Avaya Solution & Interoperability Test Lab

Application Notes for Bristol Capital Security Audit with Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe the steps required for Bristol Capital Security Audit to successfully interoperate with Avaya Aura® Communication Manager 6.0.1.

Bristol Capital Security Audit is a PBX management service. In the compliance testing, Bristrol Capital Security Audit used the System Administrator Terminal interface to obtain security related data and provide report on the security aspects of Avaya Aura® Communication Manager.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps required for Bristol Capital Security Audit to successfully interoperate with Avaya Aura® Communication Manager 6.0.1.

Bristol Capital Security Audit is a PBX management service. In the compliance testing, Bristol Capital Security Audit used the System Administrator Terminal (SAT) interface to obtain security related data and provide report on the security aspects of Avaya Aura® Communication Manager.

The Bristol Capital Security Audit service consists of a server and a central database. The Bristol Capital Security Audit server connects remotely to Avaya Aura® Communication Manager via the SAT interface, and uses a subset of the SAT commands to collect inventory related data. The collected data are passed to the central database for analysis and reporting.

The remote connectivity between Bristol Capital Security Audit and Avaya Aura® Communication Manager can be accomplished using either modem dial-up to the Avaya Server Availability Management Processor (SAMP) interface, VPN tunneling, or direct access from the public network. In the compliance testing, the direct access method from the public network was used.

In the direct access via the public network method used in the compliance testing, a spare and existing C-LAN circuit pack from Avaya Aura® Communication Manager was connected to the public network, and with the corporate firewall configured to allow traffic from the public IP address of the Bristol Capital Security Audit server. The public IP address of the C-LAN circuit pack and the SAT login credentials were passed on to Bristol Capital prior to test.

Note that the corporate firewall configuration and the configuration of the Bristol Capital Security Audit service are outside the scope of these Application Notes, and will not be described.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Security related data were manually configured on Avaya Aura® Communication Manager, and automatically collected by Bristol Capital Security Audit.

The report produced by Bristol Capital Security Audit was reviewed manually and compared with the data on Avaya Aura® Communication Manager for proper representation.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the proper collection and reporting of security data by the Bristol Capital Security Audit service. The collected security data included configuration, coverage paths, capacity, system parameters, trunk groups, attendants, hunt groups, locations, ARS analysis, AAR analysis, report scheduler, class of services, abbreviated dialing lists, route patterns, authorization codes, feature access codes, remote access, time of day, coverage remote groups, listed directory numbers, vectors, alternate FRL, trunk group measurements, route pattern measurements, tenants, ASG history, VDNs, data modules, ARS digit conversions, AAR digit conversions, class of restrictions, profiles, dial plan parameters, audio groups, software versions, stations, partition groups, partition tables, toll, call forwarding, off PBX station mapping, cabinet, media gateway, IP network region, console parameters, dial plan analysis, IP services, system parameters, extension type, node names, and UNIX users/groups/authorizations.

The serviceability testing focused on verifying the ability of Bristol Capital Security Audit to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable from the Bristol Capital Security Audit server.

2.2. Test Results

All test cases were executed and verified. The following were the observations from the compliance testing.

- The Service Observe Feature section did not include Service Observing No Talk Access Code and Allow Two Observers in Same Call.
- The Critical Feature Access Codes section did not include Abbreviated Dial Prgm Group List Access Code.
- The Digit Manipulation section will interpret route patterns with "0" deleted digits and no inserted digits as a route pattern that manipulated data.

2.3. Support

Technical support on Bristol Security Audit can be obtained through the following:

- **Phone:** (201) 476-0600
- **Email:** support@infoplusonline.com

3. Reference Configuration

The configuration used for the compliance testing is shown below.

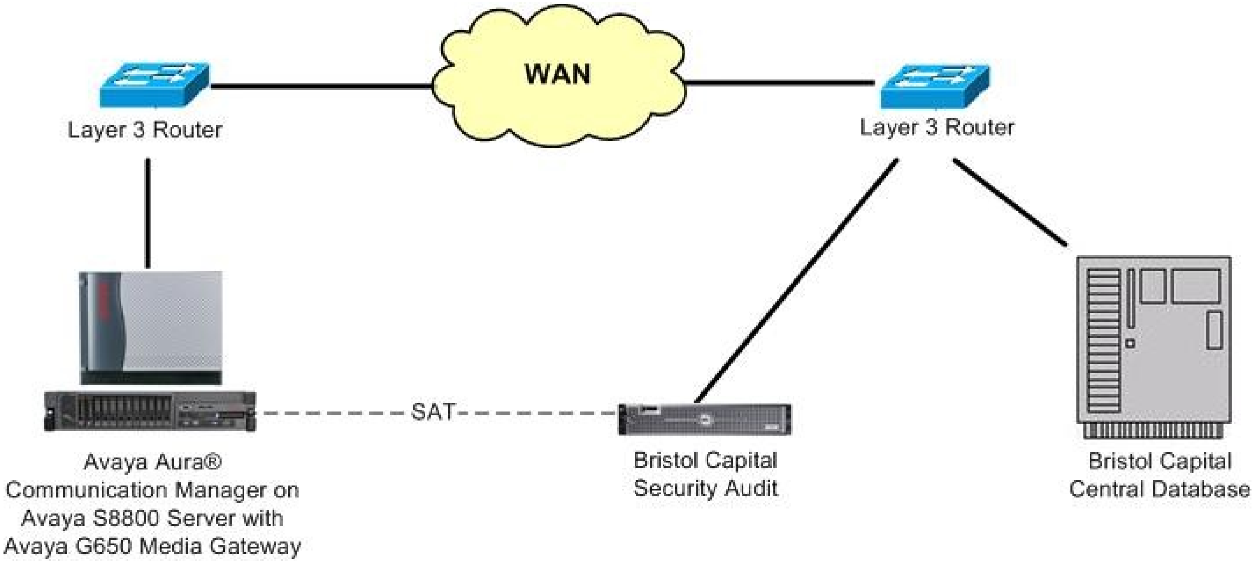

WAN
Layer 3 Router
Layer 3 Router
SAT
Avaya Aura® Communication Manager on Avaya S8800 Server with Avaya G650 Media Gateway
Bristol Capital Security Audit
Bristol Capital Central Database

Figure 1: Configuration Diagram

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 SP5.01 (R016x.00.1.510.1-19303)
Avaya G650 Media Gateway • TN799DP C-LAN Circuit Pack	 HW01 FW040
Bristol Capital Security Audit	Build 10507

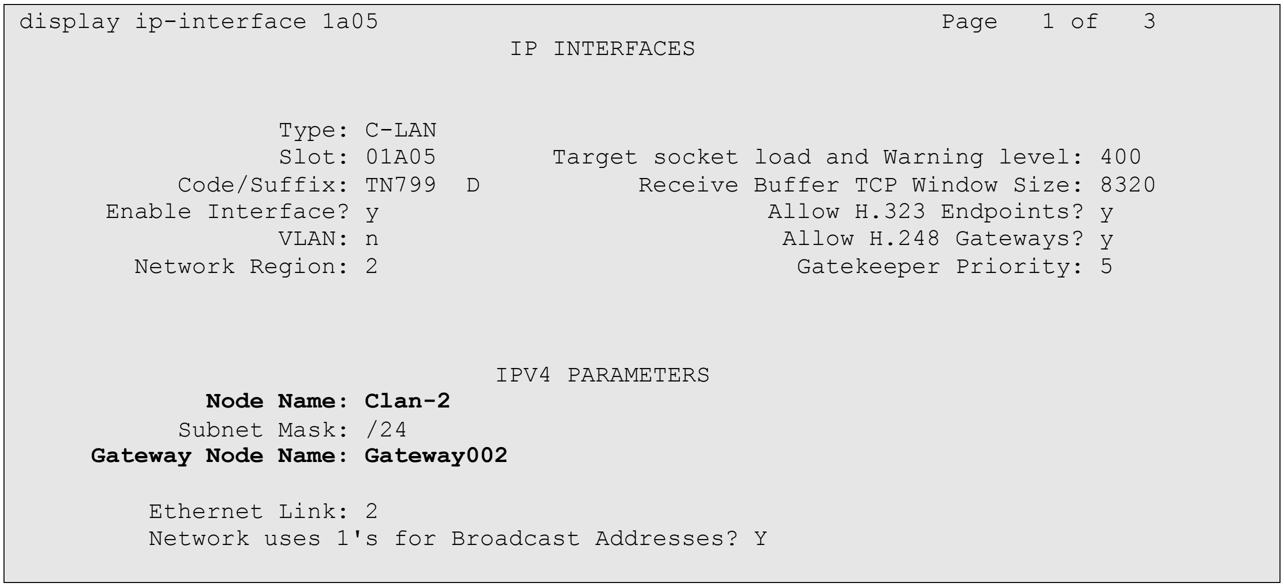
5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Obtain node names
- Administer node names
- Administer IP services

5.1. Obtain Node Names

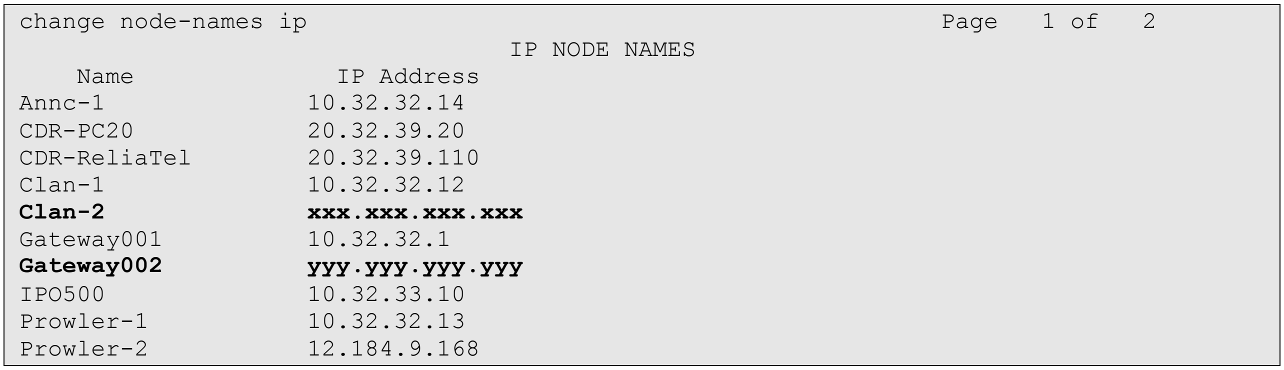
Log in to the SAT with proper credentials. Use the "display ip-interface x" command, where "x" is the location of an existing C-LAN circuit pack that will be used to connect to the public network. Note the values in the **Node Name** and **Gateway Node Name** fields.



```
display ip-interface 1a05                                       Page   1 of   3
                                  IP INTERFACES


                  Type: C-LAN
                  Slot: 01A05        Target socket load and Warning level: 400
           Code/Suffix: TN799  D           Receive Buffer TCP Window Size: 8320
      Enable Interface? y                           Allow H.323 Endpoints? y
                  VLAN: n                            Allow H.248 Gateways? y
        Network Region: 2                             Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: Clan-2
           Subnet Mask: /24
     Gateway Node Name: Gateway002

         Ethernet Link: 2
         Network uses 1's for Broadcast Addresses? Y
```

5.2. Administer Node Names

Use the “change node-names ip” command to modify the IP address of the C-LAN circuit pack from **Section 5.1**, and the IP address of the associated gateway. In this case, the C-LAN node name is “Clan-2”, and the associated gateway node name is “Gateway002”. Enter the appropriate public IP addresses for these two entries to match the network configuration. The public IP addresses for the entries are masked in the screen below for privacy.

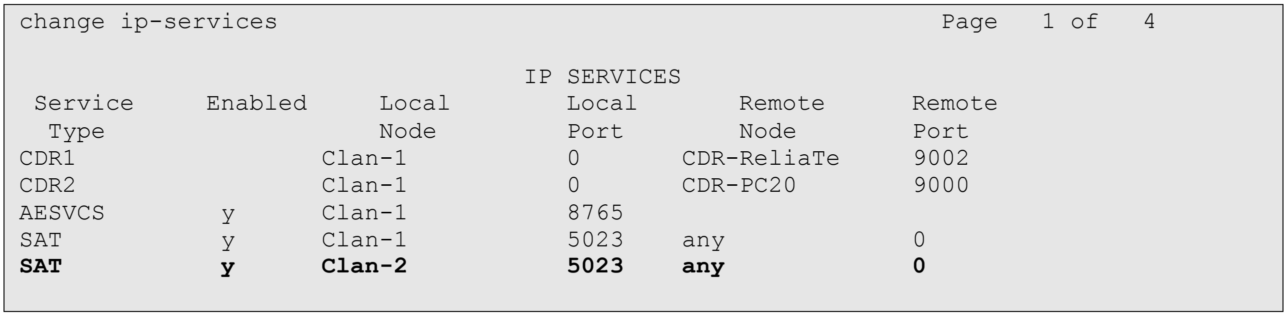


```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
Annc-1              10.32.32.14
CDR-PC20            20.32.39.20
CDR-ReliaTel        20.32.39.110
Clan-1              10.32.32.12
Clan-2              xxx.xxx.xxx.xxx
Gateway001          10.32.32.1
Gateway002          yyy.yyy.yyy.yyy
IPO500              10.32.33.10
Prowler-1           10.32.32.13
Prowler-2           12.184.9.168
```

5.3. Administer IP Services

Use the “change ip-services” command to add an entry to allow SAT access via the public facing C-LAN circuit pack. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Service Type:** “SAT”
- **Enabled:** “y”
- **Local Node:** Node name of the public facing C-LAN circuit pack from **Section 5.2**.
- **Local Port:** “5023”
- **Remote Node:** “any”
- **Remote Port:** “0”



```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
CDR1                 Clan-1           0       CDR-ReliaTe     9002
CDR2                 Clan-1           0       CDR-PC20        9000
AESVCS        y      Clan-1           8765
SAT           y      Clan-1           5023    any             0
SAT           y      Clan-2           5023    any             0
```

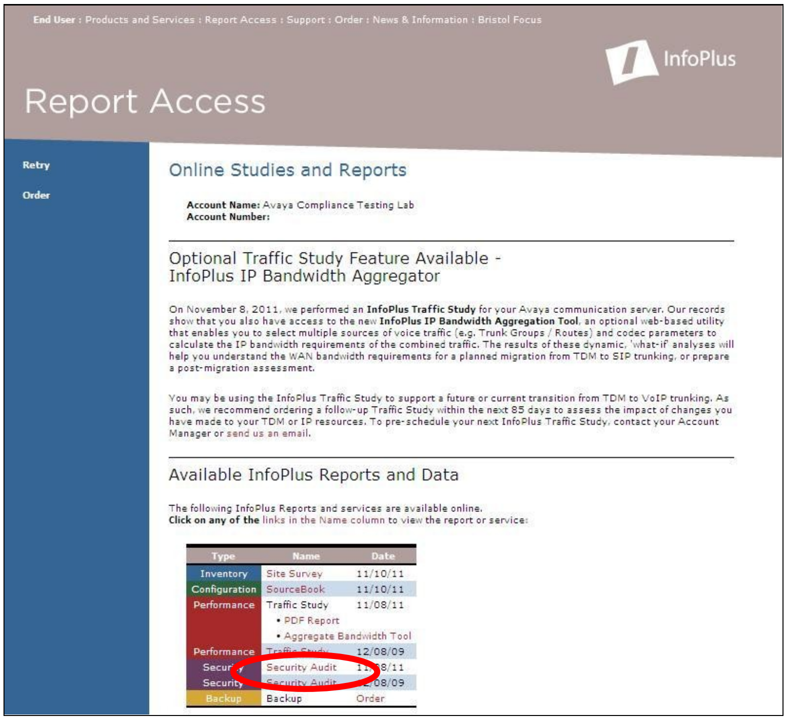
6. Navigate Bristol Capital Security Audit Report

This section provides the procedures for navigating the Bristol Capital Security Audit report. The procedures include the following areas:

- Access report
- Review administrative access
- Review system configuration
- Review assessing and measuring abuse
- Review stations
- Review trunking
- Review controlling calling privileges
- Review controlling feature access
- Review remote access
- Review call routing
- Review voice mail ports
- Review voice recognition units
- Review vectors and vector directory numbers

6.1. Access Report

At the conclusion of the inventory data collection and analysis, the Bristol Capital Security Audit service will send an automatic email notification to the customer, including a URL to access the online report. From an Internet browser window, enter the URL from the email notification to display the **Report Access** screen below. Select **Security Audit**.


End User : Products and Services : Report Access : Support : Order : News & Information : Bristol Focus
InfoPlus
Report Access
Retry
Order

Online Studies and Reports

Account Name: Avaya Compliance Testing Lab
Account Number:

Optional Traffic Study Feature Available -
InfoPlus IP Bandwidth Aggregator

On November 8, 2011, we performed an **InfoPlus Traffic Study** for your Avaya communication server. Our records show that you also have access to the new **InfoPlus IP Bandwidth Aggregation Tool**, an optional web-based utility that enables you to select multiple sources of voice traffic (e.g. Trunk Groups / Routes) and codec parameters to calculate the IP bandwidth requirements of the combined traffic. The results of these dynamic, 'what-if' analyses will help you understand the WAN bandwidth requirements for a planned migration from TDM to SIP trunking, or prepare a post-migration assessment.

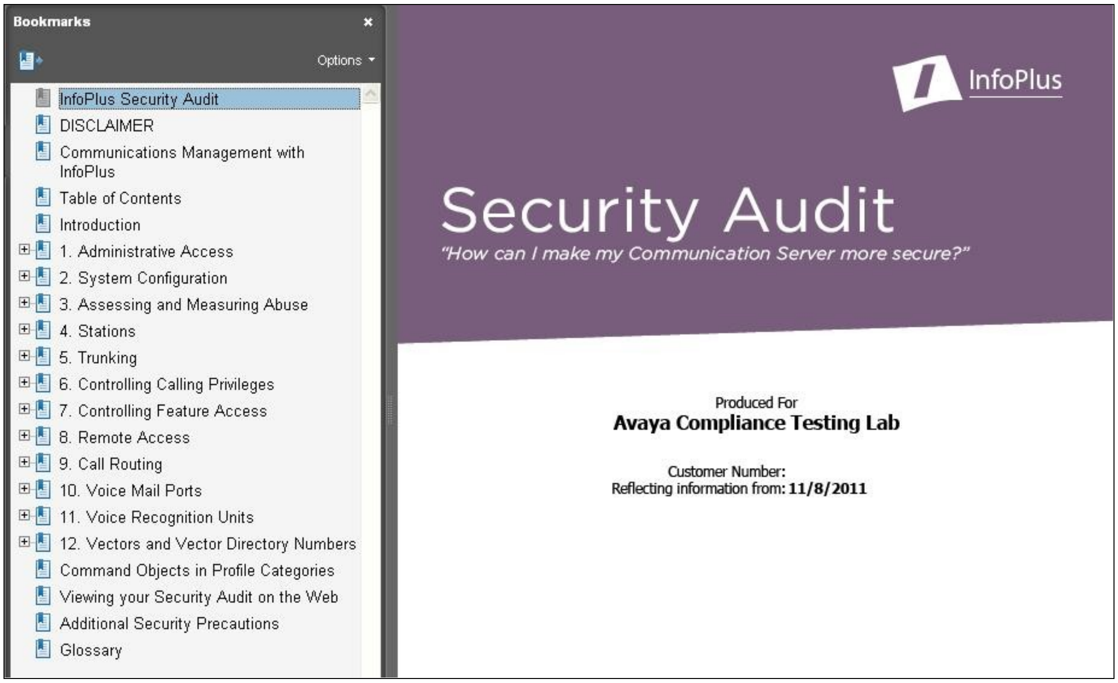
You may be using the InfoPlus Traffic Study to support a future or current transition from TDM to VoIP trunking. As such, we recommend ordering a follow-up Traffic Study within the next 85 days to assess the impact of changes you have made to your TDM or IP resources. To pre-schedule your next InfoPlus Traffic Study, contact your Account Manager or send us an email.

Available InfoPlus Reports and Data

The following InfoPlus Reports and services are available online.
Click on any of the links in the Name column to view the report or service:

Type	Name	Date
Inventory	Site Survey	11/10/11
Configuration	SourceBook	11/10/11
Performance	Traffic Study	11/08/11
	• PDF Report	
	• Aggregate Bandwidth Tool	
Performance	Traffic Study	12/08/09
Security	Security Audit	11/08/11
Security	Security Audit	12/08/09
Backup	Backup	Order

The **Security Audit** report is displayed.


Bookmarks
Options
InfoPlus Security Audit
DISCLAIMER
Communications Management with InfoPlus
Table of Contents
Introduction
1. Administrative Access
2. System Configuration
3. Assessing and Measuring Abuse
4. Stations
5. Trunking
6. Controlling Calling Privileges
7. Controlling Feature Access
8. Remote Access
9. Call Routing
10. Voice Mail Ports
11. Voice Recognition Units
12. Vectors and Vector Directory Numbers
Command Objects in Profile Categories
Viewing your Security Audit on the Web
Additional Security Precautions
Glossary
InfoPlus

Security Audit

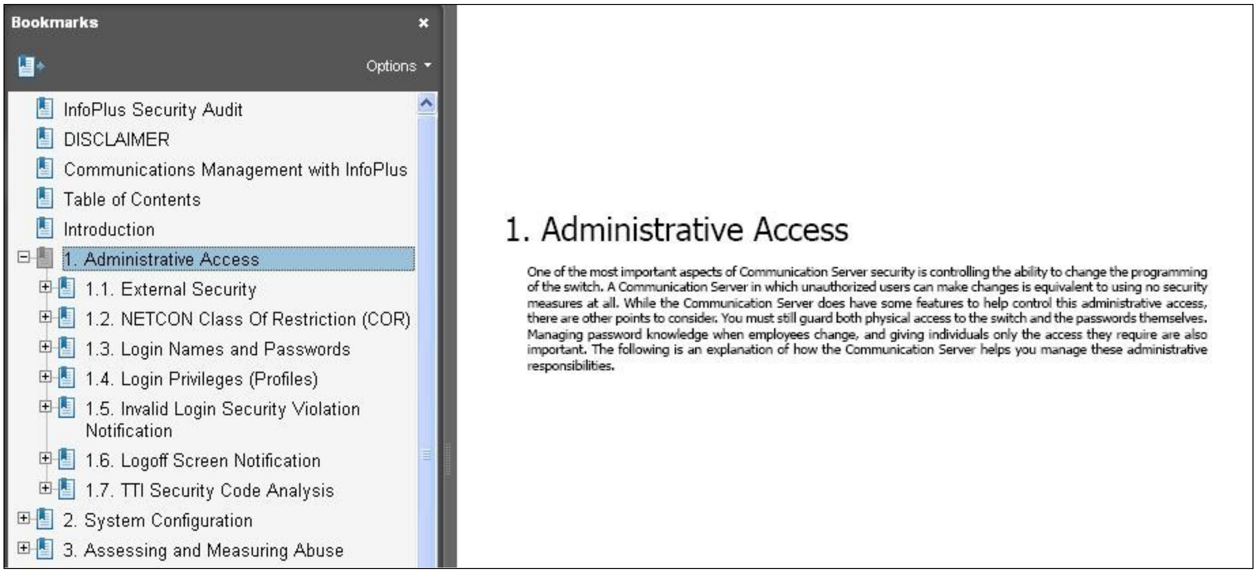
"How can I make my Communication Server more secure?"

Produced For
Avaya Compliance Testing Lab

Customer Number:
Reflecting information from: **11/8/2011**

6.2. Review Administrative Access

Select **Administrative Access** from the left pane, to display the **Administrative Access** section. This section provides information on the administrative access aspects of the system including external security, NETCON class of restriction, login names and passwords, login profiles, invalid login security violation notification, logoff screen notification, and Terminal Translation Initialization (TTI) code analysis.

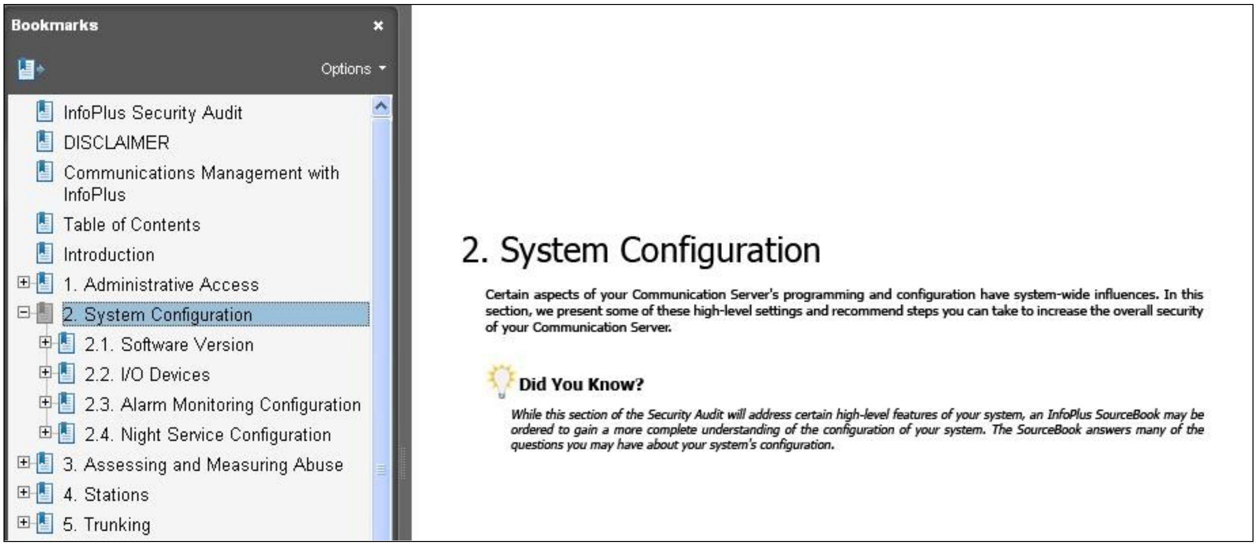

Bookmarks
Options
InfoPlus Security Audit
DISCLAIMER
Communications Management with InfoPlus
Table of Contents
Introduction
1. Administrative Access
1.1. External Security
1.2. NETCON Class Of Restriction (COR)
1.3. Login Names and Passwords
1.4. Login Privileges (Profiles)
1.5. Invalid Login Security Violation Notification
1.6. Logoff Screen Notification
1.7. TTI Security Code Analysis
2. System Configuration
3. Assessing and Measuring Abuse

1. Administrative Access

One of the most important aspects of Communication Server security is controlling the ability to change the programming of the switch. A Communication Server in which unauthorized users can make changes is equivalent to using no security measures at all. While the Communication Server does have some features to help control this administrative access, there are other points to consider. You must still guard both physical access to the switch and the passwords themselves. Managing password knowledge when employees change, and giving individuals only the access they require are also important. The following is an explanation of how the Communication Server helps you manage these administrative responsibilities.

6.3. Review System Configuration

Select **System Configuration** from the left pane, to display the **System Configuration** section. This section provides the system high level settings, including software version, input and output devices, alarm monitoring configuration, and night service configuration.



2. System Configuration

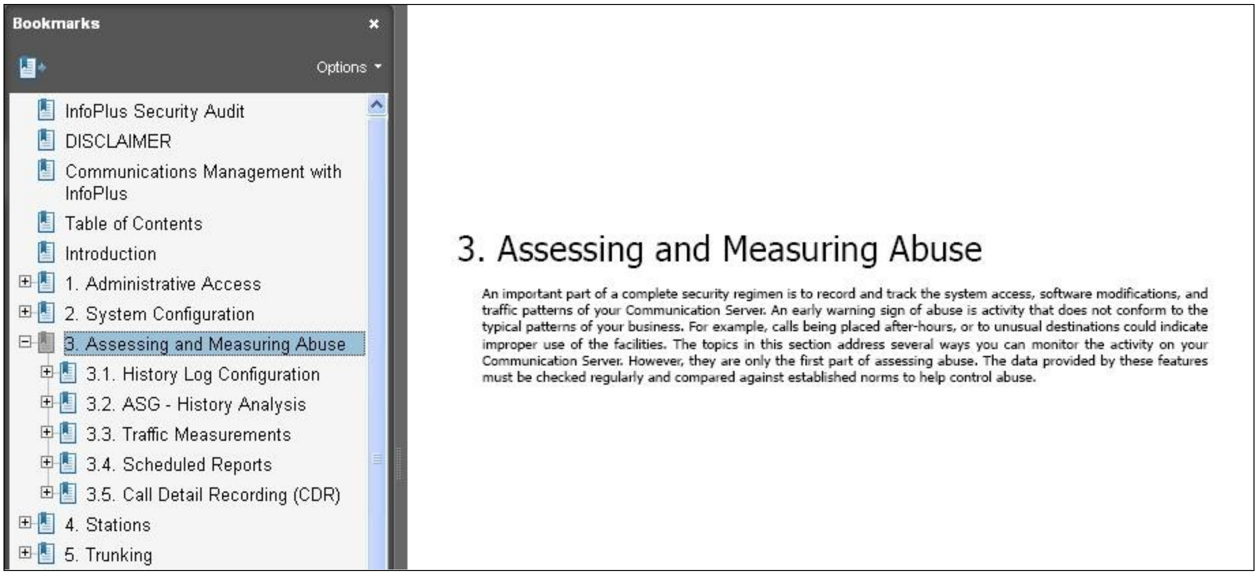
Certain aspects of your Communication Server's programming and configuration have system-wide influences. In this section, we present some of these high-level settings and recommend steps you can take to increase the overall security of your Communication Server.

Did You Know?

While this section of the Security Audit will address certain high-level features of your system, an InfoPlus SourceBook may be ordered to gain a more complete understanding of the configuration of your system. The SourceBook answers many of the questions you may have about your system's configuration.

6.4. Review Assessing and Measuring Abuse

Select **Assessing and Measuring Abuse** from the left pane, to display the **Assessing and Measuring Abuse** section. This section provides details on the system access and usage, including history log configuration, ASG history analysis, traffic measurements, scheduled reports, and call detailed recording.

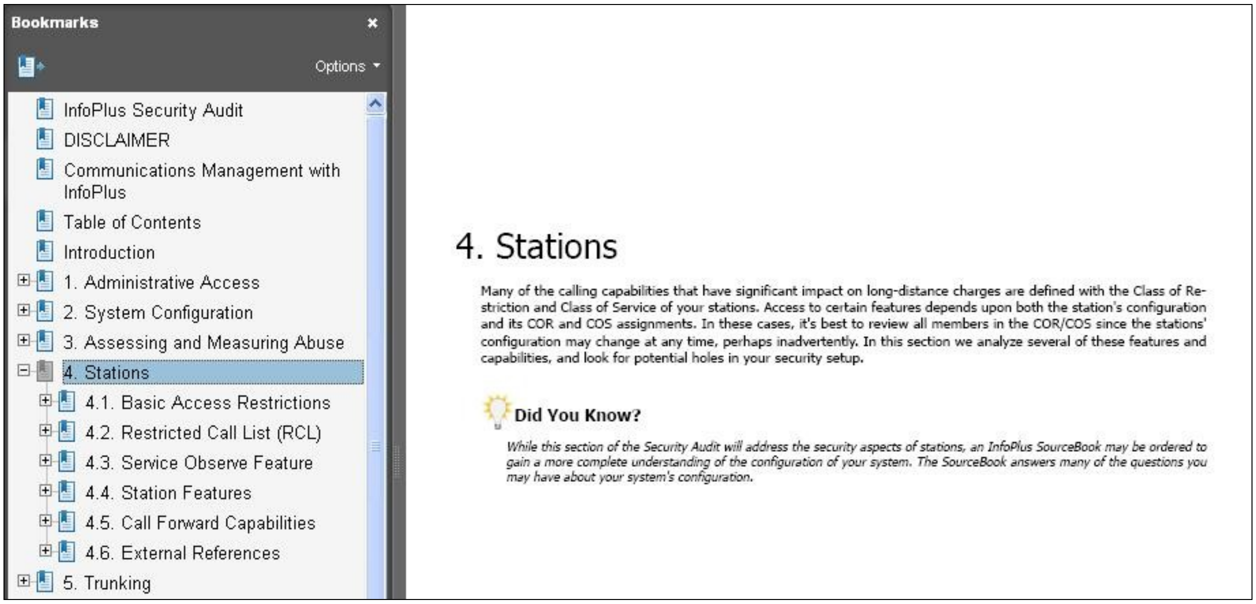

Bookmarks
Options
InfoPlus Security Audit
DISCLAIMER
Communications Management with InfoPlus
Table of Contents
Introduction
1. Administrative Access
2. System Configuration
3. Assessing and Measuring Abuse
3.1. History Log Configuration
3.2. ASG - History Analysis
3.3. Traffic Measurements
3.4. Scheduled Reports
3.5. Call Detail Recording (CDR)
4. Stations
5. Trunking

3. Assessing and Measuring Abuse

An important part of a complete security regimen is to record and track the system access, software modifications, and traffic patterns of your Communication Server. An early warning sign of abuse is activity that does not conform to the typical patterns of your business. For example, calls being placed after-hours, or to unusual destinations could indicate improper use of the facilities. The topics in this section address several ways you can monitor the activity on your Communication Server. However, they are only the first part of assessing abuse. The data provided by these features must be checked regularly and compared against established norms to help control abuse.

6.5. Review Stations

Select **Stations** from the left pane, to display the **Stations** section. This section provides detailed station information that can have significant impact on long distance charges, including access restrictions, restricted call list, service observe feature, station features, call forward capabilities, and external redirections.



4. Stations

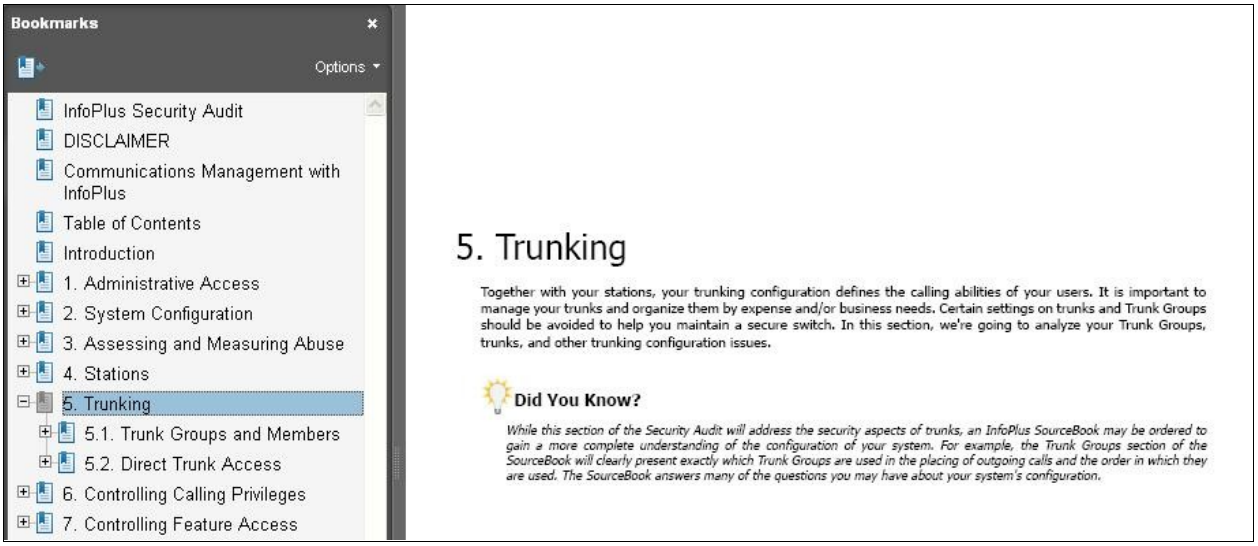
Many of the calling capabilities that have significant impact on long-distance charges are defined with the Class of Restriction and Class of Service of your stations. Access to certain features depends upon both the station's configuration and its COR and COS assignments. In these cases, it's best to review all members in the COR/COS since the stations' configuration may change at any time, perhaps inadvertently. In this section we analyze several of these features and capabilities, and look for potential holes in your security setup.

Did You Know?

While this section of the Security Audit will address the security aspects of stations, an InfoPlus SourceBook may be ordered to gain a more complete understanding of the configuration of your system. The SourceBook answers many of the questions you may have about your system's configuration.

6.6. Review Trunking

Select **Trunking** from the left pane, to display the **Trunking** section. This section provides detailed trunking analysis, including trunk groups and members, and direct trunk access.



5. Trunking

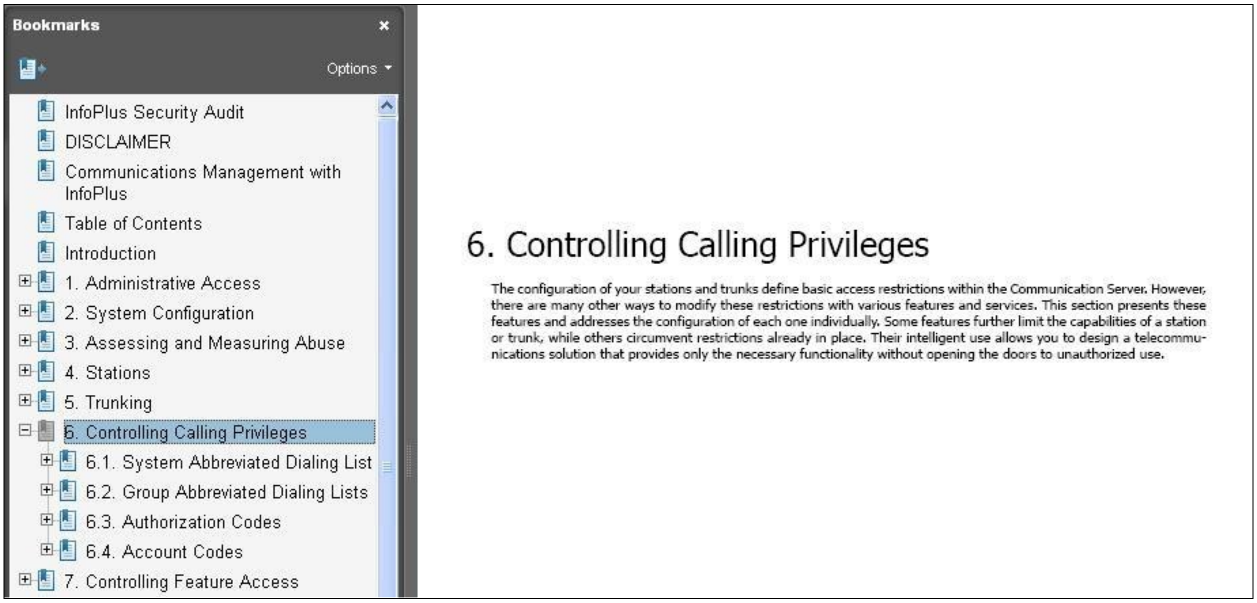
Together with your stations, your trunking configuration defines the calling abilities of your users. It is important to manage your trunks and organize them by expense and/or business needs. Certain settings on trunks and Trunk Groups should be avoided to help you maintain a secure switch. In this section, we're going to analyze your Trunk Groups, trunks, and other trunking configuration issues.

Did You Know?

While this section of the Security Audit will address the security aspects of trunks, an InfoPlus SourceBook may be ordered to gain a more complete understanding of the configuration of your system. For example, the Trunk Groups section of the SourceBook will clearly present exactly which Trunk Groups are used in the placing of outgoing calls and the order in which they are used. The SourceBook answers many of the questions you may have about your system's configuration.

6.7. Review Controlling Calling Privileges

Select **Controlling Calling Privileges** from the left pane, to display the **Controlling Calling Privileges** section. This section provides detailed information relating to calling privileges, including abbreviated dialing system list, abbreviated dialing group lists, authorization codes, and account codes.

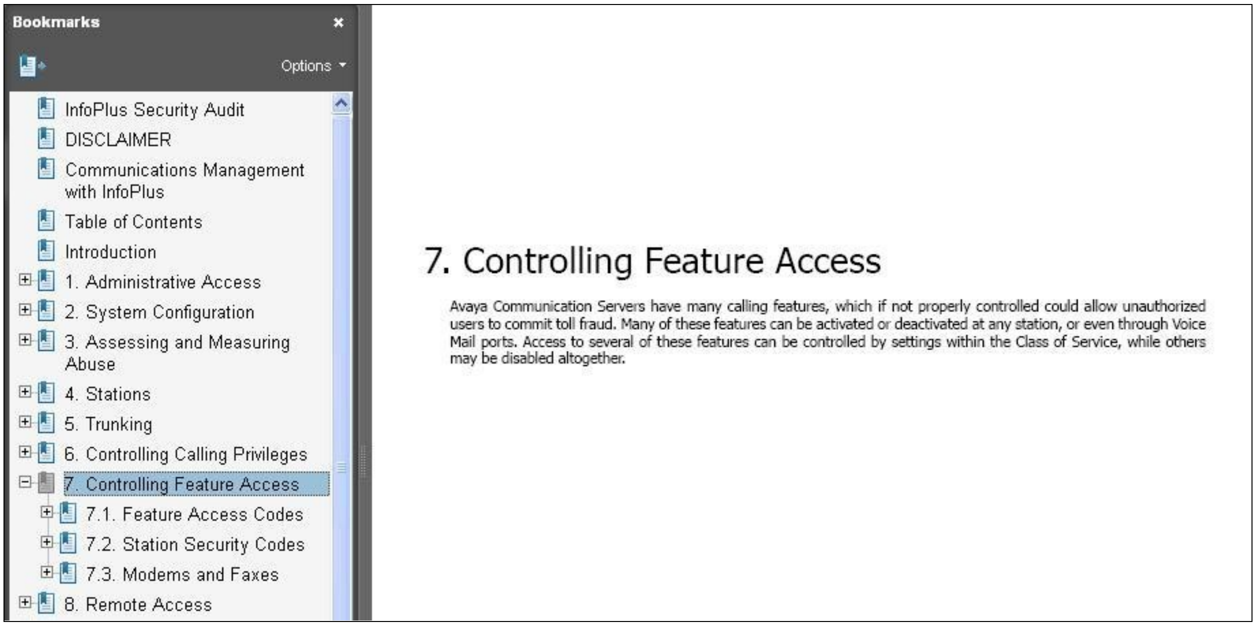

Bookmarks
×
Options
InfoPlus Security Audit
DISCLAIMER
Communications Management with InfoPlus
Table of Contents
Introduction
1. Administrative Access
2. System Configuration
3. Assessing and Measuring Abuse
4. Stations
5. Trunking
6. Controlling Calling Privileges
6.1. System Abbreviated Dialing List
6.2. Group Abbreviated Dialing Lists
6.3. Authorization Codes
6.4. Account Codes
7. Controlling Feature Access

6. Controlling Calling Privileges

The configuration of your stations and trunks define basic access restrictions within the Communication Server. However, there are many other ways to modify these restrictions with various features and services. This section presents these features and addresses the configuration of each one individually. Some features further limit the capabilities of a station or trunk, while others circumvent restrictions already in place. Their intelligent use allows you to design a telecommunications solution that provides only the necessary functionality without opening the doors to unauthorized use.

6.8. Review Controlling Feature Access

Select **Controlling Feature Access** from the left pane, to display the **Controlling Feature Access** section. This section provides detailed feature settings, including feature access codes, station security codes, modems and faxes.

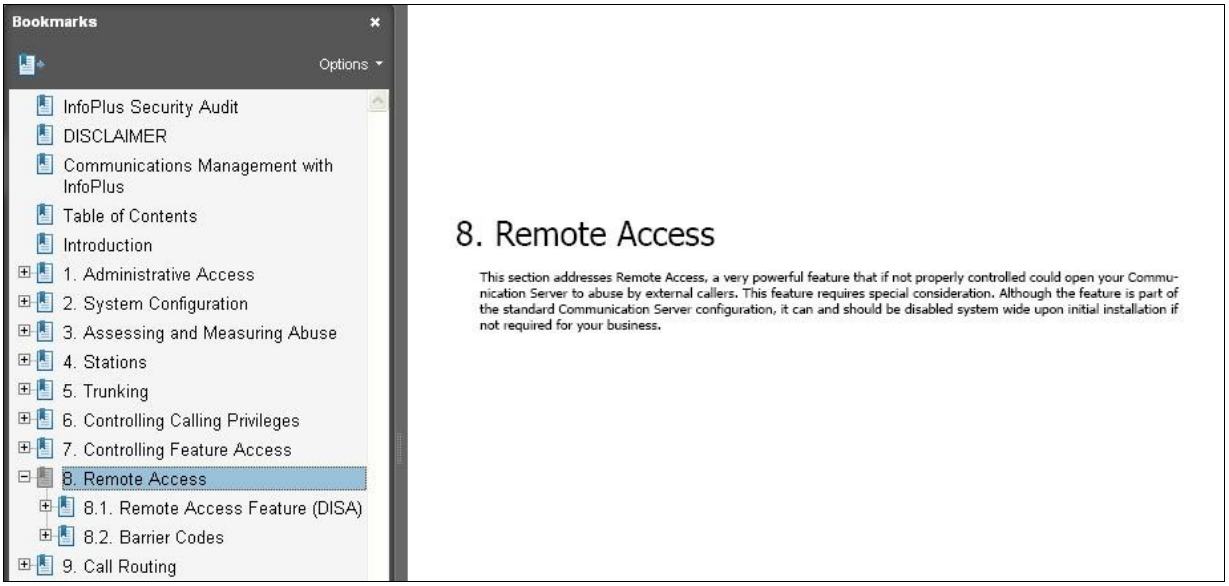

Bookmarks
×
Options
InfoPlus Security Audit
DISCLAIMER
Communications Management with InfoPlus
Table of Contents
Introduction
1. Administrative Access
2. System Configuration
3. Assessing and Measuring Abuse
4. Stations
5. Trunking
6. Controlling Calling Privileges
7. Controlling Feature Access
7.1. Feature Access Codes
7.2. Station Security Codes
7.3. Modems and Faxes
8. Remote Access

7. Controlling Feature Access

Avaya Communication Servers have many calling features, which if not properly controlled could allow unauthorized users to commit toll fraud. Many of these features can be activated or deactivated at any station, or even through Voice Mail ports. Access to several of these features can be controlled by settings within the Class of Service, while others may be disabled altogether.

6.9. Review Remote Access

Select **Remote Access** from the left pane, to display the **Remote Access** section. This section provides detailed remote access settings, including the remote access feature and barrier codes.

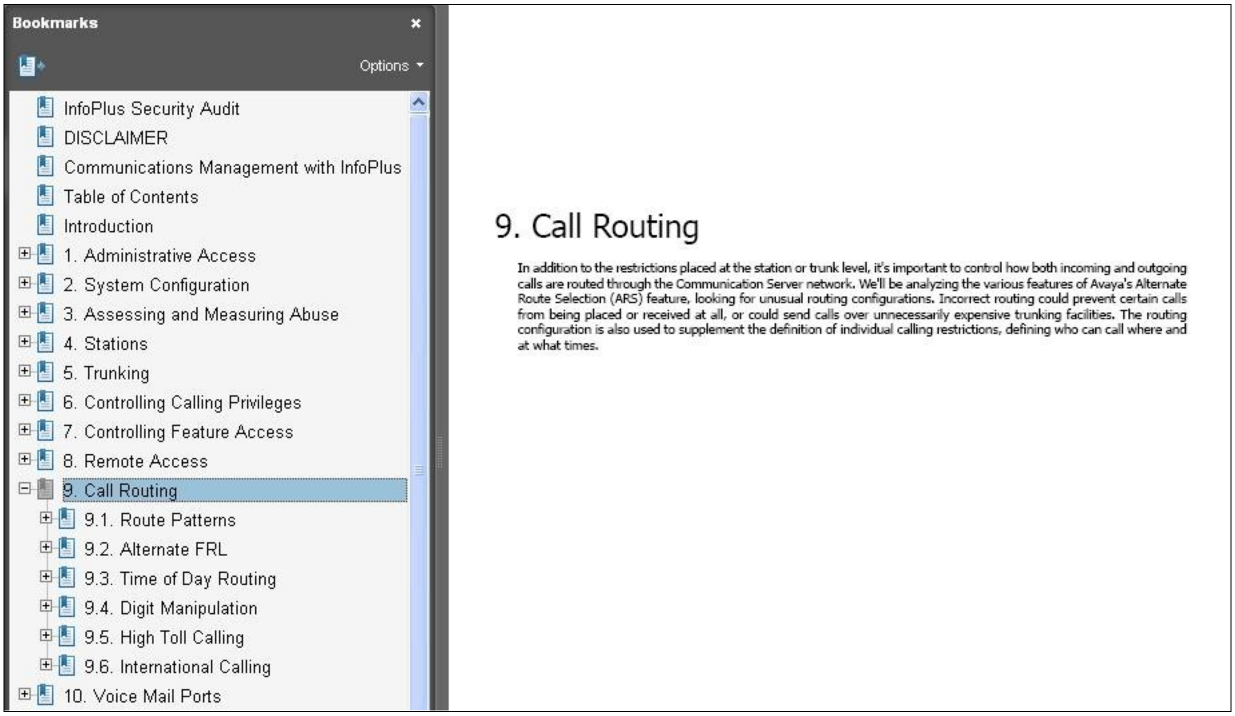


8. Remote Access

This section addresses Remote Access, a very powerful feature that if not properly controlled could open your Communication Server to abuse by external callers. This feature requires special consideration. Although the feature is part of the standard Communication Server configuration, it can and should be disabled system wide upon initial installation if not required for your business.

6.10. Review Call Routing

Select **Call Routing** from the left pane, to display the **Call Routing** section. This section provides detailed call routing configurations, including route patterns, alternate FRL, time of day routing, digit manipulation, high toll calling, and international calling.

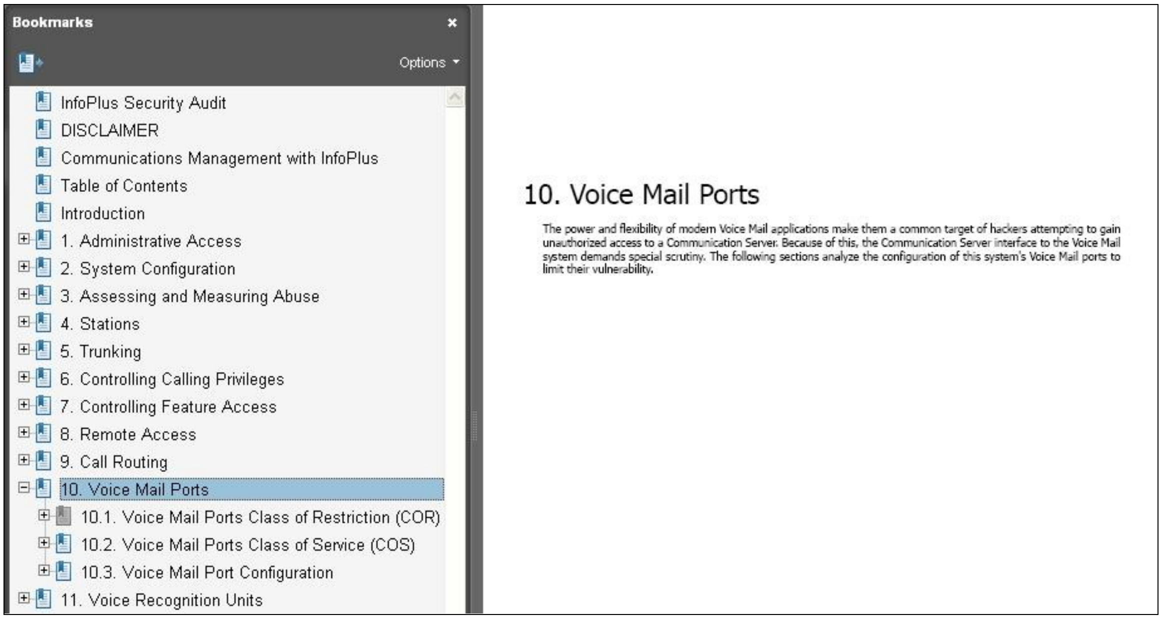


9. Call Routing

In addition to the restrictions placed at the station or trunk level, it's important to control how both incoming and outgoing calls are routed through the Communication Server network. We'll be analyzing the various features of Avaya's Alternate Route Selection (ARS) feature, looking for unusual routing configurations. Incorrect routing could prevent certain calls from being placed or received at all, or could send calls over unnecessarily expensive trunking facilities. The routing configuration is also used to supplement the definition of individual calling restrictions, defining who can call where and at what times.

6.11. Review Voice Mail Ports

Select **Voice Mail Ports** from the left pane, to display the **Voice Mail Ports** section. This section provides detailed voice mail access configuration, including class of restriction and class of service settings for the voice mail ports.

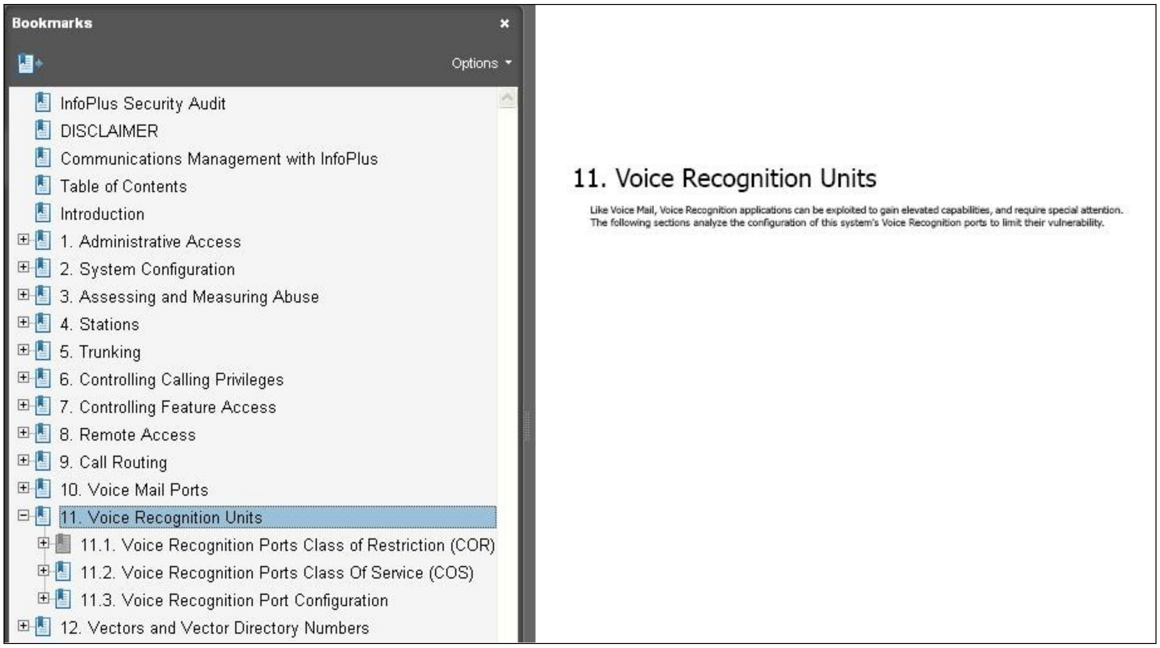

Bookmarks
×
Options ▾
InfoPlus Security Audit
DISCLAIMER
Communications Management with InfoPlus
Table of Contents
Introduction
1. Administrative Access
2. System Configuration
3. Assessing and Measuring Abuse
4. Stations
5. Trunking
6. Controlling Calling Privileges
7. Controlling Feature Access
8. Remote Access
9. Call Routing
10. Voice Mail Ports
10.1. Voice Mail Ports Class of Restriction (COR)
10.2. Voice Mail Ports Class of Service (COS)
10.3. Voice Mail Port Configuration
11. Voice Recognition Units

10. Voice Mail Ports

The power and flexibility of modern Voice Mail applications make them a common target of hackers attempting to gain unauthorized access to a Communication Server. Because of this, the Communication Server interface to the Voice Mail system demands special scrutiny. The following sections analyze the configuration of this system's Voice Mail ports to limit their vulnerability.

6.12. Review Voice Recognition Units

Select **Voice Recognition Units** from the left pane, to display the **Voice Recognition Units** section. This section provides detailed voice recognition units configuration, including class of restriction and class of service settings for the voice recognition ports.

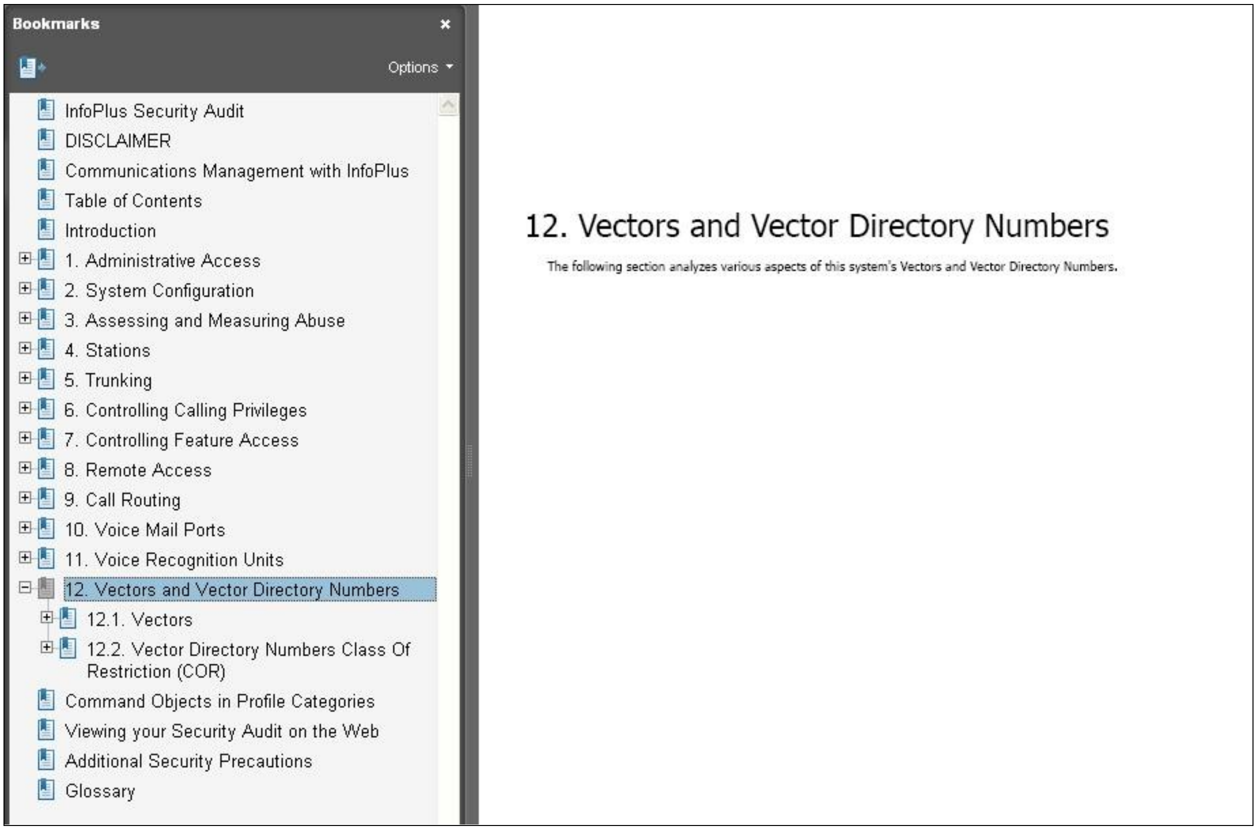

Bookmarks
×
Options ▾
InfoPlus Security Audit
DISCLAIMER
Communications Management with InfoPlus
Table of Contents
Introduction
1. Administrative Access
2. System Configuration
3. Assessing and Measuring Abuse
4. Stations
5. Trunking
6. Controlling Calling Privileges
7. Controlling Feature Access
8. Remote Access
9. Call Routing
10. Voice Mail Ports
11. Voice Recognition Units
11.1. Voice Recognition Ports Class of Restriction (COR)
11.2. Voice Recognition Ports Class Of Service (COS)
11.3. Voice Recognition Port Configuration
12. Vectors and Vector Directory Numbers

11. Voice Recognition Units

Like Voice Mail, Voice Recognition applications can be exploited to gain elevated capabilities, and require special attention. The following sections analyze the configuration of this system's Voice Recognition ports to limit their vulnerability.

6.13. **Review Vectors and Vector Directory Numbers**

Select **Vectors and Vector Directory Numbers** from the left pane, to display the **Vectors and Vector Directory Numbers** section. This section provides detailed analysis on various aspects of vectors and vector directory numbers, including security related aspects of vectors programming, and class of restrictions setting for vector directory numbers.



InfoPlus Security Audit
DISCLAIMER
Communications Management with InfoPlus
Table of Contents
Introduction
⊞ 1. Administrative Access
⊞ 2. System Configuration
⊞ 3. Assessing and Measuring Abuse
⊞ 4. Stations
⊞ 5. Trunking
⊞ 6. Controlling Calling Privileges
⊞ 7. Controlling Feature Access
⊞ 8. Remote Access
⊞ 9. Call Routing
⊞ 10. Voice Mail Ports
⊞ 11. Voice Recognition Units
⊟ 12. Vectors and Vector Directory Numbers
⊞ 12.1. Vectors
⊞ 12.2. Vector Directory Numbers Class Of Restriction (COR)
Command Objects in Profile Categories
Viewing your Security Audit on the Web
Additional Security Precautions
Glossary

12. Vectors and Vector Directory Numbers

The following section analyzes various aspects of this system's Vectors and Vector Directory Numbers.

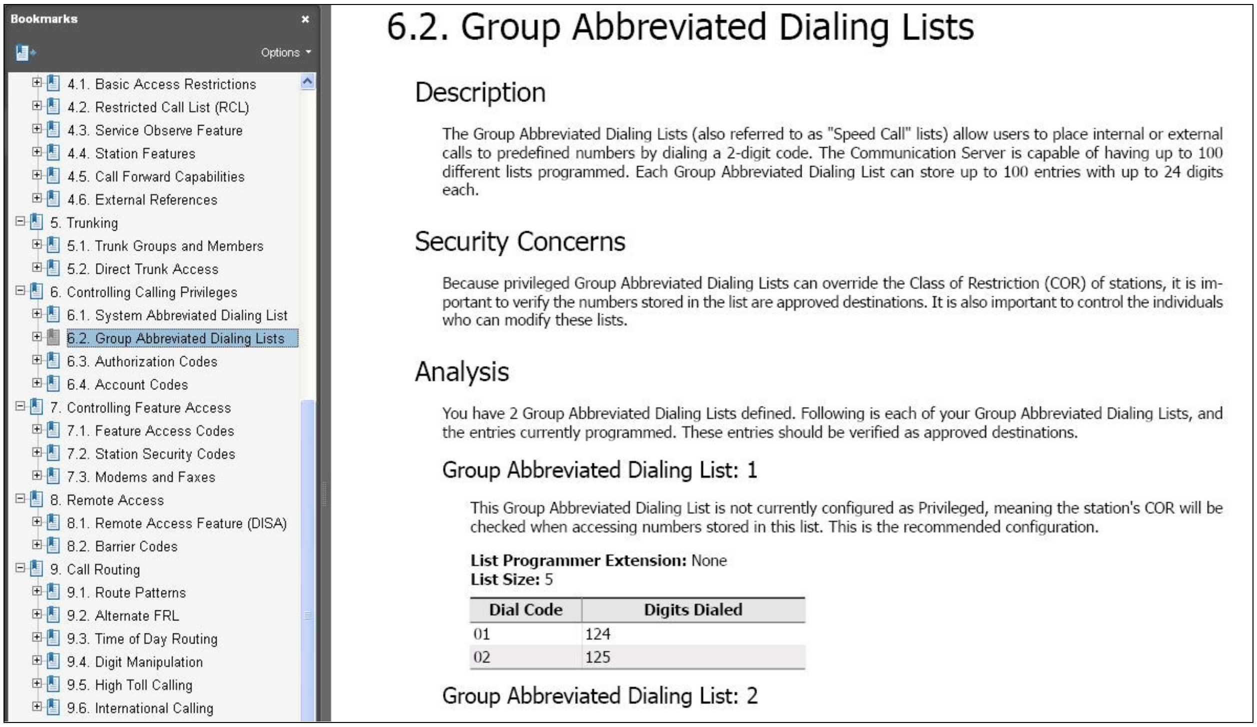
7. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager and Security Audit.

From the Communication Manager SAT, make some changes to data that will be polled by Security Audit, such as adding an abbreviated dialing group list shown below.

```
add abbreviated-dialing group 1                               Page   1 of   1
                        ABBREVIATED DIALING LIST

              Group List: 1        Group Name: Group 1
    Size (multiple of 5): 5       Program Ext:               Privileged? n
DIAL CODE
     01: 124
     02: 125
     03:
     04:
     05:
```

From the Security Audit report, select **Controlling Calling Privileges > Group Abbreviated Dialing Lists** to display the abbreviated dialing group lists. Verify that the new group list appears in the report with proper data, as shown below.


Bookmarks
Options
4.1. Basic Access Restrictions
4.2. Restricted Call List (RCL)
4.3. Service Observe Feature
4.4. Station Features
4.5. Call Forward Capabilities
4.6. External References
5. Trunking
5.1. Trunk Groups and Members
5.2. Direct Trunk Access
6. Controlling Calling Privileges
6.1. System Abbreviated Dialing List
6.2. Group Abbreviated Dialing Lists
6.3. Authorization Codes
6.4. Account Codes
7. Controlling Feature Access
7.1. Feature Access Codes
7.2. Station Security Codes
7.3. Modems and Faxes
8. Remote Access
8.1. Remote Access Feature (DISA)
8.2. Barrier Codes
9. Call Routing
9.1. Route Patterns
9.2. Alternate FRL
9.3. Time of Day Routing
9.4. Digit Manipulation
9.5. High Toll Calling
9.6. International Calling

6.2. Group Abbreviated Dialing Lists

Description

The Group Abbreviated Dialing Lists (also referred to as "Speed Call" lists) allow users to place internal or external calls to predefined numbers by dialing a 2-digit code. The Communication Server is capable of having up to 100 different lists programmed. Each Group Abbreviated Dialing List can store up to 100 entries with up to 24 digits each.

Security Concerns

Because privileged Group Abbreviated Dialing Lists can override the Class of Restriction (COR) of stations, it is important to verify the numbers stored in the list are approved destinations. It is also important to control the individuals who can modify these lists.

Analysis

You have 2 Group Abbreviated Dialing Lists defined. Following is each of your Group Abbreviated Dialing Lists, and the entries currently programmed. These entries should be verified as approved destinations.

Group Abbreviated Dialing List: 1

This Group Abbreviated Dialing List is not currently configured as Privileged, meaning the station's COR will be checked when accessing numbers stored in this list. This is the recommended configuration.

List Programmer Extension: None
List Size: 5

Dial Code	Digits Dialed
01	124
02	125

Group Abbreviated Dialing List: 2

8. Conclusion

These Application Notes describe the configuration steps required for Bristol Capital Security Audit to successfully interoperate with Avaya Aura® Communication Manager 6.0.1 using the SAT interface. All feature and serviceability test cases were completed with observations noted in **Section 0**.

9. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at http://support.avaya.com.

2. *Avaya Security Audit Demo*, available at http://www.infoplusonline.com.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.