Disable "Transfer Invalid Mailboxes"	85
		Block invalid mailbox transfer	System Operator must be a valid MM mailbox number	86
			Set outcalling restrictions	86
	Carefully configure attendant, operator, and subscriber application options	Automated attendant settings	Ensure menu option settings are appropriate	86
		Caller application settings	Ensure settings are appropriate	87
		Personal operator settings	Ensure settings are appropriate	87
		Find Me, Call Me, Notify Me settings	Ensure settings are appropriate	88
			Restrict subscriber features with COS	88
		Fax settings	Ensure external hunt group setting is correct	89

Table 3: MM Security goals

Security Goal	Method	Security Feature	Steps	Page #
Protect subscriber mailbox from unauthorized access	Configure mailbox PIN and lockout settings	Mailbox PIN and lockout settings	Configure appropriate PIN complexity and expiration settings	89
			Configure appropriate lockout settings	89
			Deactivate unused mailboxes	89
Protect administrative interfaces from unauthorized access	Limit access to IP and telephony-based administrative access	Authentication and Authorization features	Manage administrative credentials and roles	89
		COR	Use COR to restrict access to administrative ports	89

Security tips

The **MM** administrator can use the following security tips.

Disable transfer to invalid mailboxes

Ensure that MM is configured to allow transfer only to valid MM mailboxes, and not to arbitrary extension numbers, by disabling the following settings using VMSC:

- VMD / TUI / Receptionist / Transfer Invalid Mailboxes during Business Hours
- VMD / TUI / Receptionist / Transfer Invalid Mailboxes after Business Hours

System operator

Ensure that MM does not allow transfer to invalid mailboxes. For more information, see Disable transfer to invalid mailboxes on page 85.

Configure the system operator to be a valid MM mailbox number, and not an extension number. Check if any mailboxes are being used as operators to ensure that the primary extension number is correct.

For non-MultiSite systems, the system operator is configured in the following two places. The system operator number may default to 0, and must be changed:

- VMD / TUI / Receptionist / Default Receptionist Mailbox Number
- VMD / TUI / Receptionist / After Hours Receptionist Mailbox Number

For MultiSite systems, the system operator is configured for each site:

- VMD / Sites / Configure / [Site name] / Open business hours mailbox
- VMD / Sites / Configure / [Site name] / Out of hours mailbox

Automated Attendant

Ensure that MM does not allow transfer to invalid mailboxes. For more information, see Disable transfer to invalid mailboxes on page 85.

If transfers to extensions as well as mailbox numbers are needed, prevent MM from transferring to numbers entered by callers if they start with specific digits. Ensure that the digits used to access an outside line are not selected in the following VMSC setting for non-MultiSite systems:

- VMD / TUI / Caller / Outcalling Restrictions

For MultiSite systems, Automated Attendant outcalls (Including those routed through a mailbox number) are restricted based upon a combination of the cost of the call (calculated using the PBX-specific outgoing phone number translation rules) and the VMD-wide setting for the **Maximum cost for Automated Attendant outcalls**. You must configure the translation rules to ensure that external callers can transfer only to phone numbers that you explicitly allow:

- VMD / PBXs / [PBX name] / SIP / Configure
- VMD / Sites / Maximum cost for Automated Attendant outcalls

See the Modular Messaging MultiSite Guide for details. If you choose to disallow Automated Attendant calls to external numbers, be aware that it will also affect Caller Applications

Additional recommendations for preventing toll fraud on Automated Attendant:

- Never allow a menu option to transfer to an outgoing trunk without a specific destination.
- When a digit from 1 through 9 is not a menu option, program the digit to perform one of the following actions:
  - Transfer to an attendant
  - Transfer to an announcement and disconnect the call

  - Intercept the call

- When 8 or 9 is dialed to access an outgoing line, program 8 or 9 on the Automated Attendant tab to take one of the following actions:
  - Translate to an extension
  - Transfer to an attendant
  - Make an announcement and disconnect the call
  - Intercept the call
- Restrict call transfers to subscribers when Basic Call Transfer is used.

Use the Outcalling Restrictions feature to prohibit users from obtaining an external line when they dial an initial digit of an invalid mailbox number. For more information about Outcalling Restrictions, see the Messaging Application Server Administration Guide.

- If any menu option routes to a Direct Inward System Access (DISA) feature on the PBX (Avaya does not recommend this) the user hears a system dial tone. For system security, the PBX must require users to dial a barrier code. If a valid barrier code is dialed, the user hears a dial tone and can place calls the same way as an on-premises user.

Caller Applications

Check all caller applications to ensure that any custom operators correspond to a valid MM mailbox, not an extension number. Check if any mailboxes are being used as operators to ensure that the configured primary extension number is correct.

Ensure that MM does not allow transfer to invalid mailboxes. For more information, see Disable transfer to invalid mailboxes on page 85.

- For MultiSite systems, caller applications are treated the same as the Automated Attendant for the purposes of restricting outcalls. Subscriber outcalls are restricted based upon a combination of the cost of the call calculated using the PBX-specific outgoing phone number translation rules, and the VMD-wide setting for the Automated Attendant:
- VMD / PBXs / [PBX name] / SIP / Configure
- VMD / Sites / Maximum cost for subscriber outcalls

See the Modular Messaging MultiSite Guide for details. If you choose to disallow Automated Attendant calls to external numbers, be aware that it will also affect all other transfers by the Automated Attendant.

Personal operators

- Subscribers can define their own personal operator only if the relevant class of service has the **Personal Operator Configuration** option set to yes.
- Ensure that MM is configured to allow only personal operators that are valid MM mailboxes and not arbitrary extension numbers, by disabling the following option:

  - VMD / TUI / Receptionist / Allow personal operators that are not local mailboxes
- Prior to MM 5.0, default configurations allowed personal operators that are not valid MM mailboxes; this setting must be disabled to prevent an MM subscriber from setting their personal operator as the outside line prefix.
- For MultiSite systems, subscriber outcalls are restricted based upon a combination of the cost of the call calculated using the PBX-specific outgoing phone number translation rules, and the VMD-wide setting for the Automated Attendant:
  - VMD / PBXs / [PBX name] / SIP / Configure
  - VMD / Sites / Maximum cost for subscriber outcalls

See the Modular Messaging MultiSite Guide for details. If you choose to disallow subscriber calls to external numbers, be aware that it will also affect other subscriber outcalls like Find Me and Call Me.

Find Me / Call Me / Notify Me

- The Find Me feature enables your mailbox to redirect unanswered calls to a list of telephone numbers. For more information, see VMSC - VMD - Messaging - Offline Access Tab.
- The Call Me and Notify Me features deliver notifications to subscriber-designated telephone numbers, email addresses or devices. The Call Me feature places telephone calls to subscribers at a designated number whenever the subscriber receives a message that meets certain criteria. The feature invites the subscriber to log in to the telephone user interface (TUI) and review the message. For more information, see VMSC - VMD - Call Me Dialog Box.
- Transfers performed as part of these operations are not usually prone to toll fraud because the transfer is supervised, and control reverts to MM if the enquiry call is not answered. However, depending upon the precise system configuration including the integration type, an unsupervised transfer may be performed. To guard against the possibility of toll fraud, you can configure the following settings to no in the relevant class of service:
  - Find Me Allowed
  - Call Me Allowed
  - Notify Me Allowed
  - Additional recommendations for Find Me / Call Me / Notify Me:
  - Control access to these features via a Class of Service (COS) setting.
- Avaya recommends that administrators enable these features by relevant COS for only the subscribers that require this method of notification. Administrators can also assign a restrictive PBX COS to the PBX ports used to make the outbound call, or require account codes or authorization codes.
- Review your use of outbound calls to ensure that your subscribers establish reasonable rules for the Call Me and Find Me features. The rules must not waste telephone resources.

Fax

- If you are using fax with MM and have it configured to use a third-party fax server, you must check that the following setting is configured to be the correct hunt group number for the fax server that you are using:
    - VMD / Fax / General / Hunt Group Pilot Number

Configuring Subscriber Mailbox Protection

Certain types of toll fraud result from the compromise of a subscriber mailbox. The following recommendations can decrease the likelihood of a mailbox break-in:

- Increase the minimum password (PIN) length required for subscriber passwords.
- Don't use temporary passwords.
- Deactivate unassigned mailboxes, and remove unused mailboxes.
- Avoid or closely monitor the use of guest mailboxes. A guest mailbox is not allotted a physical extension. If you do not need the mailbox, deactivate it. Assign the mailbox only after changing its password
- Enable mailbox lockout after multiple consecutive unsuccessful attempts to enter a voice mailbox. Administrators can configure the number of unsuccessful attempts before lockout.
- Ensure new users set a password as soon as possible after their voice mail system extension is assigned.
- Always require each subscriber to change his or her initial password immediately upon first log-in. To do so, administer the subscriber default password to be fewer digits than the minimum password length
- Administer password aging on the System Parameters Features screen. Password aging requires subscribers to change their password at a predefined interval. It enhances overall system security and helps protect against toll fraud by making the system less vulnerable to break-ins.

Configuring Administrative Access and System Protection

Compromise of administrative accounts can be much more damaging in terms of toll fraud than the compromise of an individual mailbox. See the Modular Messaging Security Guide for more details regarding MM security features designed to protect administrative access, and consider implementing the following best practices:

- Record and store the critical administrative passwords in a secure place, preferably off-site. Never discard an active password.

- Use Class of Restriction (COR) on Avaya CM systems (or equivalent restrictions on 3rd-party PBX systems) to restrict access to administration ports. If you use scriptable PC software to access administration capabilities, do not store the following information without proper protection:
    - Dial-up numbers
    - Logins
    - Passwords as part of an automatically executed script
- Use the monitoring tool to check the performance of your system. For more information, see SPM - Port Monitor. You can also generate reports for port statistics, port usage, and port states. Examine system usage and port usage reports regularly. For more information about the various reports that you can generate, see the MAS Administration Guide

End-user and administrator awareness

Everyone who uses the system is responsible for maintaining the security of the system. Users and attendants must know how to recognize and react to potential attacker activity. Informed people are more likely to cooperate with security measures that make the system less flexible and perhaps more difficult to use. Renewed awareness in the form of a refresher course or an updated manual can enhance the general security of the system.

Here are some specific guidelines for end-users and administrators:

- Never set a personal greeting that states that the called extension accepts collect calls or third-party billed calls. If someone at your company has a similar greeting, ensure that they change the greeting immediately.
- 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 passwords. If a password needs to be written down, keep the password in a secure place, and never discard the password while it is active.
- Establish a well-controlled procedure for resetting passwords.
- Advise attendants to inform their system manager when they answer a series of telephone calls in which the caller is silent or hangs up.
- Advise users who have voice mailboxes that they must change personal passwords frequently. Do not choose obvious passwords.
- Advise users with special telephone privileges of the potential risks and responsibilities. Special telephone privileges can include remote access, voice mail outbound calling, and call forwarding off-switch.
- Advise users that they must be suspicious of any caller who claims to be with the telephone company and wants to check an outside line. Users must ask for a callback number, hang up, and confirm the caller's identity.

- Never distribute the office telephone directory to people outside the company. Be careful when discarding it.
- Never accept collect telephone calls.
- Never discuss your telephone system numbering plan with anyone outside the company.
- Distribute voice mail security policies to all employees.
- Ensure that operators and receptionists are security conscious and do not transfer callers to an outside line.
- Establish procedures to prevent social engineering. Social engineering is a con game that attackers frequently use to obtain information that can help them gain access to your system.

More recommendations

- Clear the digit or digits used to request external lines from the PBX to prohibit callers from obtaining an external line. For example, a call must use 9 to access an external line. When you clear 9 on the PBX, callers cannot access an external line when they dial the invalid mailbox 9004. By default, the PBX selects all digits.
- Ensure that outbound access to SIP trunks is restricted when using an external SIP gateway such as the AudioCodes SIP gateway.
- Restrict call transfers to the host PBX when the system does not allow transfers, uses Enhanced Call Transfer, or permits Transfer to Subscriber Only.

Avaya Aura^{TM} Session Manager

Avaya Aura^{TM} Session Manager is a SIP routing and integration tool that integrates all the SIP entities across an entire enterprise network. Because Session Manager supports centralized routing and dial plans with policy-based routing and centralized SIP trunking, you must prevent untrusted entities from communicating directly with Session Manager. Follow the security tips below to minimize your exposure to toll fraud through Session Manager.

Security tips

The following considerations are for the **Session Manager** administrator.

- Verify with your SIP service provider (or trunking peer) if the inbound SIP traffic that does not match your dial plan or DID range, will be blocked even if it contains your domain suffix. Otherwise the inbound E.164-encoded SIP traffic might be routed out to another SIP trunk.

- Add routing rules that block access to external SIP trunks for
    - Traffic to 900/976 and other commonly-abused PSTN destinations.
    - Malformed SIP addresses that end in your domain but do not match your numbering plan.
- Whenever possible, configure SIP-TLS for SIP connections to session manager and use unique server certificates for Session Manager and all the servers that communicate with it.
- Use the SIP blacklist function to block traffic from known risky SIP elements.

Chapter 4: Toll fraud detection

Toll fraud warning signs

- Customers or employees complain that the toll-free access number is always busy. The busy line can 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 with bill detail showing calls to unfamiliar or typical destinations.
- Increase in short duration calls and calls to unprovisioned numbers.
- Heavy call volume on nights, weekends, and holidays.
- CDR 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, unusual messages left in mailboxes, or suspicious changes being made to outgoing greetings by others.
- 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.

Avaya Aura^{TM} Communication Manager

Detect toll fraud

After you have taken the appropriate security measures, use the monitoring techniques described in this section to routinely review system activity.

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

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

Table 4: Reports and monitoring techniques

Monitoring Technique	**Page #**
Monitor trunks	95
Call detail recording (**CDR**)	95
Traffic measurements/ performance	96
Automatic circuit assurance	97
BCMS measurements	98
CMS measurements	98
Security Violations Measurement report	100
Security Violation Notification feature	98
Recent Change History report	109
	1 of 2

Table 4: Reports and monitoring techniques (continued)

Monitoring Technique	Page #
Service observing	110
Malicious call trace	110
list call-forwarding command	111
	2 of 2

Monitor trunks

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

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.

Call detail recording

This feature creates records of calls that must 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 is activated for the remote access trunk group.

Authorization codes, if required, are recorded by CDR; 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 *Administering Avaya Aura™ Communication Manager*.) Review the report for these condition codes, which might indicate attacker activity.

Avaya and 3rd-party partners offer several call accounting system add-ons that enhance CDR by allowing you to create customized reports. These reports can be used to isolate calls that may be suspicious.

Note:

Unless **Outg Trk Call Splitting** is configured on the **change system-parameters CDR** screen, 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 can give a false indication that your voice mail system is the source of the toll fraud.

Review **CDR** 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

Creating records of calls that must be checked regularly

1. Use the **change system-parameters cdr** feature to display CDR system-parameters screen.
2. Administer the appropriate format to collect the most information. The format depends on the capabilities of your **CDR** analyzing/recording device.
3. Use **change trunk-group** to display the Trunk Group screen.
4. Enter **y** in the `CDR Reports` field.

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 success in doing so
- High volume on AAR/ARS 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

SAT reporting

Traffic reporting capabilities are built-in and are obtained through the System Access Terminal (**SAT**). 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 must therefore be printed to monitor a history of traffic patterns. Refer *Reports for Avaya Aura*$^{\text{TM}}$ *Communication Manager* for complete details on these reports.

- 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 25 routing patterns for traffic flow and usage.

- Enter **change meas-selection route pattern** to choose the routing patterns you want to track.
- Enter **list measurements route-pattern** with assigned pattern (1-999) followed by the timeframe (**yesterday**, **today**, or **last-hour**) to review the measurements, followed by the assigned route pattern then by the time frame. (or vice versa)

Configuring Automatic circuit assurance

This monitoring technique detects a pattern of short holding time calls or a single long holding time call which may indicate attacker 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 Configuring Busy verification on page 111) to monitor the call in progress.

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

1. Enter **change system-parameters feature** to display the Features-Related System Parameters screen.
2. Enter **y** in the `Automatic Circuit Assurance (ACA) Enabled` field.
3. 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.

4. 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.
5. To review and verify the entries, enter **list aca-parameters**.
6. Enter **change trunk-group** to display the Trunk Group screen.
7. Enter **y** in the ACA Assignment field.
8. Establish short and long holding times. The defaults are 10 seconds (short holding time) and one hour (long holding time).
9. To review an audit trail of the ACA referral call activity, enter **list measurements aca**.

Configuring BCMS measurements

BCMS Measurements report traffic patterns for measured trunk groups.

1. Use **change trunk-group** to display the Trunk Group screen.
2. In the Measured field, enter **internal** if you have only **BCMS** or **both** if you have **BCMS** and **CMS**.
3. Use **change system-parameters feature** to display the Features-Related System Parameters screen.
4. To review the measurements, use **list bcms trunk**.

Configuring 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.

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

Security violation notification

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. Once an **SVN** threshold is reached, (for a remote access barrier code, or an authorization code), the system initiates a referral call to an assigned referral destination.

The referral destination can be any station, if an announcement has been administered and recorded. The **SVN** Referral Call with Announcement option provides a recorded message identifying the type of violation accompanying the **SVN** referral call, such as 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 remote access or 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 authorization code attempts is collected at two levels:

- On an immediate basis, when an invalid login attempt is made, 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.
- 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 100.)

Configuring the SVN feature

1. Enter **change system-parameters security** to display the System-Parameters Security screen.
2. To monitor remote access, enter **y** in the `SVN Remote Access Violation Notification Enabled?` field.
3. To monitor authorization codes, enter **y** in the `SVN Authorization Code Violation Notification Enabled` field.
4. Enter any valid unassigned extension number in the `Originating Extension` field(s).
5. Enter the extension number of the person who will monitor violations in the `Referral Destination` field(s). If an announcement extension is administered, the referral destination does not require a display module. A violation occurs based on the number of invalid attempts.

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

6. 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.

   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.

7. On the station form in the `Feature Button Assignment` field, enter **rsvn-halt** for the Remote Access Security Violation Notification button and asvn-halt to light the associated status lamp. 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 de-activated before referral calls are sent to the referral destination.

8. **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.

9. 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.

Security Violations Measurement reports

This report identifies the entry of invalid barrier codes. It monitors the remote access ports. Review the report daily to track invalid attempts to enter barrier codes, which may indicate attacker activity.

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

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

  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

- Use **monitor security-violations** for a real-time report of attempts to obtain remote access using invalid barrier codes or authorization codes.

  monitor security-violations

  – <remote-access>

  – <authorization-code>

  The three resulting Security Violations Measurement reports provide current status information for invalid login attempts, remote access (barrier code) attempts, and authorization code attempts.

  The report titles are as follows:

  - 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 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

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.

Administering the SVN feature

This section contains the following subsections:

- Administering the barrier code security violations parameters of the SVN feature
- Administering the authorization code component
- Administering the station security code component

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**.
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.

     Call vectoring using time of day routing allows security notification to be extended off-premises.

   - `Barrier code Threshold`

     Enter the minimum number of invalid authorization code attempts that are 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 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, change the Remote Access screen and enter **y** in the `Disable Following a Security Violation` field.
4. 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.

Enabling/disabling remote access code

1. To enable remote access that has been disabled following a security violation, or disabled manually with the **disable remote-access** command:
   a. Log in to the switch using a login ID with the proper permissions.
   b. Enter the command **enable remote-access**.
2. To disable remote access:
   a. Log in to the switch using a login ID with the proper permissions.
   b. 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 security**.

   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 must 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 authorization code component

To administer the authorization code component of the **SVN** feature, 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. 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.

Security violations reports

The security violations reports provide current status information for invalid login or remote access (barrier code) or authorization code attempts. The following security violations reports are available:

- Remote Access Barrier Code Violations
- Authorization Code Violations
- Station Security Code (SSC) Violations

Note:
Station security codes are used with many registration-related security features.

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 **remote-access**, **station-security-codes**, or **authorization-code**.

Remote access barrier code aging/access limits

Remote Access Barrier Code Aging allows the system administrator to specify both the time interval a barrier code is valid, and 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 must be removed from the system. Barrier codes must be safeguarded by the user and stored in a secure place by the switch administrator. See Chapter 3: Product policy controls for information on administering Barrier Code Aging.

Recent Change History report

The latest administration changes are automatically tracked. For each administration change that occurs, the system records the date, time, port, login, and type of change that was made.

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

Note:

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

The history log has 500 entries (1800 in larger systems), and provides login and logoff entries. This log includes the date, time, port, and login ID associated with the login or logoff. If available, calling number display information is included.

Malicious call trace

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 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 attackers. 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 the calling number identification is available on the incoming trunk, 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 *Avaya Aura*^{TM} *Communication Manager Feature Description and Implementation Guide, 555-245-205* for more information.

Configuring Service observer

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 must familiarize themselves with and comply with all applicable laws, rules, and regulations before using this feature.

1. Enter **change system-parameters features** to display the Features-Related System Parameters screen.
2. Enter **y** in the **Can be service observed?** and/or **Can be a service observer?** fields as appropriate.
3. Enter **change station** to display the Station screen.
4. Enter **serv-obsrv** in the `Feature Button Assignment` field.
5. Use **change cor** to display the Class of Restriction screen.
6. Enter **y** in the `Service Observing` field.
7. Enter **change station** to assign the associated **COR**s to the rving station and stations to be observed.

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, use barrier codes to protect remote service observing.

Configuring 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.

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

List call-forwarding command

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

Detecting adjunct-related fraud

Monitoring Technique	**Page #**
Call detail recording (**CDR**)	112
Traffic measurements and performance	114
Automatic circuit assurance	115
Busy verification	111
Call Traffic report	114
Trunk Group report	114
Traffic reports	121
Voice session record	115

Note:
The system administrator can also view a logfile to see if a mailbox is being hacked. 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 and other adjunct ports. A series of short holding times may indicate repeated attempts to enter voice mailbox passwords or similar brute-force attacks on adjunct interfaces.

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 or other adjunct 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

Activating the CDR feature:

1. Use the **change system-parameters cdr** feature to display the CDR System Parameters screen.
2. Administer the appropriate format to collect the most information. The format depends on the capabilities of your **CDR** analyzing and recording device.
3. Use **change trunk-group** to display the Trunk Group screen.
4. Enter **y** in the `CDR Reports` field.

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 attacker activity.

For Communication Manager, the traffic data reports are maintained for the last hour and the peak hour.

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 reporting

Traffic reporting capabilities are built-in and are obtained through the System Access Terminal (**SAT**). 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 must therefore be printed to monitor a history of traffic patterns.

- 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 25 routing patterns for traffic flow and usage.

- 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.

Configuring Automatic circuit assurance

This monitoring technique detects a number of short holding time calls or a single long holding time call which may indicate attacker 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 Configuring Busy verification on page 111) to monitor the call in progress.

1. Use **change system-parameters features** to display the Features-Related System Parameters screen.
2. Enter **y** in the `Automatic Circuit Assurance (ACA) Enabled` field.
3. 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.
4. Use **change trunk group x** (where ***x*** identifies the trunk group to be modified) to display the Trunk Group screen.
5. Enter **y** in the `ACA Assignment` field.
6. Establish short and long holding times. The defaults are 10 seconds (short holding time) and one hour (long holding time).
7. To review, use **list measurements aca.**
8. Administer an **aca** button on the console or display station to which the referral will be sent.

Detecting Toll Fraud with Communication Manager Messaging and Modular Messaging

Voice session records

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 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 5.

Table 5: Voice Mail System session termination values

Value	Reason for Session Termination
01	Caller transferred out of the Voice Mail System
02	Caller disconnected established call
03	Caller abandoned call before the Voice Mail System **answered**
04	Caller entered **X
05	Caller entered *R from call answer
06	Caller entered **R from voice mail
07	The Voice Mail System terminated the call due to a system problem
08	The Voice Mail System terminated the call due to a caller problem (for example, full mailbox timeout)
09	The Voice Mail System terminated call originated by another 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 records

An outgoing call record is also created for every outbound call that is originated by the Voice Mail System via a voice port. This includes call transfers, outcalling, and message waiting activation and 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 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 6.

Table 6: 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 attacker 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 Voice Mail System calls

Detecting automated attendant toll fraud with related CM functions

Monitoring Technique	Page #
Call detail recording (**CDR**)	118
Traffic measurements and performance	119
Automatic circuit assurance	120
Busy verification	111
Call Traffic report	119
Trunk Group report	119
Voice Mail System traffic reports	121
Voice Mail System call detail recording	121

Call 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 on page 98.

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

Activating CDR:

1. Display the Features-Related System Parameters screen by using **change system-parameters cdr**.
2. Administer the appropriate format to collect the most information. The format depends on the capabilities of your **CDR** analyzing/recording device.
3. Use **change trunk-group** to display the Trunk Group screen.
4. Enter **y** in the `CDR Reports` field.

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 attacker activity.

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 reporting

Traffic reporting capabilities are built-in and are obtained through the System Access Terminal (**SAT**). 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 must therefore be printed to monitor a history of traffic patterns.

- 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 25 routing patterns for traffic flow and usage.

- 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.

Configuring 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 attacker 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 Configuring Busy verification on page 111) to monitor the call in progress.

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

1. Use **change system-parameters features** to display the Features-Related System Parameters screen.
2. Enter **y** in the `Automatic Circuit Assurance (ACA) Enabled` field.
3. 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.
4. 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**.
5. Assign an **aca referral** button on that station (or the attendant station).
6. Use **change trunk group** to display the Trunk Group screen.

7. Enter **y** in the `ACA Assignment` field.
8. Establish short and long holding times. The defaults are 10 seconds (short holding time) and one hour (long holding time).
9. To review, use **list measurements aca**.
10. Administer an **aca** button on the console or display station to which the referral will be sent.

Traffic reports

Voice Messaging systems 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.

Call detail recording

This optional voice messaging 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 Voice Mail System, is redirected to the 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 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.

Table 7: Voice Mail System session termination values

Value	Reason for Session Termination
01	Caller transferred out of the Voice Mail System
02	Caller disconnected established call
03	Caller abandoned call before the Voice Mail System **answered**
	1 of 2

Table 7: Voice Mail System session termination values (continued)

Value	Reason for Session Termination
04	Caller entered **X
05	Caller entered *R from call answer
06	Caller entered ****R** from voice mail
07	The Voice Mail System terminated the call due to a system problem
08	The Voice Mail System terminated the call due to a caller problem (for example, full mailbox timeout)
09	The Voice Mail System terminated a call originated by another 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
	2 of 2

Outgoing voice call detail record

An outgoing call record is also created for every outbound call that is originated by the Voice Mail System via a voice port. This includes call transfers, outcalling, and message waiting activation and 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 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.

Table 8: 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
	1 of 2

Table 8: Outgoing Call Type Values (continued)

Value	Outgoing Call Type
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
	2 of 2

Unsuccessful call transfer attempts can result in multiple records being created for a single session. Review these records regularly for the following signs of attacker 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 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.

MM Report tool

Modular Messaging provides several monitoring functions to review and track various activities within the messaging system. One of the most common tools used for Toll Fraud Detection is the Reporting Tool, which generates comprehensive reports on the following types of information:

"Subscriber mailbox port usage

"Subscriber incoming and outgoing call activity

"Planning capacity

"Tracking system security

You can view each report for an entire day or for each hour. Review these reports on a regular basis to help establish traffic trends. Use the reporting and monitoring tools to monitor your system on a regular basis. If you notice any suspicious or unusual patterns, take corrective action. Avaya recommends that customers investigate the possibility of active toll fraud when any combination of these symptoms appears unexpectedly:

"Employees cannot get outside lines.

"Customers have difficulties connecting to your toll-free number. The busy line can impact local Direct Inward Dial (DID) lines.

"Users cannot explain an increase in long-distance usage.

"System reports an increase in short duration calls.

"Administrators notice a significant increase in internal requests for assistance in making outbound calls, particularly international ones.

"The system experiences heavy call volume during the night-time and weekend hours.

"The system receives a sudden increase in wrong numbers.

"Bills show calls made to unfamiliar or typical numbers.

"Attendants report frequent "no one there" or "sorry, wrong number" calls.

"Switchboard operators complain of frequent hang-ups or touchtone sounds when they answer.

"Sudden or unexplained inability to use specific administrative functions within the system.

"Staff or customer complaints of inability to enter the voice mail system.

"Simultaneous DISA authorization code use coming from two different places at the same time.

"Unusual increase in the use of customer premises equipment-based system memory.

"Unusual increase in the number of subscribers with locked mailboxes.

"Unexplained changes in system software parameters.

"One or more subscribers discover that a personal greeting was changed or suspicious messages were received

Avaya technical and toll fraud crisis intervention

If you suspect any toll fraud or service theft and need technical support or help, contact Avaya by telephone, e-mail, or the Internet.

Telephone. Avaya provides a telephone number that you can use to report problems or to ask questions about your products. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site at http://www.avaya.com/support/.

These services are available 24 hours a day, 365 days a year. Consultation charges may apply.

E-mail. Send information regarding any discovered security problems with Avaya products to either the contact noted in the product documentation or to securityalerts@avaya.com.

Internet. Information on Avaya Security Advisories and Notification is available at http://support.avaya.com/security.

Call Management System

Detecting toll fraud

Although it is rare to see toll fraud that occurs through a CMS system, CMS reports can help you detect potential toll fraud. Vector reports should be reviewed to ensure unauthorized vector changes are not made. You should also review Access logs and role assignments to ensure that only authorized users have access to the system and the abililty to make vector changes.

Appendix A: Security support services

Avaya support

Secure remote access to your Avaya products by Avaya support personnel can be provisioned via PSTN or IP VPN. For more information, contact your support representative.

Security Hardening Services

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.

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

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
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 AAR/ ARS 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	A Voice Mail System feature that connects the 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.
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.

Attacker A criminal who attempts to penetrate PBX systems to gain unauthorized access to their features.

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 Voice Mail System validates that the number of digits entered matches the length of extensions in the dial plan, and 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 995) that specifies the calling privileges and limitations assigned to stations, Remote Access users, and trunk groups.

Class of Service A number (0 through 15) or group that specifies if users can activate Automatic Callback, Call Forwarding, Console Permissions, Data Privacy, and Priority Calling features. 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 Voice Mail System feature that provides security by interacting with the PBX system to validate that the number entered by an 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 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.

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.

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 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 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 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

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

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 attackers 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

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 attackers that randomly dials telephone numbers (typically local or toll-free access numbers) until a modem or dial tone is obtained.

WATS Wide Area Telecommunications Service

WCR World Class Routing, an obselete term for AAR/ARS 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 Provides flexible network numbering plans (See AAR/ARS).

Index

Numerical

0 calls . . . 61, 96
00 calls . . . 61
01 calls . . . 65
010 calls . . . 65
011 calls . . . 65, 96
10xxx calls . . . 19, 61
10xxx01 calls . . . 65
10xxx11 calls . . . 65
3-way COR check . . . 45, 75
6-digit screening . . . 19
800 numbers . . . 19, 21, 38, 93
800 service
  trunks . . . 21
911 number . . . 44
950 numbers . . . 19
976-look-alike numbers . . . 19

A

AAR/ARS
  analysis . . . 57
abuse
  internal. . . 19, 24
access
  administration and maintenance . . . 29
account code
  undefined . . . 96
administration and maintenance access . . . 29
after-hours calling
  preventing . . . 42
  restricting . . . 43
alarm
  ACA . . . 97
  long holding time . . . 120
  sending to attendant . . . 98
alternate carrier access . . . 18
Alternate Facility Restriction Level . . . 43
  preventing after-hours calling . . . 42
AMIS Networking . . . 80
ANI, see Automatic Number Identification
area codes
  restricting calls . . . 77
ARS Measurement Selection . . . 97, 114, 120
attendant
  call routing . . . 39, 41
  reporting suspicious calls . . . 24
attendant console
  Facility Restriction Level . . . 55
  physical security. . . 25
attendant control
  specific extensions . . . 69
Audio Message Interchange Specification . . . 80
AUDIX Voice Mail System
  Call Detail Recording . . . 121
  disabling transfer out . . . 81
AUDIX Voice Power System
  automated attendant. . . 78
authorization code . . . 38, 43, 50, 52
  invalid login attempts . . . 101
  monitoring usage . . . 53
  removing . . . 52
  Time-Out to Attendant . . . 68
  used with barrier code . . . 48
  VDN . . . 51
Authorization Code Violations Status Report . . . 101
auto dial button. . . 24
  programming passwords. . . 28
automated attendant . . . 13, 17, 80, 81, 115
  AUDIX Voice Mail System . . . 78
  nested . . . 121
  ports . . . 77
  restricting menu options . . . 77
  symptoms of abuse . . . 118
Automatic Alternate Routing
  setting FRLs . . . 43
Automatic Circuit Assurance . . . 97, 120
  referral calls. . . 97
Automatic Number Identification . . . 94
Automatic Route Selection . . . 58

B

barrier code . . . 38, 46, 52
  aging . . . 48, 109
  COR . . . 43, 48, 52
  COS . . . 48
  default expiration dates and upgrades . . . 109
  invalid entry . . . 100
beeper scam . . . 19
bulletin board. . . 17, 80
Busy Verification . . . 111
  button . . . 111
button
  auto dial . . . 24, 28

Busy Verification 111
Login SVN 100
night service 56
Remote Access SVN 100
rsvn-halt 104
trk-ac-alm 72
Verify 111

C

call
ACA referral 97
allowing to specified numbers 77
disallowing outbound 78
international 65
monitoring 97, 110, 120
toll 57
Transfer Out of AUDIX 78
trunk-to-trunk 97, 120
volume
tracking 96
call attempt
invalid 96, 99
Call Detail Recording 16, 53, 112, 121
outgoing voice 116, 122
reviewing for abuse 95
call diverters 19
call flow through PBX system 38
Call Forward Off/On-Net 45
Call Forwarding 20, 111
call list 57
unrestricted 81
Call Management System
Measurements 98
security tips 82
call pager 81
scam 19
Call Prompting 56
call sell operations 14
Call Traffic Report 114, 119
Call Vectoring 42, 56
call volume increases 96
calling cards 15, 17, 18
CDR, see Call Detail Recording
Central Office restrictions 60
change remote-access command 105
change station command 111
Class of Restriction 41, 57
3-way calling 45
authorization code 43
barrier code 43
blocking access 57
Facility Access Trunk test option 71
maximum allowed 57
outward-restricted 52
Remote Access 52
Class of Service 45
CMS, see Call Management System
CO trunks 21
code
authorization 21, 38
barrier 21, 38, 46
command
change remote-access 105
change station 111
change system-parameters security 103
disable remote-access 105
enable remote-access 105
list bcms trunk 98
list call forwarding 111
list history 109
list measurements 97
list performance 97
monitor 95
monitor security-violations 99, 101
verify 111
Committee of the Alliance for Telecommunications . . . 9
con games 18, 19
COR-to-COR restrictions 44, 61
credit card calls 15, 17, 18

D

data channel 22
DCS, see Distributed Communication System
dial tone
accessing 17
ARS 58
authorization code 51
barrier code 47
Remote Access 38
transferring 17
digit conversion 62
direct dial access 55, 58
Direct Distance Dialing 13
Direct Inward Dialing 93
Direct Inward System Access 16, 17, 93
DISA, see Direct Inward System Access
disable remote-access command 105
disallowing outside calls 41, 78
Distributed Communication System 73, 97
Trunk Turnaround 73

E

employee
abuse 19, 24
education 24
enable remote-access command 105
Enhanced Automated Attendant 115, 121

Enhanced Call Transfer 76, 79
    coverage limitations. 76, 79
equipment rooms
    physical security 25
Escape to Attendant 76, 79

F

FAC, see Feature Access Code
Facility Restriction Level 42, 77
    attendant console. 55
    overriding 43
    providing individualized calling privileges 41
    suggested value 55
Facility Test Call 72
    access code 71
    denying 57
    disabling 71
FEAC, see Forced Entry of Account Code
Feature Access Code 17
Forced Entry of Account Code 61, 74
FRL, see Facility Restriction Level
Fully Restricted Service 41, 44
FX trunks 21

G

Generic 3 Management Application
    invalid login attempts 101
Generic 3 Management Terminal 96, 114, 119

H

hackers
    800 numbers 21
    random number generators 13, 21
holding time
    long 96, 97, 98, 120
    short 93, 95, 96, 97, 98, 120

I

individual and group-controlled restrictions 59
individualized calling privileges
    providing 41
intercept tone
    call routing 41
intercept treatment 69
Interexchange Carrier 18
internal abusers 19
international
    calls 65, 68
    operator 65

L

LEC, see Local Exchange Carrier
list bcms trunk command 98
list call forwarding command 111
list history command 109
list measurements command 97
list performance command 97
lobby
    telephones 69
Local Exchange Carrier 19
login
    invalid attempts 99
logins
    invalid attempts 100
looping. 15, 18

M

maintenance port
    target of abuse 16
Malicious Call Trace 110
Manager I 114
    reporting .96, 119
Measurement Selection
    ARS 97, 114, 120
measurements
    CMS 98
Message Delivery 80, 116, 122
modem
    flashing switch-hook 23
    protecting ports 23
monitor command 95
Monitor I 96, 114
monitor security-violations command. 99, 101

N

NETCON, see Network Control data channel
network access
    unauthorized 13
Network Control data channel 22
Network Corporate Security 28
night
    service 56
    shut-down procedure 59
North American Dialing Plan 68
Numbering Plan
    area 55

O

Observe Remotely feature 111
OTTOTT, see Outgoing Trunk to Outgoing Trunk Transfer

outcalling 80
  limiting 81
Outgoing Trunk to Outgoing Trunk Transfer
  disabling 73
Outward Restriction 44

P

Partitioned Group Number 53
passwords
  adjunct 28
  default 16
  programs to crack 13, 21
  protecting 24
PBX
  accessing 17
peg counts 96, 119
  high 96
Personal Identification Number 93
Personal Station Access (PSA) 63
PGN, see Partitioned Group Number
ports
  administration 100
  automated attendant 41
  maintenance 100
  Remote Access 99, 100
  security 22
  System Management 99
  voice 81

R

random number generators 13, 21
recall signaling 58
referral call
  SVN 99
Remote Access 13, 16, 17
  800 numbers 38
  Barrier Code Aging 109
  dialing in
    800 service trunks 21
    CO trunks 21
    FX trunks 21
  disabling 40
  invalid login attempts 101
  kill 105
  permanently disabling 50
  removing 40
  Status Report 101
  status report 101
  System 75 20
  System 85 20
  Violations Status Report 101
remote service observing 111
reports
  Authorization Code Violations Status 101
  call traffic 114, 119
  distributed 25
  G3-MT 96, 119
  Manager I 96, 119
  Remote Access status 101
  SAT 96, 119
  securing 25
  Security Violations 108
  Security Violations Measurement 99
  Security Violations Status 99
  sending to attendant 98
  SMDR 113
  traffic 121
  trunk group 114, 119
restrictions
  calling party and called party 44
  individual and group-controlled 59
  originating station 44
  originating trunk 44
routing
  patterns 97
  Time of Day 61, 99

S

SAT, see System Administrator Tool
screening
  6-digit 19
security risks
  port 22
Security Violation Notification feature 98
  referral call 99
Security Violations
  measurement report 99, 100
  report 108
  status report 99
Security Violations Summary Report 100
service observing 110
shoulder surfing 18
six-digit screening 19
social engineering 18
Station Message Detail Recording 16, 74, 93, 112
station restrictions 58
Station Security Code Violations Report 102
Station Security Violation Status Report 101
Station-to-Trunk Restrictions 55
SVN, see Security Violation Notification feature
switchhook flash
  administering 58
System 75
  detecting toll fraud 94
  security goals and tools 30, 84
System 85
  detecting toll fraud 94

security goals and tools 30, 84
System Administrator Tool 96, 114
reporting 96, 119
system console
physical security 25
system tone test call 71

T

TAC, see Trunk Access Code
telecommunications fraud
airports. 18
by employees 19
definition 13
effect 13, 15
employees 24
in lobby 58
telephone number
nonpublished 38
test call
facility 71
trunk 71
third party calls 28
tie trunk
disallowing outgoing calls 73
limiting access 74
restricting 60
tandem. 62, 73
Time of Day
plan 42
routing 61, 99
preventing after-hours calling 42
time slot test call 71
Time-Out to Attendant authorization code 68
Title 18 Section 1029. 14
Toll Analysis 57
toll fraud
contact list 127
internal. 95
Toll Restriction. 44
Tone Detector circuit pack 71
traffic
abnormal patterns 119
measurements 96
monitoring flow 97
reports 121
Transfer Out of AUDIX 80
disabling 81
transfers
limiting 77
Traveling Class Mark. 74
trunk
800 service. 21
administration 55
ARS 74
CO 21, 44
disabling direct access. 70
FX 21, 44
monitoring 95
outgoing 74
public network. 44
Remote Access 21
tie 44, 60
WATS 55, 60
Trunk Access Code. 17, 44, 62, 68, 73, 78, 111
obtaining outgoing trunk 55
Trunk Group Report 114, 119
trunk groups
CO 21
outgoing 57
Remote Access 21
trunk override 60
trunk test call. 71
Trunk Turnaround
Distributed Communication System. 73
Trunk Verification. 55
Trunk-to-Trunk Transfer
disallowing 72

U

UDP, see Uniform Dial Plan
Uniform Dial Plan. 44
United States Criminal Code 14
usage
monitoring 97

V

VDN, see Vector Directory Number
Vector Directory Number 56
authorization code. 51
COR 56
Verify button 111
voice mail 13, 17, 19, 23
detecting toll fraud. 112
security risks 23
Voice Session Record 115
voice mailboxes
passwords 24
unassigned 23, 27
voice messaging systems
automated attendant. 22
voice processing systems 23
voice session record 115, 121
voice terminal group
attendant-controlled 59

W

WCR, see World Class Routing
wild card characters 62
wiring closets
    physical security 25
World Class Routing 61
    restricting 61