Avaya Aura® Toll Fraud and Security Handbook

Release 6.3
555-025-600
Issue 3
May 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). 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 to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

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 can 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 Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.

- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. "Instance" means one unique copy of the Software. For example, if the end user customer or Business Partner would like to install two instances of the same type of Products, then two Products of that type must be ordered.

How to Get Help

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

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Product Safety Standards

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

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

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.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

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

For a Class B digital device or peripheral:

Note:

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

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

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

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.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

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 equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format

US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

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 should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

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. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

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	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
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
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment 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.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should 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 should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

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://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

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

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

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 (2004/108/EC) and Low Voltage Directive (2006/95/EC).

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://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

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。

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

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® Communication Manager
- Avaya Aura® 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 the features of certain products in relation to toll fraud security. This guide does not fully describe the capabilities of each feature.

Intended audience

Telecommunications managers, telephony administrators, and persons responsible for the security of 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 must consult with their local sales and services teams or

Authorized Avaya Business Partner for specific examples and configuration advice tailored for their locale.

Document changes since last issue

The following change has been made to this document since the last issue:

- Updated the route pattern range from 999 to 2000 in Blocking calls on page 71.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® Communication Manager Security Design, 03-601973	Describes the security-related information.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Implementation		
Deploying Avaya Aura® Communication Manager on System Platform, 03-603558	Describes the implementation instructions for Communication Manager.	Implementation Engineers, Support Personnel
Maintenance and Troubleshooting		
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers, 03-300431	Describes the commands for Communication Manager.	Implementation Engineers, Support Personnel
Administration		

Title	Description	Audience
Administering Avaya Aura® Communication Manager, 03-300509	Describes the procedures and screens for administering Communication Manager.	Implementation Engineers, Support Personnel
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation, 555-245-205	Describes the features that you can administer using Communication Manager.	Implementation Engineers, Support Personnel

Avaya Mentor videos

Avaya Mentor videos are available to provide technical content on how to install, configure, and troubleshoot Avaya products.

Videos are available on the Avaya support site, listed under the video document type, and on the Avaya-run channel on YouTube.

To find videos on the Avaya support site, select the product name, and check the *videos* checkbox to see a list of available videos.

Note:

Videos are not available for all products.

To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Understanding toll fraud security

Avaya 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 Avaya customers and to support law enforcement officials in apprehending and prosecuting the offenders.

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 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 customers 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 product and service literature, marketing information, and contractual documents address, wherever practical, the security features and limitations of Avaya products and the customer responsibility for preventing fraudulent use of Avaya products and services.
- Avaya sales and service people are highly knowledgeable and well informed. These personnel provide customers the latest information on how to do manage their systems securely and most effectively.
- Avaya trains its sales, installation and maintenance, and technical support people to focus customers on the known toll fraud risks. Avaya also describes them mechanisms that

reduce the risks and discusses the trade-off between enhanced security and diminished ease of use and flexibility. Avaya also ensures that customers understand their role in the decision-making process and their corresponding financial responsibility for fraudulent use of their telecommunications system.

- Avaya provides educational programs for internal and external customers to keep customers 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 customer 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 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 Partner of Choice for all customers and has clearly defined the Avaya mission in this end in a Statement of Direction issued in May, 1992. For more information, see the Avaya statement of direction on page 15. 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 Avaya roles and responsibilities on page 17.

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:

Note:

It is necessary to stress that the business owner, the owner or lessee of the Customer Premises Equipment (CPE), 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

- As a manufacturer: Avaya provides the customer with the technology, information resources (product documentation) to understand the capabilities of the technology, and configuration of the equipment when it is shipped from the factory.
- As a sales organization: Avaya informs the customer of potential toll fraud, how toll fraud happens, and what roles and responsibilities Avaya and the customer need to accept to work together in reducing the customer's potential for toll fraud.
- As a provisioning organization: Avaya assists 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.
- As a maintenance provider: Avaya ensures that no action taken by Avaya serves to introduce risk to the system of the customer. At the very least, Avaya must ensure that the customers are as secure after the assistance of Avaya as the customers 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

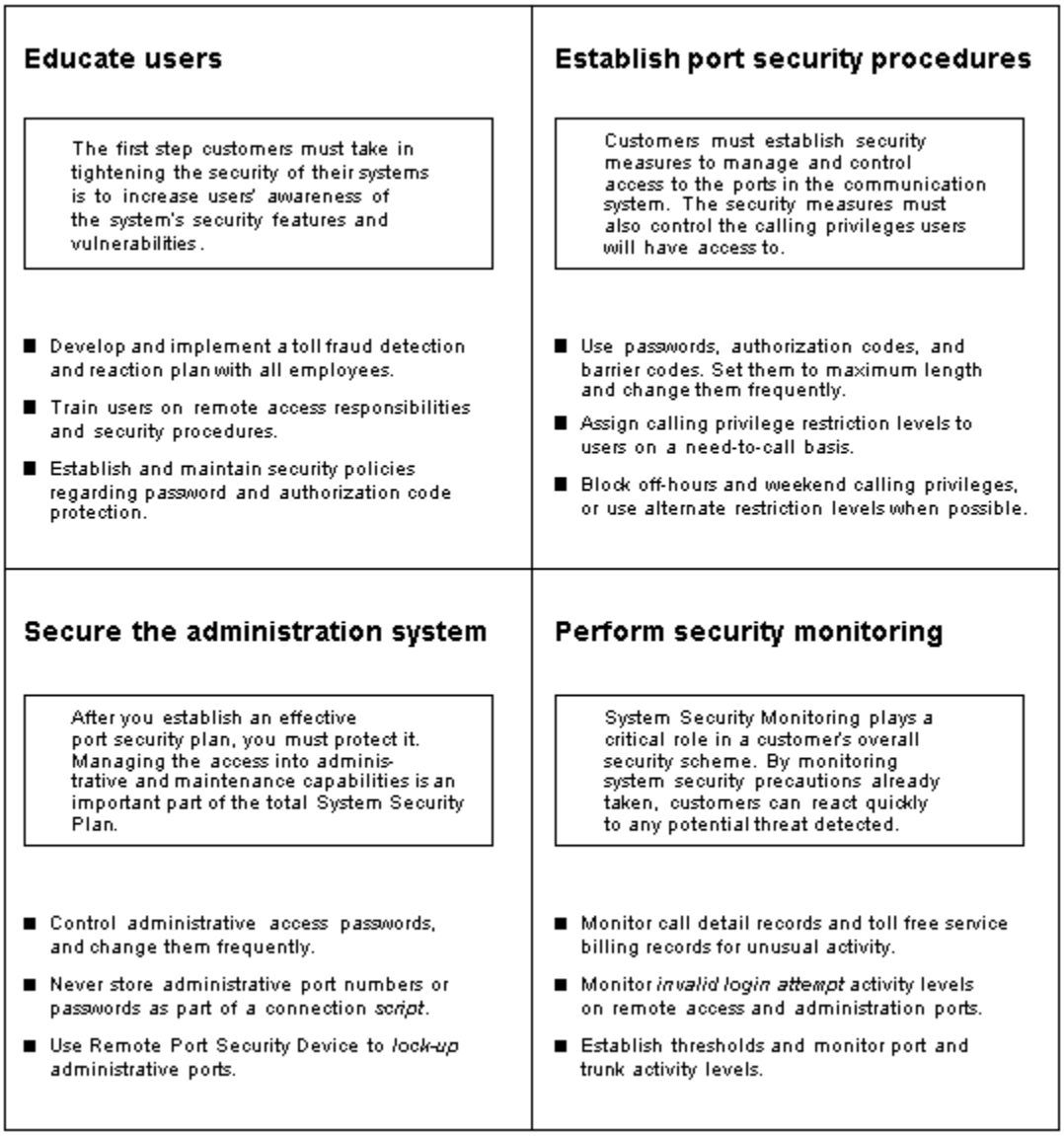

Figure 1: Toll Fraud action plan

.

Chapter 3: Toll fraud risk model

Overview

Telecommunications fraud is the unauthorized use of the telecommunications services of a company. 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. Sharp increases in reported incidents of attackers include criminals skilled in reprogramming computer systems and accessing telecommunications systems through remote administration or maintenance ports. These ports cannot be used to place telephone calls, but attackers can gain control over the setup of the system. Through these ports, attackers create security holes to permit unauthorized calling which is a serious form of electronic vandalism and other unwanted activity.

Information resources of a company are yet another target for modern criminals. Attackers can attempt to infiltrate voice mailboxes or eavesdrop on cellular telephone calls to obtain proprietary information about your products or your customers.

Hackers and phreakers

Hackers and phreakers or telephone freaks use personal computers, random number generators, and password-cracking programs to break into even the most sophisticated customer premises equipment-based system if the system is not 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. Attackers attempt to find the weakest link and break

it. Once attackers have compromised your system, attackers will use your system resources to break into another system. Attackers can also sell your information to an 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 telephone thief, who stands next to a pay telephone 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 telephones lines from the telephone company 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 they 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 stops everything and usually resurfaces at another apartment with another 30 telephones 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 depend on calling card numbers or other means to fraudulently use a customer premises equipment-based system. The major calling card vendors monitor calling card usage and shut down in a matter of minutes after detecting the fraud. However, call sell operators know that the traffic on most customer premises equipment-based systems is not monitored.

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

Drug dealers

Drug dealers want telephone 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 (PBXs) 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.

Loss to the companies

Cost of the telephone bill

No real numbers indicate 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 might 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 might 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 type of abuse is most dangerous because once inside your system, the attackers have control all the administrative commands. While in your system, the attackers can perform the following:

- Turn on Remote Access or Direct Inward System Access (DISA). On some communications systems, there 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 permit fraudulent calls. Then, at 3:00 a.m., the attackers reprogram the system back to its original configuration.
- 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. Managers cannot see records of the calls because CDR was turned off by the attackers. The administrator might notice the absence of CDR records for evening, night, and weekend calls made by employees.

Voice mail: Voice mail fraud is of two types. 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, the thieves 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 control the mailbox or simply access the information stored within the mailbox. In the first situation, an attacker dials either 9 or a TAC that permits 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. The attacker then gains access to proprietary corporate information.

Automated attendant: Many companies use auto attendants 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 telephone number and the call is completed. The PBX owner pays for the call. The scenario is the same with a voice mail system.

Remote access or DISA: Using remote access or direct inward system access (DISA), remote users can gain access to a PBX and place long distance calls as if users are 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 permits 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 stops responding 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, they can call back repeatedly in an attempt to crack the code.

Telephone network-based activities

- Shoulder surfing: Network attackers use video cameras in airports to take pictures of people using their calling cards. Attackers can also use an audio tape recorder to capture calling card numbers as they are spoken to an operator. This technique of capturing calling card numbers is known as shoulder surfing.
- Social engineering: Social engineering is a con game attackers frequently use. Con game is sometimes referred to as operator deceit. The success of operator deceit 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 the operators 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. The attackers 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 might 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 telephone bills, corporate telephone 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 features.
- Looping: Looping is a method that call sell operators use to circumvent restrictions that IXCs (Interexchange carriers) put in the networks to control calling card fraud. All carriers block calling card calls bound for the 809 area code (to the Dominican Republic) that originate in New York, NY. This is because the Dominican Republic is a common destination for stolen telephone 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, the attackers will revert to looping. The attackers 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, 1 800 COLLECT, 1 800 CALLATT, and 1 800 GETINFO. The attackers can also dial 950 carrier access numbers. Lastly, the attackers can dial various 101xxxx carrier access codes. In any case, the attackers can use the PBX to place a fraudulent call. If the PBX is not in New York, NY, the attackers can use the calling card. Use of the 101xxxx codes could permit 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. Smaller businesses normally use a call diverter to forward calls to an answering service after hours. When attackers find a number they suspect is using a call diverter, the attackers 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 (LECs) have run out of numbers in the 976 prefix, so they are using other prefixes that work the same as 976. That is, the calling party gets charged for the call at a rate set by the owner of the number. The fee charged for calling these numbers can range upwards of $250 per call. As already stated, the fee is set by the owner of the number. Unscrupulous people who own these numbers call around the country inserting these numbers into pagers to get the users to return the call so that they can collect the fee. The 976-look-alike numbers are constantly changing and expanding. Consult your LEC for a list of 976-look-alike numbers in your exchange. This same scam 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 telephone 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: Not all toll fraud is generated from outsiders. Often, toll fraud is traced to internal employees who sell the information or abuse the system for personal 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 permitted, unscrupulous employees can take advantage of it. They forward the telephone 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 telephone, and the company foots the bill for the call.

General Toll Fraud Security risks

The following illustration depicts a call transfer through the PBX.

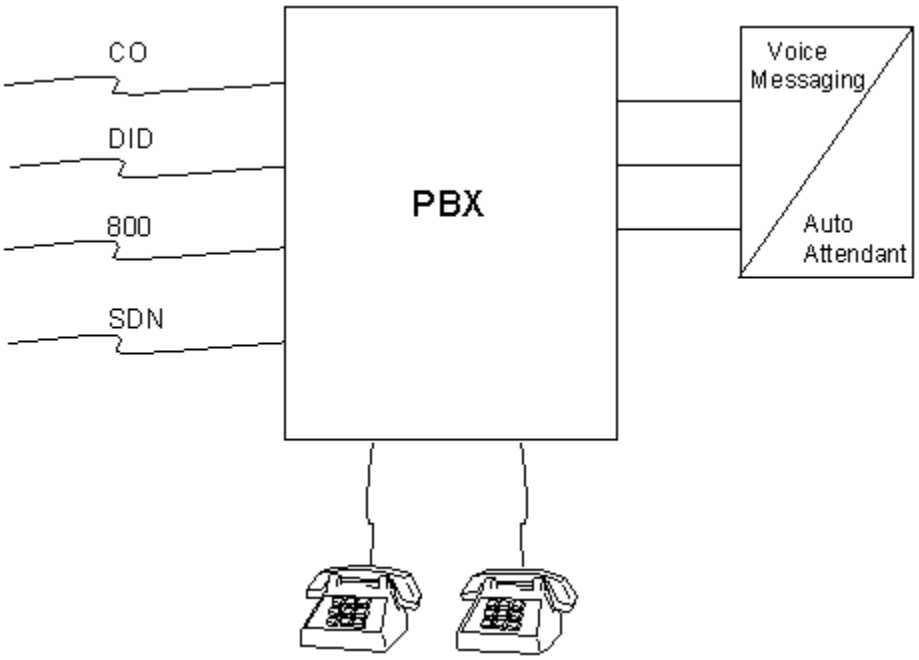

Figure 2: Call transfer through the PBX

Remote access

With remote access or DISA, callers can call 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 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, might be required to dial a barrier code, depending on the system. If a valid barrier code is dialed, the user again hears a dial tone, and the user can place calls in the same way 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 must decipher up to 14 digits to gain access to the feature, which includes a 7-digit barrier.

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, you must protect all switches in the network.

Unprotected remote access numbers are favorite targets of attackers. After being connected to the system through the Remote Access feature, a attacker can 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 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 the automated attendants 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 might also attempt to enter a portion of the toll number to verify whether the automated attendant system passes the digits directly to the PBX and then enter the remaining digits after the transfer has been made to an outside line. 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. For more information on securing automated attendant systems, see *Considerations for Communication Manager and Messaging in Automated Attendant.*

Other port security risks

Many of the security risks from voice mail, remote access, and automated attendant arise from permitting incoming callers to access outside facilities. However, you must also deny other endpoints within your system to incoming callers. You can dial many of these endpoints as internal calls within the system and use voice mail, Auto Attendant, or Remote Access to reach the endpoints. Other examples of adjunct access you must manage 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 Network Control (NETCON) data channels provide internal access to the system management capabilities of the system. You can reach NETCON on a call transfer from a Voice Mail System if not protected by appropriate restrictions. You must place any features or endpoints that incoming callers can dial but must be denied to incoming callers in restriction groups. Incoming callers cannot each restriction groups from an 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. For more information, see Recall signaling - switchhook flash on page 63.

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 permit 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. The attackers then attempt to discover a user ID and password using which the attackers can 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 that are similar to an electronic answering machine. Callers can leave messages for employees or subscribers with assigned voice mailboxes. Subscribers can play, forward, save, repeat, and delete the messages in their mailboxes. In many voice messaging systems, callers can transfer out of voice mailboxes and back into the PBX system.

After connecting to the voice messaging system, the attackers try to enter digits that connects the attackers 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 know how to gain access to an outside facility. The attackers only know the right combination of digits.

Sometimes attackers are not even looking for an outside facility. The attackers enter a voice messaging system to find unassigned voice mailboxes. After being successful, the attackers assign the mailboxes to themselves, relatives, and friends, and use the mailboxes to exchange toll-free messages. Attackers can even use cellular phones to break into voice mailboxes. In addition, with unauthorized access to voice messaging systems, attackers gain access to the switch and change administration data.

Toll fraud is possible when an incoming caller is able to make an outbound connection back to the PSTN. Once attackers obtain a mechanism for reaching an outside line, attackers can make calls anywhere in the world. Toll fraud through messaging system presents the following threats:

- 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 servers.
  - Disclosure or discovery of IP network dial-up or VPN remote access mechanism or IP-based attacks that originate from inside your network.
- Unauthorized call transfer: An intruder uses the transfer-to-extension feature by transferring the first few digits of a trunk access code or other mechanism that provides the caller access to an outside line.
- Unauthorized mailbox use: Unauthorized use of mailbox might involve toll fraud or a simple theft of messaging services. An intruder discovers how to use a particular mailbox by one of the following methods:
  - 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

Information for users to prevent toll fraud

Everyone who uses the telephone system is responsible for system security. Users and attendants must be able to recognize potential attacker activity and know how to reach to such activity. Informed people are more likely to cooperate with security measures that often make the system less flexible and more difficult to use.

- Never program passwords or authorization codes onto auto dial buttons. Display telephones reveal the programmed numbers and internal abusers can use the auto dial buttons to originate unauthorized calls.
- Do not write down passwords. If you must write a password down, keep the password in a secure place and never discard the password while the password is active.
- Attendants must inform their system manager if the attendants receive a series of calls with silence on the other end or where the caller hangs up without speaking.
- 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, hook-on, and confirm the identity of the caller.
- Never distribute the office telephone directory to anyone outside the company. Be careful when discarding the directory.
- Never accept collect telephone calls.
- Never discuss your telephone numbering plan with anyone outside the company.

Physical security considerations

You must always limit access to the system console and perform the following in the interest of security:

- 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 that the reports 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 some steps can be taken 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 permit 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 to prevent the system from 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 telephone 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.

Suggestions to prevent telephone fraud

- Protect system administration access.

  Set unique passwords for each system administration or maintenance account and 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 and egress ports.

- Deny unauthorized users direct inward system access(remote access).

  Deactivate or disable Remote Access features when not in use. Make it compulsory to use barrier codes and authorization codes if you are using remote access and set the codes to the maximum length. Change the codes frequently.

- Install protection measures on systems that prompt callers to input digits.

  Prevent callers from dialing unintended digit combinations at prompts. Restrict auto attendants and call vectors from gaining access to dial tone.

- Use system software to intelligently control call routing.

  Create ARS or AAR patterns to control how each call must 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.

Train users on how to protect themselves from inadvertent compromises to the system security. For example, how to safely use calling cards and how to secure voice mailbox passwords.

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

  Always provision a password for user accounts and force a password change on first use. You can add 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.

Suggestions for voice messaging security

- Restrict transfers back to the host PBX or use enhances call transfer, for example, AUDIX® or Communication Manager Messaging only. Do not permit transfers, or permit transfers only to subscribers.
- When you enable password protection in voice mailboxes, you must use the maximum length of password where feasible.
- Deactivate unassigned voice mailboxes. When an employee leaves the company, remove the voice mailbox.
- Do not create a voice mailbox before a voice mailbox is needed.
- Establish your password as soon as your voice mail system extension is assigned to ensure that only you have access to your mailbox. Anyone who enters your extension number and hash (#) does not gain access to your mailbox. The fact that a hash (#) indicates the lack of a password is well-known by telephone attackers.
- Do not insert a greeting that states that third-party billed calls are accepted.
- Never use obvious or trivial passwords, such as your telephone 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 can find out default passwords.
- Lock out consecutive unsuccessful attempts to enter a voice mailbox.
- Do not write down, store, or share passwords. If you must write down your password, keep the password in a secure place and never discard the password while in use.
- 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. The dial tone enables the caller to place another call as if the call is being placed from your company.
- Contact your voice messaging system supplier for additional measures you can take to prevent unauthorized users from transferring through voice mail to outgoing trunks.

Chapter 4: Product policy controls

Avaya Aura® 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	Suggestions to achieve the goal
Protect remote access feature	Limit access to authorized users.	Barrier codes	• Set Barrier codes to maximum length and administer Barrier Code Aging. For information see, Barrier codes on page 50. • Set class or restriction (COR) and Class of Service (COS). For information, see EC500 Security Features on page 70. • Restrict the number of users who access the remote dial feature. For information, see Restricting who can use remote dial access and track its usage on page 56 • Set up remote access. For informations, see Setting up remote access on page 58. • Suppress remote access dial tone. For information, see Suppressing remote access dial tone on page 78.
		Authorization codes	• Configure remote access authorization codes. For information, see Configuring Authorization codes to

Security goal	Method	Security feature	Suggestions to achieve the goal
			maximize the system security on page 56. • Set Authorization codes to maximum length. For information, see Authorization codes on page 55. • Set Facilitation Restriction Level (FRL) to COR. • Suppress remote access dial tone. For information, see Suppressing remote access dial tone on page 78.
	Disable or remove remote access feature if not needed.	Disable or remove remote access.	Permanently disable remote access. For information see, Disabling or removing the remote access feature on page 43.
	Use VDNs to route calls.	Call vectoring	• Administer call vectoring. • Use CORs to restrict calling privileges of VDNs. For information, see Configuring COR and VDN to prohibit outgoing access on page 62. • Protect vectors that contain call prompting. For information, see Protect vectors that contain call prompting on page 61.
	Limit times when remote access is available.	Night service	Administer night service. For information, see Remote access with night service on page 61.
Prevent unauthorized outgoing calls.	Limit calling area.	AAR and ARS analysis	• Set Facility Restriction Levels. For information, see Facility restriction levels on page 44. • Set Class of Restriction. For information, see Class of restriction on page 47. • Restricting calls to specified area codes. For information, see Restricting calls to specified area codes on page 74. • Permit calling to specified numbers. For information, Permitting calls to specified numbers on page 75.

Security goal	Method	Security feature	Suggestions to achieve the goal
		Digit conversion	Administer digit conversion. For information, see Digit conversion on page 68.
		Toll analysis	Identify toll areas that must be restricted. For information, see Toll analysis on page 62.
		Facility Restriction Levels (FRLs)	Limit access to AAR and ARS route patterns by setting FRL to lowest possible value. For information, see Facility restriction levels on page 44.
	Restrict the access to make outbound calls.	Attendant-controlled voice terminals	• Place telephones in an attendant-controlled group. For information, see Attendant-controlled voice terminals on page 64. • Use attendant control of trunk group access. For information, see Using attendant control of specific extensions on page 75.
		Authorization code time-out	Select authorization code time-out to attendant. For information, see Selecting authorization code time-out to attendant on page 74.
		Recall signaling	Administer the switchhook flash field to n. For information, see Recall signaling - switchhook flash on page 63.
	Screening calls	Central office restrictions	For information, see Central office restrictions on page 64.
		Carrier-based restrictions	For information, see Carrier-based restrictions on page 65.
	Restricting terminals	Restrictions — individual and group-controlled	• Activate and deactivate individual or group based terminals. For information, see Individual and group-controlled restrictions on page 64. • Use terminal translation initialization.
	Limit outgoing calls.	Facility Restriction Levels (FRLs)	• Restrict tie trunk usage. For information, see Limiting access to tie trunks on page 81. • Deny access to AAR and ARS.

Security goal	Method	Security feature	Suggestions to achieve the goal
		Authorization codes	• Set Authorization codes to maximum length. For information, see Authorization codes on page 55. • Set Facilitation Restriction Level (FRL) to COR.
		Access to trunk	• Disable direct access to trunk. For information, see Disabling direct access to trunks on page 76. • Monitor trunk. For information, see Configuring Forced Entry of Account Code on page 82.
		AAR or ARS restrictions	Restrict AAR or ARS from unauthorized use. For information, see Using AAR and ARS routing restrictions on page 67.
Prevent unauthorized outgoing calls (continued)	Limit calling permissions.	Class of Service (COS)	Set COS restrictions. For information, see Class of service on page 49.
		Class of Restriction (COR)	• Set Facility Restriction Levels. • Set calling party restrictions or outward restrictions. • Set COR to COR restrictions. For information, see COR-to-COR restrictions or calling permission on page 48.
	Require account code before calls.	Forced entry of account code	• Set account code length. For information, see Forced entry of account code on page 66. • Configure forced entry of account code. For information, see Configuring Forced Entry of Account Code on page 82.
	Create time-dependant limits on access to route patterns.	Alternate FRL	Set the lowest possible value for FRLs. For information, see Preventing after-hours calling using time of day routing or alternate facility restriction levels on page 46.
	Suppress dial tone after AAR and ARS	Suppress dial tone	Turn off AAR and ARS dial tone. For information, see ARS dial tone on page 63.

Security goal	Method	Security feature	Suggestions to achieve the goal
	feature access code.		
	Screen all AAR and ARS calls.	AAR and ARS	Administer all capabilities. For information, see AAR and ARS analysis on page 63.
	Block international calls.	ARS Digit Analysis	Deny permission to international numbers. For information, see EC500 Security Features on page 70.
			• Block international calls. For information, see EC500 Security Features on page 70. • Blocking Calls. For information, see Blocking calls on page 71.
	Limit international calls.	ARS Digit Analysis	• Deny permission to international numbers. • Limit international calling.
	Disallow or disable Trunk-to-trunk transfer.	Outgoing trunk to outgoing trunk transfer (OTTOTT) feature	Disable OTTOTT. For information, see Restricting trunk-to-trunk transfer on page 79 and Outgoing trunk to outgoing trunk transfer on page 79.
		Trunk-to-trunk transfer	Restrict trunk-to-trunk transfer. For information, see Restricting trunk-to-trunk transfer on page 79.
		Limiting access to tie trunks	Assign COR-to-COR restrictions. For information, see Limiting access to tie trunks on page 81.
	Set Station security codes (SSC).	Station security codes	SSC input. For information, see Station Security Codes on page 68.
	Carefully assign feature access codes.	Feature access codes	Feature access code administration. For information, see Feature access code administration on page 60.
	Enable EC500 security functionality.	Calling number verification	Restrict incoming EC500 calls to calling numbers that are Network Provided or User Provided Verified and Passed. For information, see EC500 Security Features on page 70.

Security goal	Method	Security feature	Suggestions to achieve the goal
		Protect remote EC500 features with Station Security Codes.	Assign Station Security Codes. For information, see Station Security Codes on page 68
-	-	Idle Appearance Select Feature Named Extension (FNE)	Do not enable Idle Appearance. Select FNE. For information, see EC500 Security Features on page 70.
-	Restrict trunk access codes.	Trunk Access Codes	Limit direct dial and facility test access to Trunk Access Codes. For information, see Trunk administration on page 61.
Prevent exit from voice messaging system	Disable distinctive audible alert for adjunct equipment.	Disable distinctive audible alert (stutter tone)	Administer analog station settings to disable distinctive audible alert. For information, see Disabling distinctive audible alert for adjunct equipment on page 83.
	Remove or change data origination code.	Data origination	Remove or change data origination code. For information, see Disabling distinctive audible alert for adjunct equipment on page 83
	Prevent messaging system transfer to dial tone (supported messaging systems only).	Station restrictions	Turn off transfer feature. For information, see Station restrictions on page 63.
		Enhanced transfer	Set Transfer Type=Enhanced. For information, see Facility restriction levels on page 44.
		Basic transfer	Set Transfer Restriction= Subscribers. For information, see Enhanced call transfer on page 83.
Prevent unauthorized calling from automated attendant service	Limit exit to outgoing calls.	Enhanced call transfer	For information, see Facility restriction levels on page 44.
		Facility Restriction Levels (FRLs)	Set the lowest possible value. For information, see Facility restriction levels on page 44.
		Station-to-trunk restrictions	For information, see Station-to-trunk restrictions on page 60.

Security goal	Method	Security feature	Suggestions to achieve the goal
		Class of restriction	For information, see Class of restriction on page 47.
		Class of service	For information, see Class of service on page 49.
	Restrict outgoing toll calls.	Toll Analysis	Identify toll areas to be restricted. For information, see Toll analysis on page 62.

Communication Manager security features

Remote Access feature

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 disabling time and date of the remote access, and barrier codes.

Security suggestions for the Remote Access feature

- Evaluate the necessity for remote access. If this feature is not vital to your organization, then you must deactivate this feature. If you need the feature, use as many of the security measures presented in this chapter as you can.
- Use an unpublished telephone number for this feature. Professional attackers scan telephone directories for local numbers and toll-free numbers used for remote access. Keep your remote access number out of the telephone book to prevent the number from getting into the wrong hands. You must not administer a night service destination to remote access on any published number.
- Keep an authorized user list and reevaluate the list 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 permit calling in from San Francisco.

- Specify maximum length barrier codes and authorization codes. You can specify codes up to 14 digits for users to again access to the feature. The 14-digit code includes a 7-digit barrier code and a 4 to 13 digit authorization code.
- 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:

1. The system switches endpoint signals switch to start the call.
   - If the originating endpoint is a station, the request for service is an off-hook call.
   - If the originating endpoint is a trunk, the request for service is a seizure signal. For example, wink start, off-hook, ground start.
2. The system switches signals endpoint to start dialing.
   - If the endpoint is a station, the system plays a dial tone for the caller.
   - If the endpoint is a trunk, a start dial signal (wink dial tone, etc.) is sent to the originating end.
3. The digit string is dialed.
4. The first digit dialed is compared to dial plan record.
5. The type of call is identified depending on the dialed digit.
6. The calls can be transferred to an extension number, trunk access code, attendant, or feature access code.
7. 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. The system has defined a 4-digit extension that begins with the digit two 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 to see if the COR of the originator is permitted 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 system completes the call. If the COR of the originator is set to `n` for the COR of the destination, the caller hears the intercept tone.

Example 3: User dials 9. The system has defined digit nine as feature access code for ARS. More digits will follow. As the digits are dialed, the system checks the digits with the ARS analysis table until a unique match is found. When a singular match is found, the system checks to see if a route pattern is identified. If a route pattern is unidentified, 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 checks for an available member. If a member is unavailable, the next choice in the pattern checks 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.

Logoff screen notification

The logoff screen displays a notification 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.

You must always use the acknowledgment option for systems utilizing both the Remote Access and Facility Test Call features or systems that require notification if Facility Test Call is linked to a hacking activity. The Facility Test Call feature is for notification if the feature is inadvertently left enabled.

Disabling or removing the Remote Access feature

About this task

You must permanently disable the Remote Access feature if you do not need the feature. Permanent removal protects against unauthorized usage even if criminals break into the maintenance port. After you disable this feature, only Avaya maintenance personnel can reactivate the feature.

Note:

The Remote Access feature of Communication Manager can be permanently removed.

You can disable or remove the remote access feature using the following steps:

Procedure

1. On the Communication Manager SAT screen, type `change remote-access`.

The system displays the Remote Access screen.

2. Set the **Remote Access Extension** field to blank.
3. Enter `y` in the **Permanently Disable** field.
4. Save the changes.

   The changes take effect only when you log out and re-login in to Communication Manager.

   On the Communication Manager SAT screen, type `display remote-access` to verify the changes. If you get an error message or you cannot display the screen, then the feature is disabled. 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 and ARS calls. FRLs are used in combination with calling permissions and routing patterns and preferences to determine where calls can be made. FRLs range from 0 to 7, with each number representing a different level of restriction (or no restrictions at all).

The AAR and ARS feature uses FRL to determine call access to an outgoing trunk group. Outgoing call routing is determined by a comparison of the FRLs in the AAR and 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 the station an FRL value of 0. Ensure that the FRLs on the trunk group preferences in the routing patterns are 1 or higher.

For example, when automated attendant ports are assigned to a COR with an FRL of 0, outside calls are restricted. 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 not configured to make outside calls cannot use AAR and ARS calls. Therefore, the FRL level does not matter since FRLs are unchecked. 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 are restricted.

Fully restricted 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.

The system redirects calls from the public network to a station with fully restricted service to intercept treatment or to the attendant. If the call is redirected to the attendant, the attendant display is FULL to indicate that the call is being redirected because of fully restricted service.

When the call is redirected to the attendant, you can perform the following actions:

- The attendant connected with a CO might 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.

Individualized calling privileges using facility restriction levels

The system uses FRLs to permit or deny calls when AAR and ARS route patterns are accessed. If the call is redirected to the attendant, the attendant display is FULL to indicate that the call is being redirected because of fully restricted service. A COR assigned an FRL of 7 is permitted 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. For a list of suggested FRL values, see Suggested values for FRLs on page 59.

Note:

If dial access is permitted 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 FRLs.

Assigning facility restriction levels

Procedure

1. On the FRL screen, type `change cor`.
   The system displays the Class of Restriction screen.
2. In the **FRL** field, type an FRL number from 0 through 7.
3. On the FRL screen, type `change route-pattern`.
   The system displays the Route Pattern screen.

4. On the Route Pattern screen, assign the appropriate FRL to the route pattern defined by AAR and ARS.

Preventing after-hours calling using time of day routing or alternate facility restriction levels

About this task

You can regulate the days of the week and specify the time of making outgoing calls. Depending on the time of day and day of the week, you can block calls 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 office hours, block the toll calls after office hours.

You can also use call vectoring to route to different trunk groups, for example, after hours you might want only 50 trunks available instead of 200.

To regulate the after-hours calling:

Procedure

1. On ARS analysis table screen, enter `change ars analysis partition x` to define an ARS analysis table to be used for after hours calling.
2. Enter `change time-of-day y` to select and define a time of day plan.
3. Administer the number of times to offer remote access and the times you do not.
4. Enter `change cor xx` to assign the time of day plan to the COR for barrier codes or authorization codes.

Facility restriction levels for unauthorized outgoing calls

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

Note:

ARS and ARS route patterns must never be assigned an FRL of 0 (zero).

The FRL is used by AAR and ARS to determine call access to an outgoing trunk group. Outgoing call routing is determined by a comparison of the FRLs in the AAR and 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. You do not need to modify AAR and ARS pattern preference FRLs. You can set FRLs to a lower value outside normal business hours to place more restrictions on after-hours calling.

Note:

Typically, the associated button is assigned to the attendant console to activate alternate FRLs.

Class of restriction

Class of Restriction (COR) places calling permissions and restrictions on both the calling party and the called extension. You can define a maximum of 996 CORs in the system.

For complete details and full descriptions of COR features and configuration, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Each COR might be assigned a unique name through the Class of Restriction screen. CORs are assigned to trunks, stations, authorization codes, attendant consoles (as a group), remote access barrier codes, and loudspeaker paging access zones. With CORs, you can provide or prevent specific types of calls or calls to trunks and stations with other specified CORs.

You can use the COR calling permissions (COR-to-COR restrictions) that set calling permissions on the COR to restrict stations to access trunks, and to restrict trunk groups to access other trunk groups. The COR also assigns FRLs that AAR and ARS use for 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 unrestricted and the vector contains a collect digit step, the caller can dial 9 or a TAC to route the call out of the system.

To maximize system security, you can:

- 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 FRLs.
- 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 value ensures that the ability to place calls that access public network facilities is assigned only when appropriate.

You can impose the following restrictions on the originating station or trunk:

- Outward Restricted: Disables public network calls through AAR and ARS or TACs. Calls can be placed to internal stations, to tie trunks via TACs, and off-switch via the Uniform Dial Plan (UDP).

  Note:

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

- Toll Restriction: Disables 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 and 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 vulnerability to toll fraud.

- Fully Restricted: Disables outgoing calls, including dial access to trunks. Incoming calls through public network trunks are restricted.

COR-to-COR restrictions or calling permission

If you cannot block dial access on an outgoing or two-way trunk, then you can use COR-to-COR restrictions to prevent direct access to the trunk groups.

Additional COR options related to toll fraud prevention

- APLT: Callers can dial public network numbers from the EPSCS private network.
- FRL: Users can gain access to AAR and ARS routes.
- CDR Account Code: You must enter an account code before the system processes an AAR and ARS call or completes a TAC call to a toll destination.

Note:

Account code entries are not validated.

Restriction override in a 3-way COR check

With the Restriction Override feature, you can determine whether the system makes a 3-way COR check on conference and transfer calls.

The default value of the **Restriction Override** field on the COR screen is none for all CORs. The default value helps to ensure that the feature is assigned only when appropriate.

If the **Restriction Override** field is set to all, the system checks only the controlling party COR with the CORs of all other parties on the conference and transfer call for station-controlled transfers and conferences. The check is not for parties on the conference and transfer call for attendant-controlled conferences and attendant-extended calls.

If the **Restriction Override** field is set to none, the system checks the COR of the new party against the CORs of all other parties on attendant extended calls and attendant-controlled conferences, as well as on all station-controlled conferences and transfers.

Class of service

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. Assign the following COS-configurable features only to users with a legitimate need for the associated feature functionality: The following COS options are related to toll fraud prevention.

- Call Forward Off/On-Net: A user can forward the call outside the switch (Off-Net), or inside, and outside the switch to non-toll locations (Off/On-Net). A default setting 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 the 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 value for both fields is n.
- COS controls the availability of certain features for a given extension. COR and COS do not overlap in the access or restrictions they control.
- Using Call Forwarding Enhanced in Communication Manager 4.0 and later, you can forward incoming calls to different destinations depending on whether the incoming calls are from internal or external sources. The default value for this field is n.

Barrier codes

To understand how barrier codes and authorization codes provide added security for remote access calls, see the flowchart in the figure on page 51

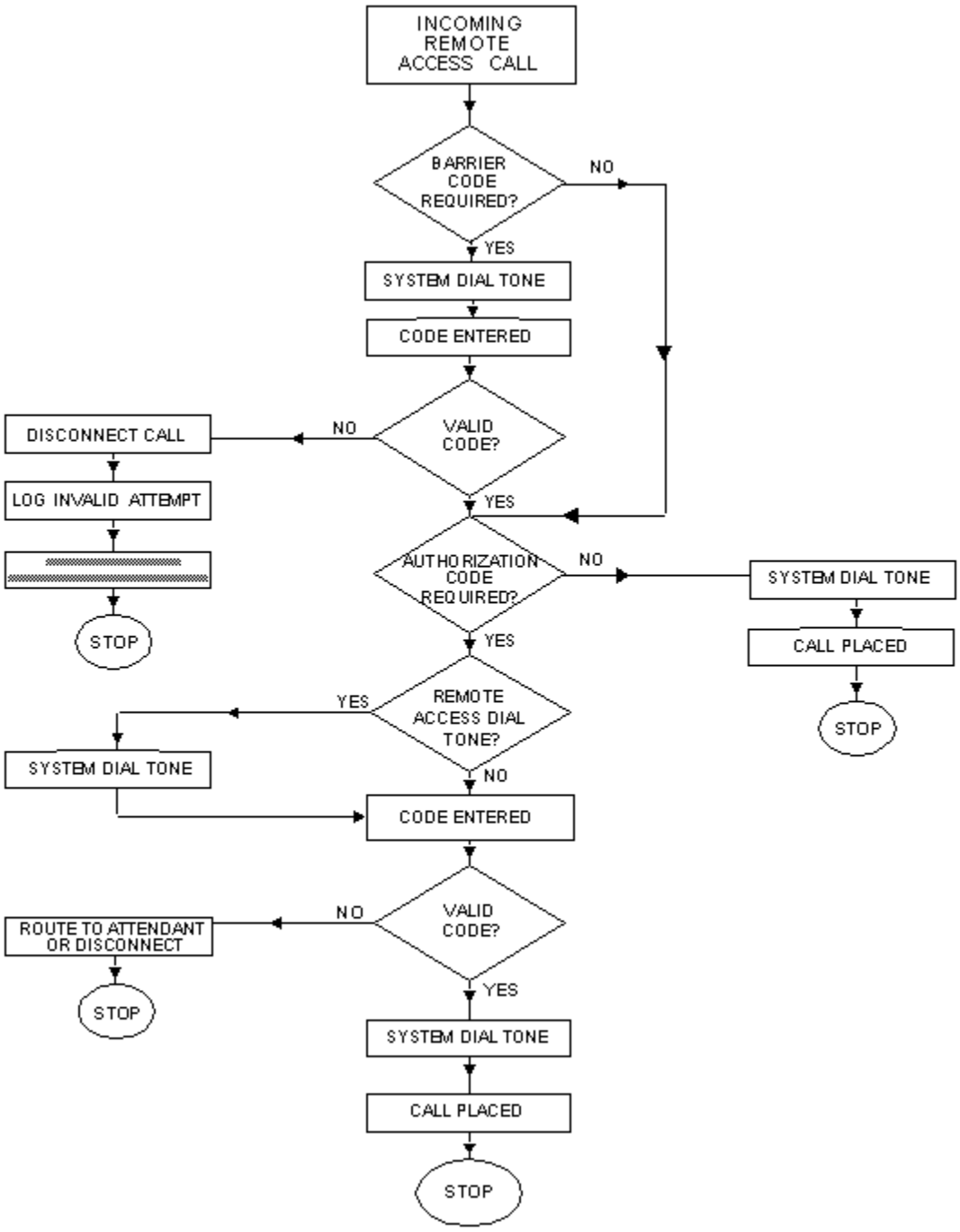

Figure 3: Remote access call path

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. To gain access to the system, the caller must enter a valid barrier code.

Note:

You can make the entry of an authorization code compulsory after the barrier code prior to callers receiving system dial tone for placing calls.

Barrier codes can be up to seven digits long. You can use all seven digits for maximum security. You can assign each barrier code a different Class of Restriction (COR) and Class of Service (COS) to identify the calling privileges available to the user who enters the code. For remote access calls, dialing a barrier code overrides the COR administered for the incoming facility. If no barrier code is required, the system uses the default COR on the trunk group.

Note:

For the COS assigned to a barrier code, the console permission field must be 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 the lifespan of the barrier code and automatically retire barrier code at the end of its usefulness, or to specify the number of times the barrier code can be used before the code 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 or access limits on page 124.

Remote Access Notification provides automatic reporting when remote access is in use.

Administering the Barrier Code Aging feature

Procedure

1. On the SAT screen, type the **`change remote-access`** command.

   The system displays the Remote Access screen.

2. On the Remote Access screen, enter the required information in the fields.

   For a description of the fields, see the *Remote Access field descriptions* section.

3. In the **Remote Access Extension** field, type 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 value of this field is blank.

4. In the **Authorization Code Required** field, enter `y` if Remote Access users must dial an authorization code to gain access to the remote access facilities of the system.

   The default for this field is n.

5. In the **Remote Access Dial Tone** field, enter `y` in this field if remote access dial tone is required as a prompt to the user.

This field is visible only if the **Authorization Code Required** field has been set to `yes`.

6. In the **Barrier Code** field, assign a barrier code that conforms to the number entered in the **Barrier Code Length** field.

   The length of the codes must be between 4 digits to 13 digits. The code can be any combination of the digits 0 through 9.

7. In the **Class of Restriction (COR)** field, enter the COR (0 through 995) associated with the barrier code that defines the call restriction features.

   The default value for this field is 1.

8. In the **TN** field, enter the partition number for tenant partitioning.

   The default value for this field is 1.

9. In the **Class of Service (COS)** field, 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.

10. In the **Expiration Date** field, 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.

11. In the **No. of Calls** field, enter the value for the number of remote access calls that you can place using the associated barrier code.

    The default is 1.

12. In the **Permanently Disable** field, enter `y` to permanently disable the Remote Access feature.

13. In the **Disable following a Security Violation?** field, enter `y` to disable the Remote Access feature following a remote access security violation.

Remote Access field descriptions

Name	Description
Remote Access Extension	Use the remote access extension like a DID extension. You can assign only one DID extension as the remote access extension. Calls to that number are treated in the same way 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 incoming destination field of the trunk group.

Name	Description
Authorization Code Required	Use of an authorization code in conjunction with barrier codes increases the security of the Remote Access feature.
Remote Access Dial Tone	For maximum security, do not use the authorization code dial tone.
Barrier Code	If the **Barrier Code Length** field is blank, the first barrier code field must be specified as none. Duplicate entries are not permitted. The system default for this field is blank. Assign a 13-digit number in this field for maximum security.
Class of Restriction (COR)	For maximum security, assign the most restrictive COR that will define only the level of service required.
TN	The default value for this field is 1.
Class of Service (COS)	Assigning the most restrictive COS that will define only the level of service required, provides the maximum security.
Expiration 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 administrator can modify the expiration date to extend the time interval if required.
No. of Calls	Valid entries are 1 to 9999, or blank. You can use the **Expiration Date** field and **No. of Calls** field independently. For maximum security, use the two fields 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 might indicate improper use.

Name	Description
Permanently Disable	Upon entering y to permanently disable the Remote Access feature, the Remote Access screen will no longer be accessible.
Disable following a Security Violation?	The system administrator can re-enable Remote Access with the **enable remote-access** command.

Authorization codes

Authorization codes protect outgoing trunks if an unauthorized caller gains entry into the Remote Access feature. Authorization codes also override originating FRLs to provide access to restricted AAR and ARS facilities. You can record the codes on CDR and CAS to check against abuse. To display all administered authorization codes, use the **list** command.

Note:

The number of digits, 4 to 13, in the authorization code remains fixed in all established systems unless you remove and reenter all codes. All authorization codes used in the system must be the same length. If the number of digits is increased, the system adds trailing zeros. Customers must establish new full-length random codes and must not decrease the length of the codes.

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. For maximum security, use all 13 digits.

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 calls but permitted other local ARS calls, then the authorization code COR must have an appropriately low FRL.

Note:

The PBX call detail recording feature (CDR) also records authorization codes. The individual assigned the authorization code must perform call verification. Ensure proper security to protect any printed copies of 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 and ARS calls for outgoing calls, For more information, see Facility restriction levels on

page 44. Up to 90,000 authorization codes can be issued to the Communication Manager users. You must keep the number of authorized users to a minimum.

Configuring Authorization codes to maximize the system security

Procedure

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 permitted 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 use 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 unused, 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

About this task

For maximum security, give barrier codes and authorization codes only to the people who need to use the feature.

Procedure

1. On barrier codes and authorization codes page, enter `change system-parameters CDR`.

   The system displays the CDR System Parameters screen.

- If the software has been purchased, enter *y* in the `Authorization Code Enabled` field.
- In the **Authorization Code Length** field, enter **13 or the preferred length less than 13**.
- In the **Authorization Code Cancellation Symbol** field, enter **#** or **1**.
- 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. On barrier codes and authorization codes page, enter change remote-access.

   The system displays the Remote Access Status screen.

   - In the **Remote Access Extension** field, enter the appropriate extension number.
   - In the **Barrier Code Length** field, enter 7 or the preferred length less than 7.
   - 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 permit 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 or access limits on page 124.

4. Enter **change authorization-code <code>** to display the Authorization Code-**COR** Mapping screen.

   When assigning authorization codes used only to upgrade **FRL**s, use an outward-restricted **COR** with the appropriate **FRL**.

   Note:

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

5. Use a special partition group for the remote access **COR**, and administer the AAR and ARS tables only for those external locations that you permit 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**.

For more information, see Monitoring trunks on page 105.

Setting up remote access

About this task

Use the following procedure to set up the Remote Access feature to help prevent unauthorized use. It creates a new ARS and AAR networking plan in a separate Partitioned Group Number (**PGN**) for remote access only. By using the ARS and AAR Analysis table that corresponds with the remote access **PGN**, you can easily control the numbers that are permitted and the numbers that are not permitted.

Procedure

1. Enter **change remote-access** to display the Remote Access screen.
2. In the **Barrier Code Length** field, enter 13 or preferred length less than 13.
3. In the **Authorization Code Required** field, enter *n*.
4. In the first **Barrier Code** field, enter 7 or preferred length less than 7 digits.
5. Select a unique **COR** (**0** through **995**) that is unused for any facility other than remote access.

   For example, enter **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 unused for any facility other than remote access, and does not permit console permissions. A group number might be required when setting COS. For more information, see *Administering Avaya Aura® Communication Manager*, 03-300509.

   For this example, 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. In the **FRL** field, enter **0**.
11. Select a **PGN** (**1** through **8**) that is not in use in any other **COR**.

    This **PGN** is reserved for remote access only. Enter this number in the **Partitioned Group Number** field. For this example, 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, go to the Avaya Support website at http://support.avaya.com to open a service request to enable the ARS and AAR Partitioning feature.

12. Use the **change cos-group** and advance to the 15th column or go to the **COS** that you have selected in Step 7.
13. Enter ***n*** in *all* the fields associated with the **COS**.
14. Use **change trunk-group** <trunk group number> to administer the trunk groups.
15. Enter ***n*** in the **Dial Access** field. For more information, see Disabling direct access to trunks on page 76.

Note:

Repeat Step 14 and Step 15 for all the trunk groups in the system so that all outgoing calls route through ARS and AAR.

16. Use **change ars analysis x partition 8** and **change aar analysis x partition 8**, **where x is a value between 0** and **9**, to enter the dialed strings and the route pattern and other pertinent information for the entry where calling is permitted.

    You might need to delete some default entries that are already there.
17. Set the `Route Pattern` field to **blank** for all dialed strings to restrict calls such as international and operator calls.

    Any ARS and AAR calls starting with that dialed string will be blocked.
18. For all the route patterns assigned to ARS and 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 system will always prompt the remote access caller for an authorization code for outside calls.
19. Assign authorization codes for your remote access users that provide the lowest possible **FRL** to match the calling requirements of each user.

Suggested values for FRLs

Table 2: Suggested values for FRLs

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

FRL	Suggested Value
3	Supports local calls plus calls on FX and WATS trunks.
4	Supports toll calls within the home NPA.
5	Supports calls to certain destinations within the continental USA.
6	Supports calls throughout the continental USA.
7	Supports international calling. Assign Attendant Console FRL 7.

Feature access code administration

Certain feature access codes might facilitate egress from the system and must be used with care. For example:

- Data Origination
- Data Privacy
- Data Restriction
- Abbreviated Dialing
- ARS and AAR
- Call Forwarding
- Facility Test Calls.

In addition, be careful about 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

You can assign station-to-trunk restrictions to restrict the automated attendant ports from dialing specific outside trunks. By implementing these restrictions, callers cannot transfer out of voice mail to an outside facility using trunk access codes.

Note:

If you permit TAC access to tie trunks on the switch, the caller gains 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, the system assigns the trunk groups a Trunk Access Code (TAC). Unless required, prohibit both direct-dial access and facility test call access to trunk groups to prevent callers from using TACs 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 feature limits the amount of duration of remote access availability and also reduces risks.

Trunks translated for remote access can be given a night service destination, but the use of trunk translation must be minimized or eliminated. Trunks accessing the system can be assigned a remote access extension as a night service destination. The system will change to either permit 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 (VDNs) makes the feature more secure. Call vectoring permits 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 and 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 permitted 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 VDNs or soft switch extensions not assigned to a physical equipment location. The soft switch has many of the properties of a normal extension number, including a COR. 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

About this task

To deny incoming callers access to outgoing facilities, including tie lines, configure the COR of the VDN to prohibit outgoing access. Also see Calls processed by the vector carry the permissions and restrictions associated with the COR of the VDNTrunk-to-trunk transfer on page 65.

Procedure

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 CORs 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 permits the system to require a touch-tone response before the caller hears a remote access dial tone. In the absence of a response, the call can be routed to an attendant, announcement, or intercept tone. With this routing, attackers cannot easily detect a remote access port.

   Note:

   For both security and performance reasons, the Ethernet connectivity between Communication Manager and any SPI-enabled hosts with which Communication Manager communicates must be on a separate LAN segment. If the communication path is the same, then hackers can gain unauthorized access to the Communication Manager vectoring functions and can commit toll fraud and also tamper with the real-time aspects of CTI applications.

   For additional information, see *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 and ARS analysis

ARS routing permits 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 permit or prohibit calling at certain times.

Note:

Never route public network calls with the leading digit 0 or 1 through 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 might 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 and ARS calls, use FRLs to limit the calling area. For more information, see Facility restriction levels on page 44.

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 the dial tone. Conversely, the elimination of the dial tone also serves to confuse authorized users who are accustomed to the second dial tone.

Station restrictions

If access to trunks via TACs is necessary for certain users to permit 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

Using recall signaling, analog station users can place a call on hold and consult with another party or activate a feature. After consulting with the third party, the user can include the third

party in a conference call 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 can activate recall signaling to gain second dial tone and conference incoming and outgoing paths together. To prevent this, administer switchhook flash to n for FAX machines and modems. To administer switchhook flash, use the Add or Change Station screen.

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 then connect 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. For details, contact your local telephone company.

Individual and group-controlled restrictions

With individual and group-controlled restrictions, an attendant or voice terminal user with console permission can activate and deactivate the following restrictions for an individual terminal or a group of voice terminals:

- Outward: Cannot place calls to the public network.Such call attempts receive an intercept tone.
- Total: Cannot place or receive calls. DID calls are routed to the attendant or a recorded announcement. All other calls receive an intercept tone. The following call types are exceptions: calls to a remote access extension, terminating trunk transmission tests, and emergency access to attendant calls.
- Station-to-station: Cannot receive or place station-to-station calls. Such call attempts receive an intercept tone.
- Termination: Cannot receive any calls. Incoming calls are routed to the attendant, through call coverage, or receive intercept treatment.

Cannot receive any calls. Incoming calls are routed to the attendant, through call coverage, or receive intercept treatment.

To activate the preferred controlled restriction, the attendant or voice terminal user with console permission dials the following numbers in the specified order:

1. The feature access code for either the extension or the group.
2. The number 1 for Outward, 2 for Total, 3 for Termination, or 4 for Station-to-Station.
3. The voice terminal extension number, that is, Attendant Control — Extension, or the COR for a group of voice terminals, that is, Attendant Control — COR.

This feature is especially helpful in businesses with multiple endpoints. For example, in a hotel you can restrict telephones in empty conference rooms, in guest rooms after a client checks out, or in an entire wing of a building as required.

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 enables a station to connect an incoming trunk to an outgoing trunk and drop the connection. When you disable this feature, stations cannot transfer an incoming trunk call to an outgoing trunk. If the controlling station drops the call, the call is dropped.

Note:

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

Communication Manager can either permit or restrict trunk-to-trunk transfer. This feature is for public network trunks only. DS1 and WATS trunks assigned as tielines are not 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 disable this feature, see Restricting trunk-to-trunk transfer on page 79.

Note:

To prevent inadvertent trunk-to-trunk transfers during conference calls, always conference together two outgoing calls. When the calling station disconnects, the trunks must 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, you must enable and administer the Forced Entry of Account Code feature on the system.

You can make the entry of an account number, 1 to 15 digits, compulsory for the originating station COR, toll calls, or AAR and 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. With this feature, the attacker must crack another level of digit entry to gain access to an outside line.

AAR and ARS routing

Specific digit strings are assigned to either permit 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 permits 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 might prevent you from blocking these calls. 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 and ARS routing restrictions

About this task

To restrict AAR and ARS from unauthorized use:

Procedure

1. Miscellaneous restrictions (COR-to-COR restrictions) are not observed during AAR and 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 the **`change toll`** command to display the Toll screen. Identify what calls are permitted or not permitted.
6. Use the **`change ars analysis`** command 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-digit or 4-digit strings.
9. Use **`change ars analysis`** to distinguish between 7-digit 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. Assigning a toll-restricted COR to the originating endpoint prevents TAC toll calls.

    Note:

    Whenever possible, restrict TAC calls. See Disabling direct access to trunks on page 76.

Digit conversion

Digit conversion enables 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, you must protect WHAT by assigning a code that is not 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, customers must periodically change the SSC for each administered extension.

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. With this feedback, an automated attack cannot 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.

Accessing the Security Violations Status report

About this task

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 to display the date, time, port or extension, FAC, and dialed digits for each invalid attempt.

Procedure

To access this report, enter the **monitor security-violations station-security-codes** command at the prompt .

Accessing the Security Violations Summary report

About this task

The Security Violations Summary report summarizes the SSC violations.

Procedure

To gain access to this report, enter the **list measurements security-violations summary** command.

Accessing SSC-enabled transactions

About this task

Most SSC-enabled transactions are recorded in the history log.

Procedure

1. To gain access to the transactions, enter the **list history** command at the prompt.
2. To prevent unauthorized PSA/TTI transactions, enter the **change logging-levels** command and gain access to the Feature-Related System Parameters screen.
3. To enable logging for those transactions, enter y in the **Log CTA/PSA/TTI Transactions** field.

   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.

For security report information, see *Avaya Aura® Communication Manager Reports*, 555-233-505and *Administering Avaya Aura® Communication Manager*, 03-300509.

EC500 Security Features

When Extension to Cellular is administered and active, a call to a configured user Avaya Aura® CM office extension is simultaneously extended to a configured destination such as a cellular phone. When EC500 is enabled for a given Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® 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, customers must retain the default setting for EC500 Calling Number Verification. If this setting is changed and EC500 is enabled, an attacker with knowledge of assigned cellular destinations can 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 that data, and in some cases, this spoofed ANI data can appear to be trustworthy. Even with EC500 Calling Number Verification set to y, this transitive trust problem remains an issue for customers in North America for the forseeable future.

Because of a potential for toll fraud in conjunction with ANI spoofing, customers must not enable the Idle Appearance Select feature of EC500 off-PBX-telephone feature. This FNE enables an EC500 extension, usually the cellphone of the user, to receive a dial tone from Avaya Aura® CM as the office extension.

For a complete description of EC500 functionality and security feature configuration options for EC500 and one-X Server, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Blocking international calling

About this task

If your company does not do business overseas, block the international dial prefix, for example, 011. Note that this action impacts the ability to reach the Telco operator since 0+ dialing is blocked. This action can affect credit card calls, collect calls, third-party calls, and special use (0700+) numbers. Use this procedure to block international calls.

Procedure

1. Enter **`change ars analysis`** 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:

   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.

Blocking calls

About this task

In the following procedure, international and operator-assisted numbers are permitted, but 0700 calls and certain destinations, which tend to have high toll fraud rates are denied. Use the following procedure to block calls.

Procedure

1. On the Communication Manager SAT screen, type **`change ars analysis`**.
2. In the **Dialed String** field, enter the digits `0-9`, `x`, or `X`.
3. In the **Min** field, enter the minimum number of digits. Valid entry can be a number less than 23 or blank.
4. In the **Max** field, enter the maximum number of digits. Valid entry can be a number not greater than 23 or blank

5. In the **Route Pattern** field, enter route pattern (1-2000), partition-route-table index (p1-p2000), RHNPA index (r1-r250), deny, or node.
6. In the **Call Type** field, enter the specific call type.

ARS digit analysis

The ARS DIGIT ANALYSIS TABLE on page 72 shows examples of values for the **Call Type** field.

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

ARS DIGIT ANALYSIS TABLE				
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
101xxxx1809	16	16		fnpa
180	11	11	1	fnpa
1809	11	11		fnpa

Limiting international calling

About this task

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

Procedure

1. Enter `change ars analysis` to display the ARS Analysis screen.
2. Enter the telephone numbers in the **Dial String** field and set the routing pattern or routing to a pattern that contains a high FRL to block dialing the numbers.
3. Disable TAC/DAC dialing.

   For more information, see Disabling direct access to trunks on page 76.
4. To block calls to countries in the North American dial plan, enter the area code plus any required prefix digit (0 and 1). You must also 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 the **Max** fields.

Selecting authorization code time-out to attendant

About this task

Attendant Time Out Flag indicates that a call cannot be routed if a caller does not dial an authorization code within 10 seconds or dials an invalid authorization code.

Procedure

1. To administer authorization codes, select the Timeout to Attendant feature.
2. To request authorization code timeout, use the System-Parameters features screen.

Restricting calls to specified area codes

About this task

If your business does not require users to make calls to certain area codes, you can block entry of those area codes. Certain destinations are common toll-fraud destinations, such as 1+809 and 0+809 (Dominican Republic), 900/976 services and lookalikes, and Alliance teleconference service (0700). You must restrict these destinations if your business does not require regular access to them.

Procedure

1. Enter `change ars analysis`.

   The system displays the ARS Analysis screen.

2. In the **Dial String** field, enter the telephone numbers to block. For example, 1+809 and 0+809.

   Note:

   In addition to blocking area codes, you can block specific destinations using this method. For instance, blocking toll-free access numbers for long-distance services which can also be a source of abuse.

3. Disable **TAC** dialing. For more information on TAC dialing, see Disabling direct access to trunks on page 76.

Permitting calls to specified numbers

About this task

To permit outbound calls to certain numbers by specifying the area codes or telephone numbers of calls:

Procedure

1. Enter `change ars analysis`.

   The system displays the ARS Analysis screen.

2. Enter the area codes or telephone numbers and assign an available routing pattern to each of the area codes. You can also use remote HNPAs.

Using attendant control of specific extensions

About this task

Telephones 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 telephones from the console.

Procedure

1. Enter `change feature-access-codes`.

   The system displays the FAC screen,

2. In the **User-Control Restrict Activation/Deactivation** fields, enter a valid FAC.

3. Enter `change system-parameters feature`.

   The system displays the Feature-Related System Parameters screen

4. Specify the type of intercept treatment, such as announcement, attendant, extension, or tone, that the controlled stations receive.
5. Enter `change COS`.

   The system displays the Class of Service screen.
6. In the Console Permissions field, enter `y`.
7. Enter `change station` or `change attendant` to assign the COS to the station handling the controlled restrictions.

Disabling direct access to trunks

About this task

To make external calls, use AAR/ARS and not direct trunk access through DACs. To disable DACs for outgoing calls system wide:

Procedure

1. For each trunk group in the system, enter `change trunk group` *n*, where *n* is the trunk group number.

   The system displays the Trunk Group screen.
2. In the **Dial Access** field, enter *n*.
3. To permit individual stations to use DACs but deny DAC access to others:
   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

About this task

To permit direct access to trunk groups, you must configure the trunk groups as attendant-controlled trunk groups. The attendant can screen the incoming and outgoing calls.

You can control up to 12 trunk groups.

Procedure

1. Enter `change attendant`.

   The system displays the Attendant screen.

2. In the **Feature Button Assignment** field, enter `act-tr-grp` or `deact-tr-grp` to activate or deactivate attendant control of a trunk group.
3. In the **Direct Trunk Group Select Button Assignment** field, enter the corresponding trunk access code.
4. To activate attendant control of the trunk group, press the `act-tr-grp` button.

Note:

The attendant-controlled trunk groups affects all users, not just remote access users. If calls are dialed via AAR and ARS, these trunks will be skipped in the routing pattern.

Facility test calls

Using the Facility Test Call feature, you can 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 branch 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, ensure that the Facility Test Calls access code is assigned. The access code must be left blank except when actually testing trunks. The COR of the station user must 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, customer must 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 might 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 COR permits disabling facility test calls, test calls can be made to access specific trunks. Do not disable test call facility unless you need the facility, and remove the facility after the test is completed.

Removing the Facility Test Calls Access Code

Procedure

1. Enter `change feature-access-codes`.

   The system displays the FAC screen

2. Leave the `Facility Test Calls Access Code` field blank.
3. To permit stations with a specified COR to perform the test, but deny the ability to other stations:

   Enter `change cor`.

   The system displays the Class of Restriction screen.

   a. In the **Facility Access Trunk Test** field, enter `y`.
   b. To assign the COR with the FAC test permission to the appropriate station, enter `change station`.
   c. Assign all other stations to a COR with the **Facility Access Trunk Test** field set to n.
   d. To monitor test call access code use, assign a trunk access alarm button to a voice terminal.

4. To help secure the Facility Test Call feature from unauthorized use:

   a. Remove the access code when not in use.
   b. Change the code frequently if used, else disable the test call code by leaving the code blank).
   c. Protect records of the code.
   d. Use CORs 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.

Result

Use the sign-off feature to alert the administrator that the code is administered.

Suppressing remote access dial tone

About this task

When an authorization code is required, you can eliminate the remote access dial tone that callers hear after entering the required barrier code. Callers also do not receive a prompt for the authorization code.

Procedure

1. Enter `change remote-access`.

   The system displays the Remote Access screen.

2. To suppress the remote access dial tone, in the **Remote Access Dial Tone** field, enter `n`.

Restricting trunk-to-trunk transfer

About this task

Trunk-to-trunk transfer is a feature that permits 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.

Procedure

1. Enter `change system-parameters`.

   The system displays the Features-Related System Parameters screen,

2. In the **Trunk-to-Trunk Transfer** field, perform one of the:

   a. To permit all trunk-to-trunk transfers, enter `a`.
   b. To restrict all public trunks, enter `r`.
   c. To restrict all trunks from being transferred except DCS and CAS, enter `n`.

   Note:

   Even if you restrict trunk-to-trunk transfer, the START 9 RELEASE sequence supplies a dial tone to the caller, enabling trunk-to-trunk transfer to proceed.

Outgoing trunk to outgoing trunk transfer

The outgoing trunk to outgoing trunk transfer (OTTOTT) feature permits 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.

Using OTTOTT, you can establish calls in which the only parties involved are external to the switch and are on outgoing trunks. However, this enhancement of trunk-to-trunk transfer is perilous.

Caution:

Using OTTOTT feature, an outside party can be transferred to a trunk to make toll calls.

Enabling the outgoing trunk to outgoing trunk transfer feature

About this task

To mitigate the problems associated with the accidental use of this feature, you can only administer this feature on trunk groups on the Trunk Group screen.

Procedure

To enable this feature, use the **Disconnect Supervision Out** field.

This feature is not a system wide option.

Note:

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, the use of OTTOTT with DCS is not prohibited, and might be helpful when one or more of the trunks go off the DCS network.

Configuring outgoing trunk to outgoing trunk transfer

Procedure

1. Since trunks must be specifically administered for OTTOTT, ensure that the COR and FRL of the trunk group are appropriate.
2. If the feature is not relevant to your business, do not enable OTTOTT feature. If a temporary need for the feature arises, enable OTTOTT and turn the feature off after use.

Restricting outgoing calls from tie trunks

About this task

If you use tie trunks solely for office-to-office calling, you can deny access from tie trunks to outgoing AAR/ARS calls.

Procedure

1. Use the **change cor-group** command 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 do not give direct access calling permissions to CORs of trunk groups to incoming tie lines 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

About this task

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

Procedure

1. To display the Class of Restriction screen, enter `change cor`.
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 do not give calling permissions to other trunk group CORs.

   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

About this task

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).

Procedure

1. Enter `change system-parameters feature`.

   The system displays the Features-Related System Parameters screen.
2. Enter `15` in the **CDR Account Code Length** field.
3. To activate the measure system-wide, in the **Force Entry of Account Codes** field, enter **y**.

   Note:

   To activate the feature on an individual basis, use **`change cor`** to display the Class of Restriction screen.
4. In the **Force Entry of Account Code** field, enter `y`.
5. Use the **`change station`** command to assign the COR to the appropriate stations.

   Note:

   CDR and account codes are only required for toll calls.
6. Enter `change toll`.

   The system displays the Toll Analysis screen.
7. 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. The COR restrictions assigned to stations, trunks, and sometimes other entities, such as other equivalent extension where multiple CORs apply, such as when both

the agent log-in ID and the extension CORs have the needed restrictions, the COR of the log-in ID takes precedence.

Disabling distinctive audible alert for adjunct equipment

About this task

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

Analog ports assigned to adjunct equipment must have the Distinctive Audible Alert feature set to no. The Distinctive Audible Alert feature is a field on the Analog Station screen, and the default value is yes.

Procedure

1. Type the`change station <ext>` command to display the Station screen.
2. Enter `n` in the **Distinctive Audible Alert** field.

Remove data origination code

The Data Origination feature is used in conjunction with modem pooling. The data origination code permits users to bypass many system restrictions and gives them access to outside facilities. The data origination code can 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 telephone, the switch returns outside dial tone and permits a call to be processed.

You must remove or change the data origination code.

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 system performs the following actions:

1. The voice mail system verifies that the digits entered contain the same number of digits as administered for extension lengths.

   If call transfer is restricted to subscribers, 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.

2. If Step 1 is successful, the voice mail system sends a transfer control link message containing the digits to the switch.

   If Step 1 is unsuccessful, the voice mail system plays an error message to the caller and prompts for another try.

3. The switch verifies that the digits entered match a valid station number in the dial plan.

   - If Step 3 is successful, the switch completes the transfer, disconnects the voice mail system voice port, and sends a successful transfer control link message to the voice mail system.
   - If Step 3 is unsuccessful, the switch leaves the voice mail system voice port connected to the call, sends a fail control link message to the voice mail system, and 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, and the caller enters 0 to connect 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 the call must follow the coverage path of the transferred-to station. Administer enhanced call transfer to permit this type of transfer. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, knowledge articles related to the topic, or to open a service request.

Considerations for Communication Manager and Messaging in Automated Attendant

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 might keep trying to get through.

Limiting tansfers to internal destinations

About this task

You can restrict Automated Attendant menu options to transfer only to internal extension numbers or announcements by making the automated attendant ports outward restricted.

Procedure

Procedure

1. On the **Class of Restriction** screen, create an outward-restricted **COR** by entering **outward** in the **Calling Party Restriction** field.
2. Assign the outward-restricted **COR** to the automated attendant port.
3. Assign an FRL of 0 and enter **n** for all trunk group CORs.

Preventing calls to certain numbers

About this task

If some menu options transfer to off-premises locations, 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.

Procedure

Procedure

1. On the **Class of Restriction** screen for the automated attendant ports, enter **y** in the **Restricted Call List** field.

2. On the **Toll Analysis** screen, specify the telephone numbers that automated attendant callers must restrict from dialing.

Permitting calling to specified numbers

Procedure

1. Enter **`change ars analysis`** to display the **ARS** Analysis screen.
2. Enter the area codes or telephone numbers and assign an available routing pattern to each of them.
3. 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

Restricting outside calls

Procedure

1. On the voice mail system appearance screen, in the **Call Transfer Out of AUDIX** field, enter `y`.
2. In the **Enhanced Call Transfer** field, enter `y`.
3. Press `Change/Run`.
4. On the SAT screen, enter `change listed-directory-numbers` to add a valid extension for your attendant.
5. After you activate Enhanced Call Transfer, dial in to 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 hash sign (#).

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

   You might notice that the call transfers much faster than with Basic Call Transfer.

Note:

To test correctly, you must first dial outside of the system, and dial back in on the number assigned to the automated attendant. A station-to-station connection will not test correctly.

Avaya Aura® Communication Manager Messaging

Enhanced call transfer for Avaya Aura® CM Messaging

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, Communication Manager may accept the calls as a valid extension number. Even with the Enhanced Call Transfer feature activated, toll attackers can choose a menu option that permits 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.

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:

1. The voice mail system verifies that the digits entered contain the same number of digits as administered for extension lengths.

   If call transfer is restricted to subscribers, 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.

2. If the verification is successful, the voice mail system sends a transfer control link message. If the verification is unsuccessful, the voice mail system plays an error message to the caller and prompts for another try.
3. The switch verifies that the digits entered match a valid station number in the dial plan.
4. 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.
5. 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 permit this type of transfer. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, knowledge articles related to the topic, or to open a service request.

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 telephone 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 permits 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 permits 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 permits calls to be placed to destinations that are off-premises.

Disabling transfer out of the system

About this task

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, then deactivate this feature. For more information, see Transfer out of the system on page 88 for details.

Procedure

1. On the SAT screen, type the command `change system-parameters features`.

   The system displays the Feature-Related System Parameters screen.

2. In the **Transfer Type** field, type `none`.

Note:

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

Limit outcalling

About this task

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.

Procedure

1. 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.
2. Assign the outward restricted **COR** to the voice mail system voice ports.

Result

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 permits 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, enter `n` in the **Outcalling** field to turn off outcalling.
- On the voice mail system Outcalling screen, limit the number of digits that can be dialed for outcalling; permitting exactly the number of digits required to complete the call.

Note:

For outcalling to a pager, additional digits might be required.

Protect AMIS networking

To increase security for AMIS analog networking, including the message delivery service, restrict the number ranges that might be used to address messages. Ensure to assign all the appropriate Communication Manager 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 Avaya Aura® CM to the CMS system, vector modifications can be sent from the CMS system to Avaya Aura® 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 Avaya Aura® CM.

Note:

For both security and performance reasons, the Ethernet connectivity between the CMS and Avaya Aura® CM must be a separate LAN segment. If CMS and Avaya Aura® CM are on the same LAN segment, hackers 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 restrict 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 Communication Manager 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 CMS product documentation heading on http://support.avaya.com.

For switch restrictions, see the *Communication Manager* section in this chapter. You can also refer to the Avaya Aura® 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: Modular Messaging Security goals

Security Goal	Method	Security Feature	Suggestions to achieve the goal
Prevent unauthorized calling	Block transfers to invalid mailboxes	Block invalid mailbox transfer	Disable Transfer Invalid Mailboxes. For information, see Disable transfer to invalid mailboxes **on page 87** on page 94.

Security Goal	Method	Security Feature	Suggestions to achieve the goal
		Block invalid mailbox transfer	• System Operator must be a valid Modular Messaging mailbox number. • Set outcalling restrictions. For information, see System operator on page 94.
	Carefully configure attendant, operator, and subscriber application options	Automated attendant settings	Ensure menu option settings are appropriate. For information, see Automated Attendant on page 95.
		Caller application settings	Ensure settings are appropriate. For information, see Caller Applications on page 96.
		Personal operator settings	Ensure settings are appropriate. For information, see Caller Applications on page 96.
		Find Me, Call Me, Notify Me settings	• Ensure settings are appropriate. • Restrict subscriber features with COS. For information, see Find Me / Call Me / Notify Me on page 97.
		Fax settings	Ensure external hunt group setting is correct. For information, see Fax on page 98.
	Block transfers to invalid mailboxes	Block invalid mailbox transfer	Disable Transfer Invalid Mailboxes. For information, see Disable transfer to invalid mailboxes on page 94.
Protect subscriber mailbox from unauthorized access	Configure mailbox PIN and lockout settings	Mailbox PIN and lockout settings	• Configure appropriate PIN complexity and expiration settings. • Configure appropriate lockout settings. • Deactivate unused mailboxes. For information, see Configuring Subscriber Mailbox Protection on page 98.

Security Goal	Method	Security Feature	Suggestions to achieve the goal
Protect administrative interfaces from unauthorized access	Limit access to IP and telephony-based administrative access	Authentication and Authorization features	Manage administrative credentials and roles. For information, see Configuring Administrative Access and System Protection on page 98.
		COR	Use COR to restrict access to administrative ports. For information, see Configuring Administrative Access and System Protection on page 98.

Security suggestions for Modular Messaging

The Modular Messaging administrator can use the following security tips.

Disable transfer to invalid mailboxes

Ensure that Modular Messaging is configured to permit transfer only to valid Modular Messaging mailboxes, and not to arbitrary extension numbers, by disabling the following settings using Voice Mail System Configuration (VMSC):

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

System operator

Ensure that Modular Messaging does not permit transfer to invalid mailboxes. For more information, see Disable transfer to invalid mailboxes on page 94.

Configure the system operator to be a valid Modular Messaging 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 might 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 for Modular Messaging

Ensure that Modular Messaging does not permit transfer to invalid mailboxes. For more information, see Disable transfer to invalid mailboxes on page 94.

If transfers to extensions as well as mailbox numbers are needed, prevent Modular Messaging 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 telephone 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 telephone numbers that you explicitly permit:

- 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 restrict Automated Attendant calls to external numbers, be aware that it will also affect Caller Applications

Additional suggestions for preventing toll fraud on Automated Attendant:

- Never permit 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 *Messaging Application Server Administration*.

- If any menu option routes to a Direct Inward System Access (DISA) feature on the PBX 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 Modular Messaging 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 Modular Messaging does not permit transfer to invalid mailboxes. For more information, see Disable transfer to invalid mailboxes on page 94.

- 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 telephone 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 restrict 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 Modular Messaging is configured to permit only personal operators that are valid Modular Messaging mailboxes and not arbitrary extension numbers, by disabling the following option:
  - VMD / TUI / Receptionist / Permit personal operators that are not local mailboxes

- Prior to Modular Messaging 5.0, default configurations permitted personal operators that are not valid Modular Messaging 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 telephone 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 restrict subscriber calls to external numbers, then other subscriber outcalls like Find Me and Call Me can also be affected.

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 Modular Messaging if the enquiry call is not answered. However, depending upon the precise system configuration including the integration type, an unsupervised transfer can 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.
- Administrators must 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 use fax with Modular Messaging configured with a third-party fax server, you must ensure that the VMD / Fax / General / Hunt Group Pilot Number is the correct hunt group number for the fax server.

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.
- Do not use temporary passwords.
- Deactivate unassigned mailboxes, and remove unused mailboxes.
- Minimize 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.
- Ensure that subscribers change their passwords immediately upon first log-in. 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. For more information regarding Modular Messaging

security features designed to protect administrative access, see the *Modular Messaging Security Guide.* You must also implement 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 Communication Manager systems (or equivalent restrictions on third-party PBX systems) to restrict access to administration ports. If you use scriptable Personal Computer 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 MAS Administration.

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.

The following are some 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, hook-on, 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 permit transfers, uses Enhanced Call Transfer, or permits Transfer to Subscriber Only.

Avaya Aura® Session Manager

Avaya Aura® 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 suggestions for Avaya Aura® Session Manager

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 5: 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.
- An unexplained increase in long distance usage with bill detail showing calls to unfamiliar destinations.
- An increase in the number of short duration calls and calls to unprovisioned numbers.
- Heavy call volume at nights, on weekends, and holidays.
- CDR shows an unusual number of short duration calls.
- Established thresholds on trunk groups are exceeded.
- Switchboard operators note or complain about frequent calls from individuals with foreign accents.
- Inability of customers or staff to enter voice mail system, unusual messages left in mailboxes, or suspicious changes 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.
- A sudden or unexplained inability to gain access to specific administrative functions within the system.
- Employees complain of difficulty in obtaining an outside line.
- 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.
- An unusual increase in equipment-based system memory usage at customer premises.
- 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).
- Discrepancies in telephone bills, such as unusual calling patterns, calls to international locations with which the user does not normally interact, and unaccounted calls.

Avaya Aura® Communication Manager

Toll Fraud Detection

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.

The table on page 104 shows the reports and monitoring techniques that track system activity and help detect unauthorized use:

Table 4: Reports and monitoring techniques (continued)

Monitoring Technique	Page No.
Monitor trunks	97 on page 105
Call detail recording (CDR)	97 on page 105
Traffic measurements/performance	98 on page 106
Automatic circuit assurance	100
BCMS measurements	101 on page 109
CMS measurements	101 on page 109
Security Violations Measurement report	103 on page 111
Security Violation Notification feature	101 on page 109
Viewing Recent Change History report	115 on page 124
Service Review/Analysis	116 on page 126
Malicious call trace	115 on page 125
`list call-forwarding` command	117 on page 127

Monitoring trunks

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

Any superuser or non-super user with permission to display administration and maintenance data can use the **monitor** command.

Using the **monitor** command, you can locate facilities to which the trunk is communicating and track hacking activity. 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 might 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.

CDR records authorization codes, if required, but does not record barrier codes. If you set the **Suppress CDR for Ineffective Call Attempts** field to no, calls that fail because the caller has inadequate calling privileges generate a condition code in the report to reflect the failed attempt. Review the report for these condition codes, which might indicate attacker activity. For more information on CDR description, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Avaya and third-party partners offer several call accounting system add-ons that enhance CDR by creating customized reports. You can use these reports to isolate suspicious calls.

Note:

If Outg Trk Call Splitting is not 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 and transfer to another extension before terminating the call. Internal toll abusers can transfer unauthorized calls to another extension before the calls 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 fraud:

- Short holding times on one trunk group
- Patterns of authorization code usage (same code used simultaneously or frequent usage)
- Calls to international locations not required 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

Procedure

1. Enter the **`change system-parameters cdr`** command.

   The system displays the CDR System Parameters screen.
2. Administer the appropriate format to collect the maximum information. The format depends on the capabilities of your CDR analyzing or recording device.
3. Enter the **`change trunk-group`** *n* command, where *n* is the trunk group number.

   The system displays the Trunk Group screen.
4. In the CDR Reports, enter `y`.

Traffic measurements and performance

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

- Unusually high peg counts on trunk groups
- A series of short or long holding times that can 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.

For more information about reports, see *Avaya Aura® Communication Manager Reports, 555-233-505*.

Reviewing traffic measurements

Procedure

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).

Reviewing performance

Procedure

Enter `list performance` followed by one of the performance types (summary or trunk-group) and the timeframe (yesterday or today).

Tracking routine patterns

About this task

The ARS Measurement Selection feature can monitor up to 25 routing patterns for traffic flow and usage. Use this procedure to track routine patterns:

Procedure

1. Enter `change meas-selection` *route pattern* to choose the routing patterns to track.
2. Enter `list measurements` *route-pattern* with assigned pattern (1-2000) 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).

Automatic Circuit Assurance

This monitoring technique detects a pattern of short holding time calls or a single long holding time call which can indicate attacker activity. Long holding times on trunk-to-trunk calls can be

a warning sign. Use the Automatic Circuit Assurance (ACA) feature to establish time limit thresholds that define 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 audio message accompanies the call.

When a notification occurs, determine if the call is still active. If you suspect toll fraud, for example, the designated telephone displays `aca-short` or `aca-long`, use the busy verification feature to monitor the call in progress. For more details see Configuring Busy verification on page 127.

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 an automated attendant answers the call, an attacker might be attempting to gain access to the system facilities using TACs.

Configuring Automatic circuit assurance

Procedure

1. On the SAT screen, type the command `change system-parameters feature`.

   The systems displays the Features-Related System Parameters screen.
2. In the **Automatic Circuit Assurance (ACA) Enabled** field, enter `y`.
3. In the **ACA Referral Calls** field, enter `local`, `primary`, or `remote`.

   If you select primary, the system can receive calls from other switches. Use remote if the PBX that is administered is a DCS node, perhaps unattended, that wants ACA referral calls to route to an extension or console at another DCS node.
4. Enter appropriate values in the following fields: **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` *n*, where *n* is the trunk group number.

   The system displays the Trunk Group screen.
7. In the **ACA Assignment** field, enter `y`.
8. In the **Long Holding Time (hours)** field, enter the maximum holding time.

   The default value for this field is 1, which means that the maximum holding time is one hour.
9. In the **Short Holding Time (sec)** field, enter the short holding time.

The default value for this field is 10, which means that the short holding time is 10 seconds.

10. To review an audit trail of the ACA referral call activity, enter `list measurements aca`.

Configuring BCMS measurements

About this task

BCMS Measurements report traffic patterns for measured trunk groups.

Procedure

1. Enter `change trunk-group` *n*, where *n* is the trunk group number.
   The system displays 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. Enter `change system-parameters feature`.
   The system displays the Features-Related System Parameters screen.
4. To review the measurements, enter `list bcms trunk`.

Configuring CMS measurements

About this task

This monitoring technique measures traffic patterns and times on calls and compares them to traffic counts and time limit thresholds. The system maintains an exceptions log whenever the traffic counts or time limits exceed the preset thresholds.

Procedure

1. Enter `change trunk-group` *n*, where *n* is the trunk group number.
   The system displays the Trunk Group screen.
2. In the **Measured** field, enter `external` if you have only CMS or both if you have BCMS and CMS.

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.

If an announcement has been administered and recorded, the referral destination can be any station. 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 the problem occurs and it provides an opportunity to interrupt unauthorized calls before charges are incurred and 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, the SVN feature can send an invalid log-in attempt message to any station if an announcement has been administered and recorded. On receiving the notification, 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. For more information, see Security Violations Measurement report on page 111.

Configuring the SVN feature

Procedure

1. Enter `change system-parameters security`.

   The system displays the System-Parameters Security screen.
2. To monitor remote access, in the **SVN Remote Access Violation Notification Enabled?** field, enter `y`.
3. To monitor authorization codes, in the **SVN Authorization Code Violation Notification Enabled** field, enter `y`.

4. In the **Originating Extension** field, enter any valid unassigned extension number.
5. In the **Referral Destination** fields, enter the extension number of the person who monitors violations. If you administer an announcement extension, 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 permitted 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 the **Barrier Code Threshold** field is set to 1, an authorized user who enters the barrier code unsuccessfully the first attempt triggers a violation. A suggestion is to set the threshold to permit three attempts within 5 minutes.

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 turn on 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, you must deactivate the feature activation buttons 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 if a remote access security violation has occurred. Any attempt to use the Remote Access feature once it has been disabled will fail even if a correct barrier code or barrier code and authorization code combination is provided 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 report

The Security Violations Measurement report identifies the entry of invalid barrier codes and monitors the remote access ports. Review the report daily to track invalid attempts to enter barrier codes, which can indicate attacker activity.

For complete details, see *Avaya Aura® Communication Manager Reports*, 555-233-505.

- Use the **`list measurements security-violations summary`** command to obtain this report, which is updated on an hourly basis.

  The report is divided into two sub-reports, a Summary report and a Detail report. Refer the table.

  Note:

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

- Use the monitor security-violations feature to obtain 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 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

  The report displays data that 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.

Security Violations Summary report field descriptions

Name	Description
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

Name	Description
	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

Remote Access Violations Status report field descriptions

Name	Description
Date	The day 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 number associated with the trunk where the authorization code attempt terminated.
Ext	The extension used to communicate with the Remote Access feature
Barrier Code	The incorrect barrier code that resulted in the invalid access attempt.

Authorization Code Violations Status report field descriptions

Name	Description
Date	The date the violation occurred.
Time	The time the violation occurred.

Name	Description
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 is visible 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 is visible 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 is visible only when a authorization code is entered to invoke remote access.
Ext	The extension associated with the station or attendant originating the call. It is visible only when a authorization code is entered from a station or attendant.

Station Security Code Violations report field descriptions

Name	Description
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.

Name	Description
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. By analyzing the digits, you can judge whether the caller was actually trying to break in to the system or an authorized user made a mistake while entering the feature code.

Administration of the SVN feature

Administering the barrier code security violations parameters of the SVN feature

Procedure

1. Enter `change system-parameters security`.

   The system displays the Security-Related System Parameters screen.
2. To enable the remote access component of the feature, in the **SVN Remote Access Violation Notification** field, enter `y`.

Result

The following fields are required to activate the SVN feature. Refer the table for more information.

1. In the **Originating Extension** field, 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.
2. In the **Referral Destination** field, enter an extension assigned to a station or attendant console that will receive the referral call when a security violation occurs.
3. In the **Barrier code Threshold** field, enter the minimum number of invalid authorization code attempts that are permitted before a referral call is made.
4. In the **Time Interval** field, enter the time interval within which a login security violation must occur.

5. In the **Announcement Extension** field, enter an extension that is assigned to the SVN announcement.
6. Save and submit the screen.
7. Enter `change remote-access`.

   The system displays the Remote Access screen.
8. To activate the Disable Following A Security Violation feature, in the **Disable Following a Security Violation** field, enter `y`.
9. Save and submit the screen.
10. Administer an **rsvn-halt** button on any station or attendant console.

    To determine the location of the SVN button, enter the `display svn-button-location` command. If you activate the rsvn-halt feature button, you cannot make any referral calls until the feature button is deactivated.

Activating SVN feature field descriptions

Name	Description
Originating Extension	The originating extension initiates the referral call in the event of a log-in security violation and sends the appropriate alerting message or display to the referral destination.
Referral Destination	The referral destination must be equipped with a display module unless the Announcement Extension has been assigned. Call vectoring using time of day routing permits security notification to be extended off-premises.
Barrier code Threshold	Using the values assigned to the Barrier code Threshold and the Time Interval fields, you can determine whether a security violation has occurred. The system default for this threshold is 10.
Time Interval	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	The announcement must be recorded for the SVN referral call to be made. Repeat the

Name	Description
	announcement if the SVN is routed to an answering machine.

Enabling or disabling remote access code

Procedure

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 proper permissions.
   b. Enter the `enable remote-access` command.
2. To disable remote access:
   a. Log in to the switch using a login ID with the proper permissions.
   b. Enter the `disable remote-access`command.

Administering the Remote Access Kill After N Attempts feature

About this task

The following is an example of how to administer this feature.

Procedure

1. Enter `change system-parameters security`.
2. On the System-Parameters Features screen, enter data in the following fields:
   - To enable the remote access component of the SVN feature, in the **SVN Remote Access Violation Notification Enabled** field, enter `y`.
   - In the **Originating Extension** field, enter an unassigned extension that conforms to the switch dial plan.
   - In the **Referral Destination** field, enter an extension that is assigned to a station equipped with a display module.
   - In the **Barrier Code Threshold** field, enter the number of times you can enter an invalid barrier code before a security violation is detected.
   - In the **Time Interval** field, enter the time duration within which the invalid barrier code attempts must occur.
3. Enter `change remote-access`.
   The system displays the Remote Access screen.

4. In the **Disable Following A Security Violation** field, enter `y` to disable remote access following a security violation.

   Note:

   The **Disable Following A Security Violation** field is dynamic. The system displays this field only if the remote access component of the SVN feature is enabled.

Result

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.

1. Check 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 might assist you in tracing the source of the violation. Do not re-enable the Remote Access feature until the source of the violation is identified and the feature is secure.
2. Enter the `enable remote-access` command to re-enable the Remote Access feature.
3. If the Remote Access feature is to be dormant for a period of time, you can disable the feature using the **`disable remote-access`** command.

Administering the authorization code component

About this task

To administer the authorization code component of the SVN feature, perform the following:

Procedure

1. Enter the `change system-parameters security` command.

   The system displays the System Parameters Security screen.
2. In the **SVN Authorization Code Violation Notification Enabled** field, enter `y`.

   The table provides a description of the fields that appear when the **SVN Authorization Code Violation Notification Enabled** field is set to `y`.
3. In the **Originating Extension** field, 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.
4. In the **Referral Destination** field, enter an extension assigned to a station or attendant console that will receive the referral call when an authorization code security violation occurs.

5. In the **Authorization Code Threshold** field, enter the minimum number of invalid authorization code attempts that you can make before a referral call is made.
6. In the **Time Interval** field, enter the time interval within which the authorization code security violations must occur.
7. In the **Announcement Extension** field, enter an extension that is assigned to an **SVN** authorization code announcement.
8. Administer the **asvn-halt** button on any station/attendant console.

   To determine the location of the SVN button, enter the **`display svn-button-location`** command. Activation of this button stops the placement of authorization code referral calls until the button is deactivated.

Related topics:

Authorization code component field descriptions on page 119

Authorization code component field descriptions

Name	Description
Originating Extension	The originating extension initiates the referral call in the event of an authorization code security violation and also sends the appropriate alerting message or display to the referral destination.
Referral Destination	If the announcement extension field is blank, the referral destination must be on the switch and a display module is required. Using call vectoring and time of day routing, you can extend security notification off-premises.
Authorization Code Threshold	The value assigned to this field, in conjunction with the **Time Interval** field, determines whether a security violation has occurred. The system default for this threshold is 10.
Time Interval	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	The announcement must be recorded for the SVN referral call to be made. A repeating

Name	Description
	announcement is suggested, especially if the SVN referral call might go to an answering machine.

Administering the station security code component

About this task

Users can administer parameters relevant to Station Security Codes on page 2 of the Security-Related System Parameters screen. To administer parameters for station security codes:

Procedure

1. Enter the `change system-parameters security` command.

   The system displays Security-Related System Parameters screen.

   On page 2 of the Security-Related System Parameters screen, the following fields need to be filled.
2. In the **Minimum Station Security Code Length** field, enter station security code from 3 through 8.
3. In the **SVN Station Security Code Violation Notification Enabled?** field, enter `y` to activate, or enter `n` to deactivate the security violation notification for station security codes.
4. In the **Originating Extension** field, you can enter any unassigned extension containing five digits.
5. In the **Referral Destination** field, enter an assigned extension containing 5 digits or `attd` for attendant.
6. In the **Station Security Code Threshold** field, enter a number between 1 and 255. The default code is 10.
7. In the **Time Interval** field, 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.
8. In the **Announcement Extension** field, enter a 5-digit extension to be assigned to the appropriate announcement.

Related topics:

Station security code component field descriptions on page 121

Station security code component field descriptions

Name	Description
Minimum Station Security Code Length	The security code is used to verify all subsequent security code changes. Any existing security code is valid. The default code is **4**.
SVN Station Security Code Violation Notification Enabled?	The default value is **n**.
Originating Extension	The system displays this dynamic field only when the **SVN Station Security Code Violation Enabled** field is set to **y**. When the system makes a Station Security Code SVN Referral call, the extension in this field is internally the originating extension. You cannot use the originating extension as a normal extension.
Referral Destination	The system displays the dynamic field only when the **SVN Station Security Code Violation Notification Enabled** field is set to **y**. When the system makes a station security code SVN referral call, the call is made either to the extension, if provided, in this field or to the attendant, if the value of 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.
Station Security Code Threshold	The system displays this dynamic field only when the **SVN Station Security Code Violation Notification Enabled** field is set to **y**. The value in this field is used in conjunction with the value in the **Time Interval** field. The value in the former field indicates the 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. When the security violation occurs, a station security code SVN referral call is made. Also, invalid attempts are logged, but are ignored unless the count of such attempts exceeds the administered threshold.

Name	Description
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**.
`Announcement Extension`	The system displays this dynamic field only when the corresponding **SVN Violation Notification Enabled** field is set to **y**. This field contains an extension corresponding to a recorded announcement to be played whenever a station security code SVN referral call is made and the referral destination can also be a telephone without a display.

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.

Related topics:

Displaying Remote Access Barrier Code Violations report on page 123

Displaying Remote Access Barrier Code Violations report

Procedure

To display this report, enter the `monitor security-violations remote-access` command.

Displaying Authorization Code Violations report

Procedure

To display this report, enter the `monitor security-violations authorization-code` command.

Displaying Station Security Code (SSC) Violations report

Procedure

To display this report, enter the `monitor security-violations station-security-code` command.

Remote access barrier code aging or access limits

Using the Remote Access Barrier Code Aging feature, the system administrator can specify the time interval during which a barrier code is valid, and the number of times a barrier code can be used to gain access to 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 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 administrator can modify the expiration date to extend the time interval if needed. Once the 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. Ten types of barrier codes, 4 to 7 digits long, are possible. If the Remote Access feature has 10 features, the codes are shared.

Note:

For upgrades, default expiration dates are automatically assigned to barrier codes (one day from the current date and one access). Customers must modify these parameters. If the customers do not modify these parameters, the Remote Access feature will no longer function when the barrier codes expire.

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. For information on administering Barrier Code aging, see
Chapter 4: Product policy controls
.

Viewing Recent Change History report

About this task

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

Procedure

To review the report, enter the`list history` command.

Check for unauthorized changes to security-related features discussed in this guide.

History log

The Recent Change History report or the history log has 500 entries (1800 in larger systems), and provides login and logoff entries. Details such as the date, time, port, and login ID associated with the log-in or log-off are also provided. If available, calling number display information is included.

Note:

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

Malicious call trace

Using Malicious call trace (**MCT**) feature, terminal users can notify a predefined set of users that they might be victims to a malicious call. The users can retrieve certain information related to the call and track the source of the call. The feature also provides for 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, businesses that do not normally experience malicious calls can also benefit from the security tool.

Depending on whether the call originates within the system or outside, 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, activated number, whether the call is active or not, and identification of any additional parties on the call.

You can activate the MCT feature using several methods. For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation Guide, 555-245-205*.

Service observer

When toll fraud is suspected, an authorized person, such as a security supervisor, can use the service observer feature to establish whether an authorized user is on the call. The service observer feature has the option of only listening to a call or listening and talking during the call.

An optional warning tone can be administered on each system 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 feature can be subject to federal, state, or local laws, rules, or regulations and might be prohibited pursuant to the laws, rules, or regulations. The feature can be used only if one of the parties or both the parties to the conversation give consent. Customers must familiarize themselves with and comply with all applicable laws, rules, and regulations before using this feature.

Configuring Service observer

About this task

To configure service observer:

Procedure

1. Enter **`change system-parameters features.`**
   The system displays the **Feature-Related System Parameters** screen.
2. In the **Can be service observed?** or **Can be a service observer?** or both the fields, enter **y**.
3. Enter the **`change station station number`** command, where **`station number`** is the extension number.
   The system displays the **Station** screen.
4. In the **Feature Button Assignment** field, enter **serv-obsrv**.
5. Save and submit the screen.
6. Enter **the `change cor cor number`** command, where **`cor number`** is the Class of Restriction number.
   The system displays the **Class of Restriction** screen.
7. In the **Service Observing** field, enter **y**.

8. Use the **change station** command to assign the associated **CORs** to the observing station and stations that must be observed.

Result

Using the Observe Remotely (remote service observing) feature, you can monitor 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

About this task

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.

Procedure

1. Enter **change station number** command, where **number** is the extension number.

   The system displays the **Station** screen.
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

The **list call-forwarding** command provides the status of stations that have initiated Call Forwarding On Net and Off Net and Call Forwarding Busy/Don’t Answer. The system displays the Call Forwarding initiating station and the call forwarding destination station.

Adjunct-related fraud

With the following monitoring techniques, administrators can detect adjunct-related fraud.

- Call detail recording (CDR). For more information, see Call detail recording and station message detail recording on page 128.
- Traffic measurements and performance. For more information, see SAT reporting on page 106.
- Automatic circuit assurance. For more information, see Configuring Automatic circuit assurance on page 108.
- Busy verification. For more information, see Configuring Busy verification on page 127.
- Call Traffic report. For more information, see Call detail recording and station message detail recording on page 128.
- Trunk Group report. For more information, see Call detail recording and station message detail recording on page 128.
- Traffic reports. For more information, see Traffic reports on page 139.
- Voice session record. For more information, see Voice session records on page 133.

Related topics:

SAT reporting on page 106
Reviewing traffic measurements on page 107
Reviewing performance on page 107
Tracking routine patterns on page 107
Automatic Circuit Assurance on page 107
Configuring Automatic circuit assurance on page 108
Call detail recording and station message detail recording on page 128
Activating the CDR feature on page 129
Call Traffic report on page 129
Trunk Group report on page 130
Recording traffic measurements on page 130

Call detail recording and station message detail recording

If you activate Call Detail Recording (CDR) feature for the incoming trunk groups, you can check the calls in your voice mail and other adjunct ports. A series of short holding times can indicate repeated attempts to enter voice mailbox passwords or similar brute-force attacks on adjunct interfaces.

Note:

Most call accounting packages do not use the security information provided by CDR. If you are using a call accounting package, check if the CDR information can be saved by making

changes in the software. If the CDR information cannot be saved, check the raw data provided 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

Procedure

1. Enter the `change system-parameters cdr` command.

   The system displays the CDR System Parameters screen.
2. Administer the appropriate format to collect the maximum information. The format depends on the capabilities of the CDR analyzing and recording device.
3. Enter the `change trunk-group` *n* command, where *n* is the trunk group number.

   The system displays the Trunk Group screen.
4. In the **CDR Reports** field, enter `y`.

Call Traffic report

The Call Traffic report provides data about hourly port usage and 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

The Trunk Group report tracks call traffic on trunk groups at hourly intervals. As trunk traffic is fairly predictable, you can easily establish the normal usage for each trunk group. Use this report to identify 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. For more information about reports, see *Avaya Aura® Communication Manager Reports, 555-233-505*.

Recording traffic measurements

Procedure

1. Enter `change trunk-group` *n*, where *n* is the trunk group number.
   The Trunk Group screen is displayed.
2. 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.

Reviewing traffic measurements

Procedure

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).

Reviewing performance

Procedure

Enter `list performance` followed by one of the performance types (summary or trunk-group) and the timeframe (yesterday or today).

Tracking routine patterns

About this task

The ARS Measurement Selection feature can monitor up to 25 routing patterns for traffic flow and usage. Use this procedure to track routine patterns:

Procedure

1. Enter `change meas-selection` *route pattern* to choose the routing patterns to track.
2. Enter `list measurements` *route-pattern* with assigned pattern (1-2000) 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).

Automatic Circuit Assurance

This monitoring technique detects a pattern of short holding time calls or a single long holding time call which can indicate attacker activity. Long holding times on trunk-to-trunk calls can be a warning sign. Use the Automatic Circuit Assurance (ACA) feature to establish time limit thresholds that define 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 audio message accompanies the call.

When a notification occurs, determine if the call is still active. If you suspect toll fraud, for example, the designated telephone displays `aca-short` or `aca-long`, use the busy verification feature to monitor the call in progress. For more details see Configuring Busy verification on page 127.

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 an

automated attendant answers the call, an attacker might be attempting to gain access to the system facilities using TACs.

Configuring Automatic circuit assurance

Procedure

1. On the SAT screen, type the command `change system-parameters feature`.

   The systems displays the Features-Related System Parameters screen.
2. In the **Automatic Circuit Assurance (ACA) Enabled** field, enter `y`.
3. In the **ACA Referral Calls** field, enter `local`, `primary`, or `remote`.

   If you select primary, the system can receive calls from other switches. Use remote if the PBX that is administered is a DCS node, perhaps unattended, that wants ACA referral calls to route to an extension or console at another DCS node.
4. Enter appropriate values in the following fields: **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` *n*, where *n* is the trunk group number.

   The system displays the Trunk Group screen.
7. In the **ACA Assignment** field, enter `y`.
8. In the **Long Holding Time (hours)** field, enter the maximum holding time.

   The default value for this field is 1, which means that the maximum holding time is one hour.
9. In the **Short Holding Time (sec)** field, enter the short holding time.

   The default value for this field is 10, which means that the short holding time is 10 seconds.
10. To review an audit trail of the ACA referral call activity, enter `list measurements aca`.

Detection of 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, is transferred 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 entered 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.

The record also reports the session termination method. Each possible termination method is assigned a value as shown in the table on page 133.

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 attended the call
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	Call transferred from an automated attendant to another automated attendant mailbox
11	Call transferred from an automated attendant to a call answer mailbox

Value	Reason for Session Termination
12	Call transfer from an automated attendant to a mailbox with guest greeting

Outgoing voice call detail records

An outgoing call record is created for every outbound call that is originated by the Voice Mail System using a voice port. The record includes call transfers, outcalling, and message waiting activation and deactivation using access codes. Attempts to make calls using the Message Delivery feature are also recorded.

The outgoing voice call detail record provides 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 the table on page 134.

Table 6: Voice Mail System outgoing call type values (continued)

Value	Outgoing Call Type
10	Transfer from voice mail with *T or *0
11	Transfer from voice mail through return call
12	Transfer from call answer with *T, *0 or 0
13	Transfer from automated attendant through menu selection
14	Transfer from automated attendant through extension specification
15	Transfer from automated attendant through 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 or deactivation or both
40	Message delivery

Unsuccessful call transfer attempts can result in multiple records being created for a single session. Review the outgoing voice call detail 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 places not required for business
- Heavy volume of Transfer Out of Voice Mail System calls

Detection of automated attendant toll fraud with related Communication Manager functions

- With the following monitoring techniques, administrators can detect automated attendant toll fraud with related Communication Manager functions.
- Call detail recording. For more information, see Call detail recording on page 135.
- Traffic measurements and performance. For more information, see SAT reporting on page 106.
- Automatic circuit assurance. For more information, see Configuring Automatic circuit assurance on page 108.
- Busy verification. For more information, see Configuring Busy verification on page 127.
- Call Traffic report. For more information, see Call Traffic report on page 129.
- Trunk Group report. For more information, see Trunk Group report on page 130.
- Voice mail System traffic reports. For more information, see Traffic reports on page 139.
- Voice mail System call detail recording. For more information, see Call detail recording on page 139.

Call detail recording for incoming trunk groups

If you activate CDR for the incoming trunk groups, you can monitor the number of calls in your automated attendant ports. For further details, see Security violation notification on page 109.

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

Procedure

1. Enter the `change system-parameters cdr` command.
   The system displays the Features-Related 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. Enter the `change trunk-group` *n* command, where *n* is the trunk group number.
   The system displays the Trunk Group screen.
4. In the **CDR Reports** field, enter `y`.

Call Traffic report

The Call Traffic report provides data about hourly port usage and 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

The Trunk Group report tracks call traffic on trunk groups at hourly intervals. As trunk traffic is fairly predictable, you can easily establish the normal usage for each trunk group. Use this report to identify 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.

For more information about reports, see *Avaya Aura® Communication Manager Reports, 555-233-505*.

Recording traffic measurements

Procedure

1. Enter `change trunk-group` *n*, where *n* is the trunk group number.
   The Trunk Group screen is displayed.
2. 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.

Reviewing traffic measurements

Procedure

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).

Reviewing performance

Procedure

Enter `list performance` followed by one of the performance types (summary or trunk-group) and the timeframe (yesterday or today).

Tracking routine patterns

About this task

The ARS Measurement Selection feature can monitor up to 25 routing patterns for traffic flow and usage. Use this procedure to track routine patterns:

Procedure

1. Enter `change meas-selection` *route pattern* to choose the routing patterns to track.
2. Enter `list measurements` *route-pattern* with assigned pattern (1-2000) 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).

Automatic Circuit Assurance

This monitoring technique detects a pattern of short holding time calls or a single long holding time call which can indicate attacker activity. Long holding times on trunk-to-trunk calls can be a warning sign. Use the Automatic Circuit Assurance (ACA) feature to establish time limit thresholds that define 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 audio message accompanies the call.

When a notification occurs, determine if the call is still active. If you suspect toll fraud, for example, the designated telephone displays `aca-short` or `aca-long`, use the busy verification feature to monitor the call in progress. For more details see Configuring Busy verification on page 127.

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 an automated attendant answers the call, an attacker might be attempting to gain access to the system facilities using TACs.

Configuring Automatic circuit assurance

Procedure

1. On the SAT screen, type the command `change system-parameters feature`.

   The systems displays the Features-Related System Parameters screen.
2. In the **Automatic Circuit Assurance (ACA) Enabled** field, enter `y`.
3. In the **ACA Referral Calls** field, enter `local`, `primary`, or `remote`.

If you select primary, the system can receive calls from other switches. Use remote if the PBX that is administered is a DCS node, perhaps unattended, that wants ACA referral calls to route to an extension or console at another DCS node.

4. Enter appropriate values in the following fields: **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` *n*, where *n* is the trunk group number.

   The system displays the Trunk Group screen.
7. In the **ACA Assignment** field, enter `y`.
8. In the **Long Holding Time (hours)** field, enter the maximum holding time.

   The default value for this field is 1, which means that the maximum holding time is one hour.
9. In the **Short Holding Time (sec)** field, enter the short holding time.

   The default value for this field is 10, which means that the short holding time is 10 seconds.
10. To review an audit trail of the ACA referral call activity, enter `list measurements aca`.

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.

Optional 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 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, is transferred 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 entered 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.

The record also reports the session termination method. Each possible termination method is assigned a value as shown in the table on page 140.

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 attended the call
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	Call transferred from an automated attendant to another automated attendant mailbox
11	Call transferred from an automated attendant to a call answer mailbox
12	Call transfer from an automated attendant to a mailbox with guest greeting

Outgoing voice call detail records

An outgoing call record is created for every outbound call that is originated by the Voice Mail System using a voice port. The record includes call transfers, outcalling, and message waiting activation and deactivation using access codes. Attempts to make calls using the Message Delivery feature are also recorded.

The outgoing voice call detail record provides 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 the table on page 141.

Table 8: Voice Mail System outgoing call type values (continued)

Value	Outgoing Call Type
10	Transfer from voice mail with *T or *0
11	Transfer from voice mail through return call
12	Transfer from call answer with *T, *0 or 0
13	Transfer from automated attendant through menu selection
14	Transfer from automated attendant through extension specification
15	Transfer from automated attendant through 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 or deactivation or both
40	Message delivery

Unsuccessful call transfer attempts can result in multiple records being created for a single session. Review the outgoing voice call detail 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 places not required for business
- Heavy volume of Transfer Out of Voice Mail System calls

Avaya Modular Messaging Report tool

Modular Messaging report tool provides several monitoring functions to review and track various activities within the messaging system. The Modular Messaging reporting tool is one of the most common tools used for Toll Fraud Detection and 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. Customers must investigate the possibility of active toll fraud when any combination of the following situations become common:

- 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.
- The system reports an increase in short duration calls.
- A significant increase in internal requests for operator assistance in making outbound calls, particularly international calls.
- The system experiences heavy call volume during the night-time and weekend hours.
- The system records 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 system memory customer premises equipment-based system memory.
- Unusual increase in the number of subscribers with locked mailboxes.
- Unexplained changes in system software parameters.
- Subscribers discover that a personal greeting is changed or receive suspicious messages.

Avaya technical and toll fraud crisis intervention

If you suspect any toll fraud or service theft and need technical support or help, goto the Avaya Support website at http://support.avaya.com for current documentation, product notices, knowledge articles related to the topic, or to open a service request. These services are available 24 hours a day, 365 days a year. Consultation charges might apply.

You can send information regarding any security problems that you have discovered in Avaya products to either the contact provided in the product documentation or to securityalerts@avaya.com.

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

Toll fraud detection for Call Management System

Toll fraud rarely occurs through a CMS system. However, using CMS reports you can detect potential toll fraud. You must review vector reports to ensure unauthorized vector changes are not made. You must also review Access logs and role assignments to ensure that only authorized users can gain access to the system and 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. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, knowledge articles related to the topic, or to open a service request.

Security Hardening Services

The Security Tune-Up Service is a fee-based, consultative service designed to provide an expedient, online review of your system security to prevent toll fraud.

Customer support engineers specializing in security will remotely access your system, analyze the potential risks in the system, and implement agreed-upon changes to secure the system.

For more information, call **1 800 643-2353.**

Toll fraud contact list

Contact:	**For:**
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

Appendix B: PCN and PSN notifications

Avaya issues a product-change notice (PCN) in case of any software update. For example, a PCN must accompany a service pack or a patch that needs to be applied universally. Avaya issues product-support notice (PSN) when there is no patch, service pack, or release fix, but the business unit or services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a workaround for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.

   Note:

   If the Avaya Support website displays the login page, enter your SSO login credentials.

2. On the top of the page, click **DOWNLOADS & DOCUMENTS**.
3. On the Downloads & Documents page, in the **Enter Your Product Here** field, enter the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select **Documents** as the content type.
6. Select the appropriate filters as per your search requirement. For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   Note:

   You can apply multiple filters to search for the required documents.

Related topics:

Signing up for PCNs and PSNs on page 148

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. The Avaya E-Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: eNotifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications.

   For detailed information, see the **How to set up your E-Notifications** procedure.

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W