



Avaya Solution & Interoperability Test Lab

Application Notes for Bristol Capital Security Audit Service with Avaya AuraTM Communication Manager – Issue 1.0

Abstract

These Application Notes describe the steps required for the Bristol Capital Security Audit service to successfully interoperate with Avaya AuraTM Communication Manager. The Bristol Capital Security Audit is a PBX management service that uses the Avaya System Administrator Terminal interface to obtain security related data and provide report on the security aspects of Avaya AuraTM 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 the Bristol Capital Security Audit service to successfully interoperate with Avaya Aura™ Communication Manager. The Bristol Capital Security Audit is a PBX management service that uses the Avaya System Administrator Terminal (SAT) interface to obtain security related data and provide report on the security aspects of Avaya Aura™ Communication Manager.

1.1. 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, and UNIX users/groups/authorizations.

The serviceability testing focused on verifying the ability of the Bristol Capital Security Audit service to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable and restarting the SAT session with Avaya Aura™ Communication Manager.

1.2. Support

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

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

2. Reference Configuration

As shown in **Figure 1**, the Bristol Capital Security Audit service consists of a server that connects remotely to the Avaya AuraTM Communication Manager SAT interface, and uses a subset of the SAT commands to collect security related data. The collected security data are passed on to the Bristol Capital Central Database for analysis and reporting.

The remote connectivity between the Bristol Capital Security Audit service and Avaya AuraTM Communication Manager can be accomplished using either modem dialup 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 method via the public network, a spare and existing C-LAN circuit pack from Avaya AuraTM Communication Manager was connected to the public network, 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.

Note that the corporate firewall configuration is outside the scope of these Application Notes, and will not be described.

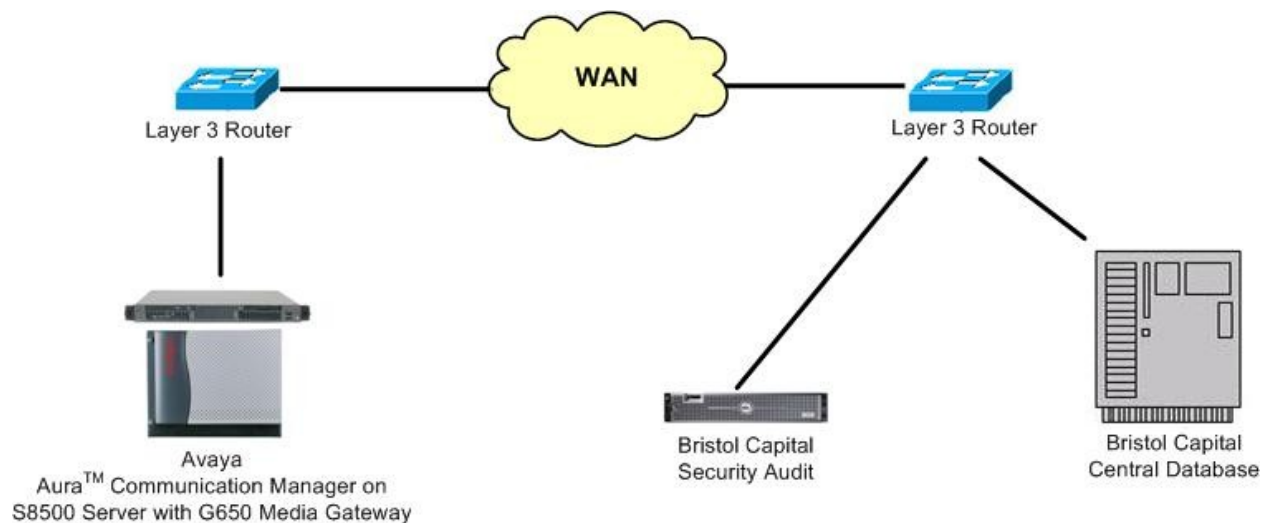


Figure 1: Bristol Capital Security Audit with Avaya AuraTM Communication Manager

3. Equipment and Software Validated

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

Equipment	Software
Avaya Aura™ Communication Manager on Avaya S8500 Server	R015x.02.0.947.3
Avaya G650 Media Gateway <ul style="list-style-type: none">• TN799DP C-LAN Circuit Pack	HW01 FW032
Bristol Capital Security Audit	Build 8026

4. Configure Avaya Aura™ Communication Manager

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

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

4.1. 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
```

4.2. Administer Node Names

Use the “change node-names ip” command to modify the IP address of the C-LAN circuit pack from **Section 4.1**, 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	
AES-Test	10.32.32.20	
Annc-1	10.32.32.14	
CDR-2nd	192.168.1.12	
CDR-Metropolis	192.2.5.25	
Clan-1	10.32.32.12	
Clan-2	xxx.xxx.xxx.xxx	
G150-Lan2	192.10.20.1	
G350-S8300	10.32.38.10	
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	
S8300-G250	10.10.1.5	

4.3. 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 4.2**.
- **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	TestSite	9002		
CDR2		Clan-1	0	CDR-2nd	9004		
AESVCS	y	Clan-1	8765				
SAT	y	Clan-2	5023	any	0		

5. 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

5.1. 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:

Attention Required

On December 8, 2009, we performed an **InfoPlus Traffic Study** for your Avaya communications system. The results of the Traffic Study indicated that you have 3 Trunk Group(s) that may be **under-trunked**. Proper trunking levels ensure that you are: avoiding excess trunking costs, meeting your current service level agreements, and providing superior service to your employees and customers. It is recommended that, once you have adjusted your trunking levels, you perform a follow-up Traffic Study to verify the impact of these changes.

For a cost that is in the hundreds of dollars, you have the potential to realize an annual cost reduction in the thousands of dollars. For further information, please contact your maintenance provider and request that an InfoPlus Traffic Study be conducted on your Avaya communications system.

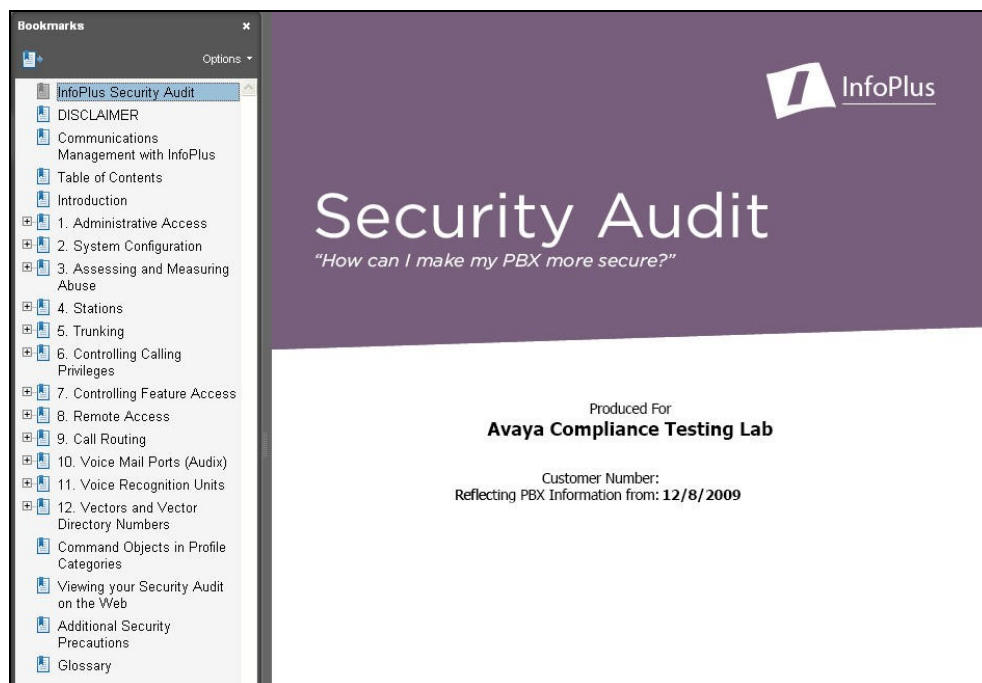
Available InfoPlus Reports and Data

The following InfoPlus Reports and services are available online:

Type	Name	Date
Inventory	Site Survey	12/08/09
Configuration	SourceBook	12/08/09
Performance	Traffic Study	12/08/09
Performance	Cost Accounting (CDR)	Request Quote
Security	Security Audit	12/08/09
Security	ServiceMonitor	Request Quote
Backup	Backup	Order

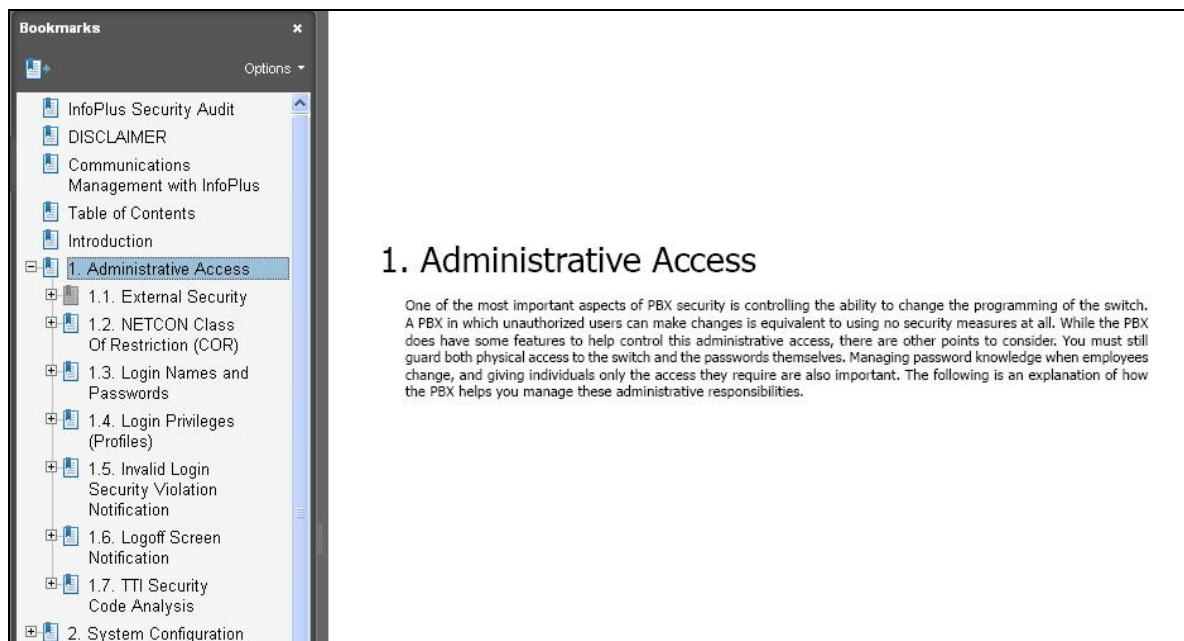
InfoPlus reports provided by Bristol Capital, Inc. Portland, ME
Copyright © 2009 Bristol Capital, Inc. All rights reserved.

The **Security Audit** report is displayed.



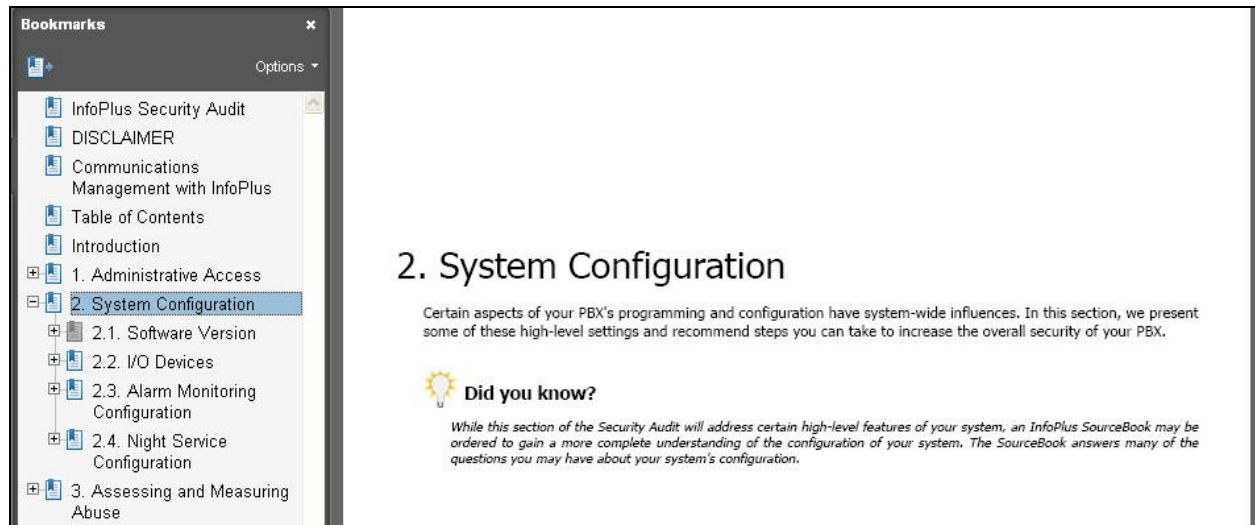
5.2. Review Administrative Access

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.



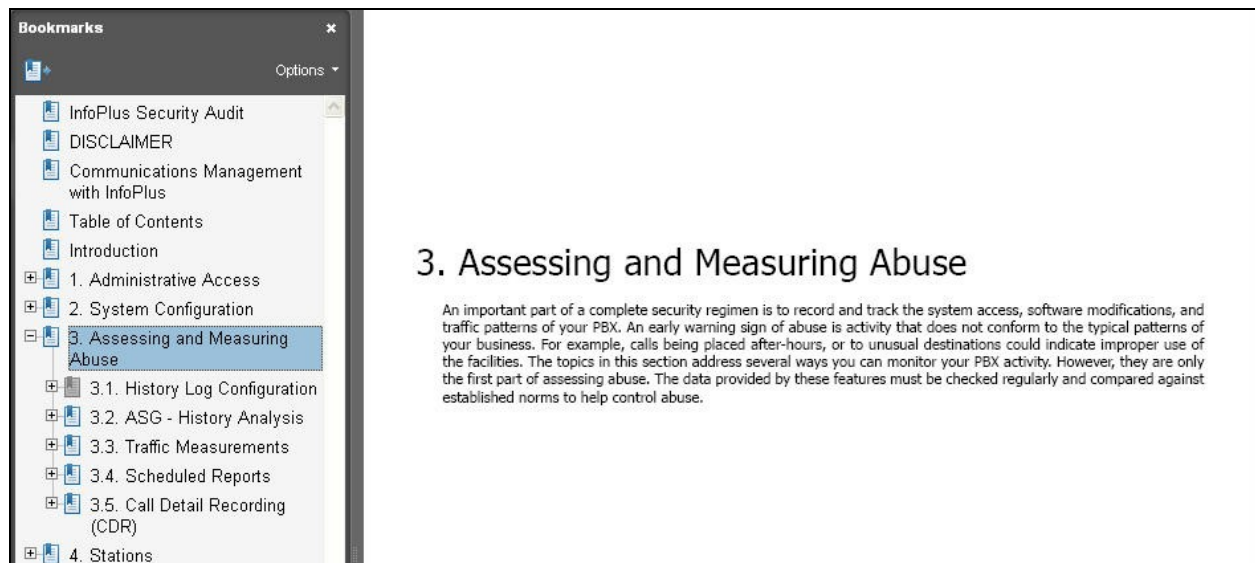
5.3. Review System Configuration

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.



5.4. 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.



5.5. 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.

The screenshot shows the 'Bookmarks' pane on the left with the following items: 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 (selected), 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, and 5. Trunking. The main content area displays the title '4. Stations' followed by a paragraph: '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.' Below this is a 'Did you know?' section with a lightbulb icon and text: '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.'

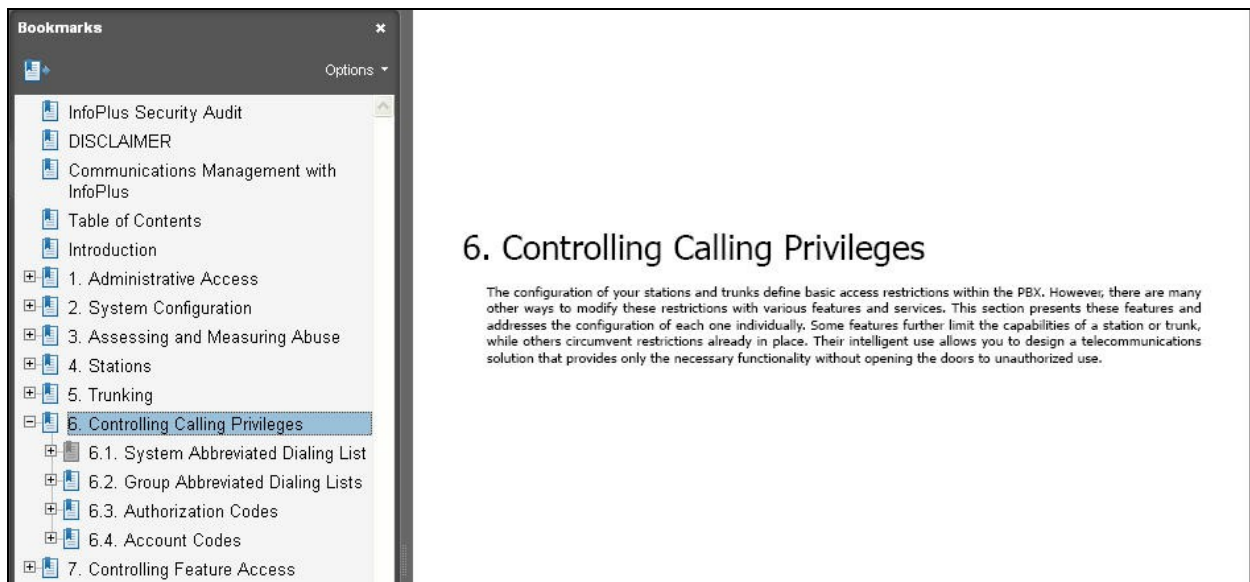
5.6. Review Trunking

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.

The screenshot shows the 'Bookmarks' pane on the left with the following items: 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 (selected), 5.1. Trunk Groups and Members, 5.2. Direct Trunk Access, 6. Controlling Calling Privileges, and 7. Controlling Feature Access. The main content area displays the title '5. Trunking' followed by a paragraph: '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.' Below this is a 'Did you know?' section with a lightbulb icon and text: '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.'

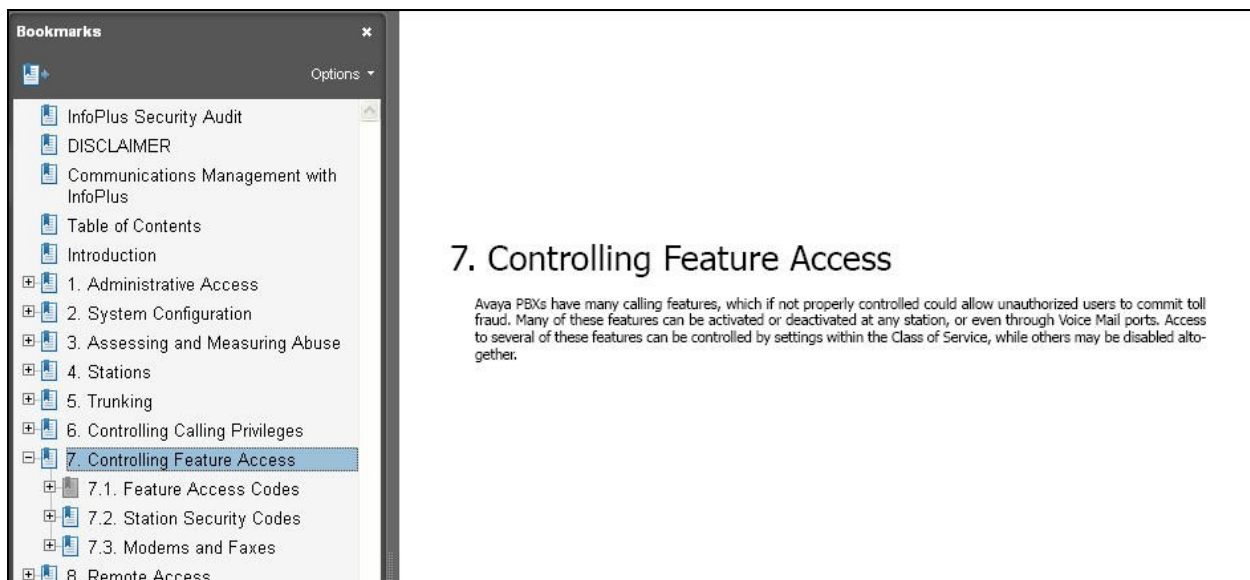
5.7. Review Controlling Calling Privileges

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.



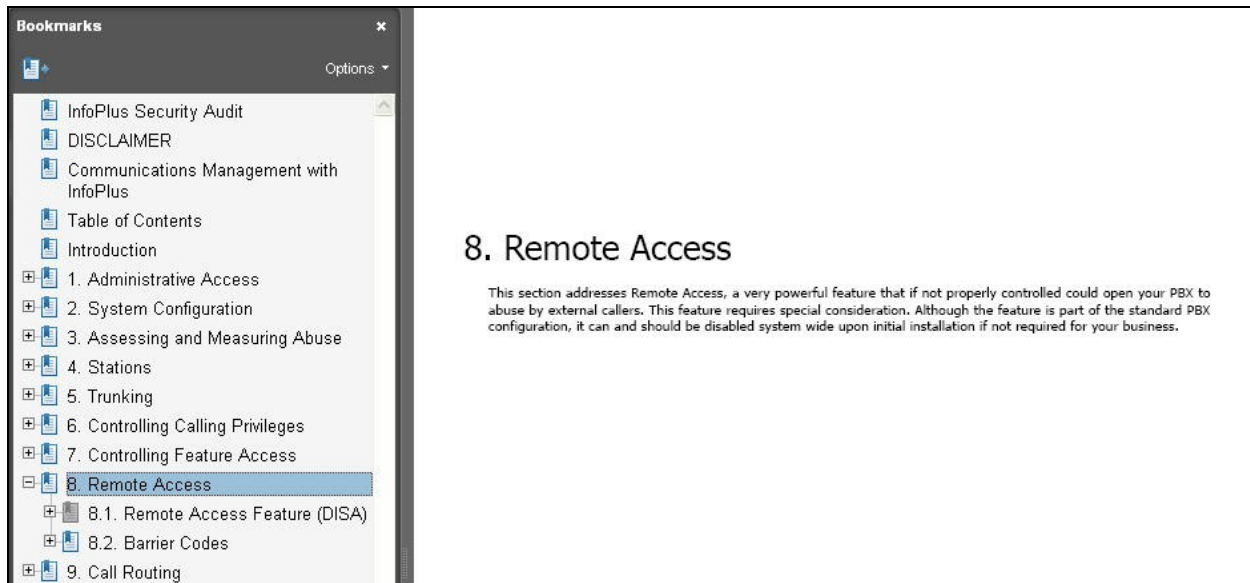
5.8. Review Controlling Feature Access

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.



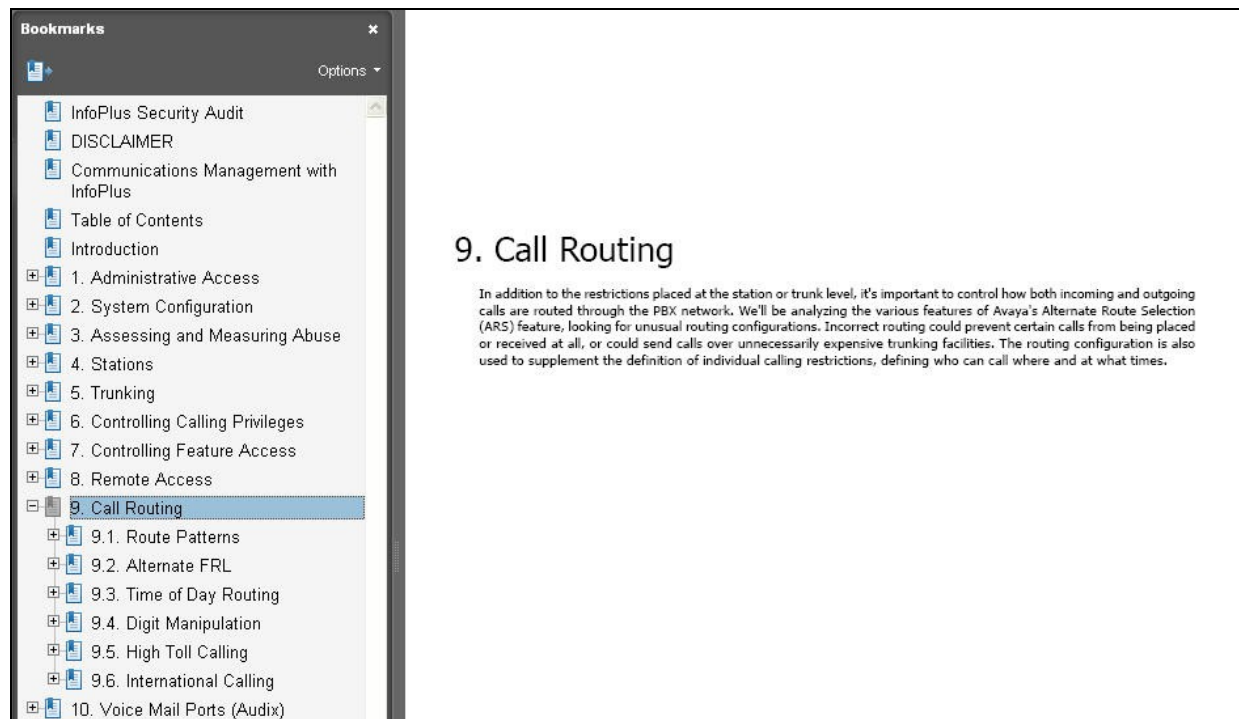
5.9. Review Remote Access

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.



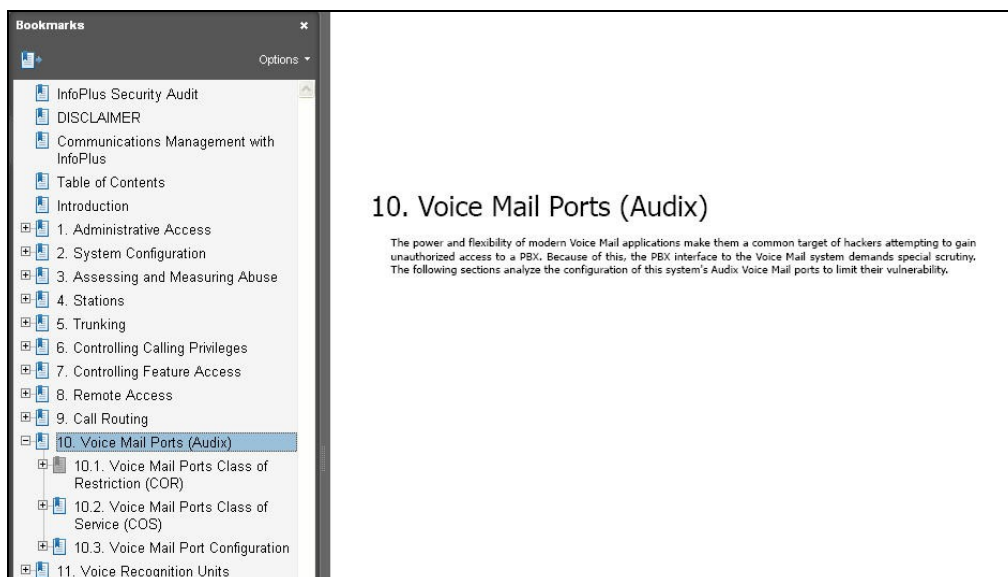
5.10. Review Call Routing

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.



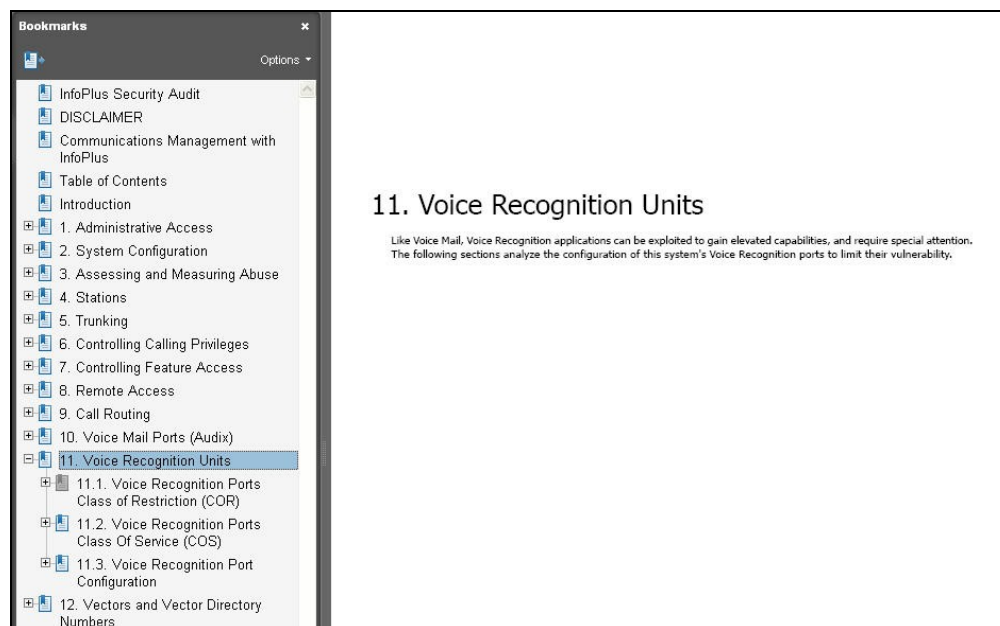
5.11. Review Voice Mail Ports

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



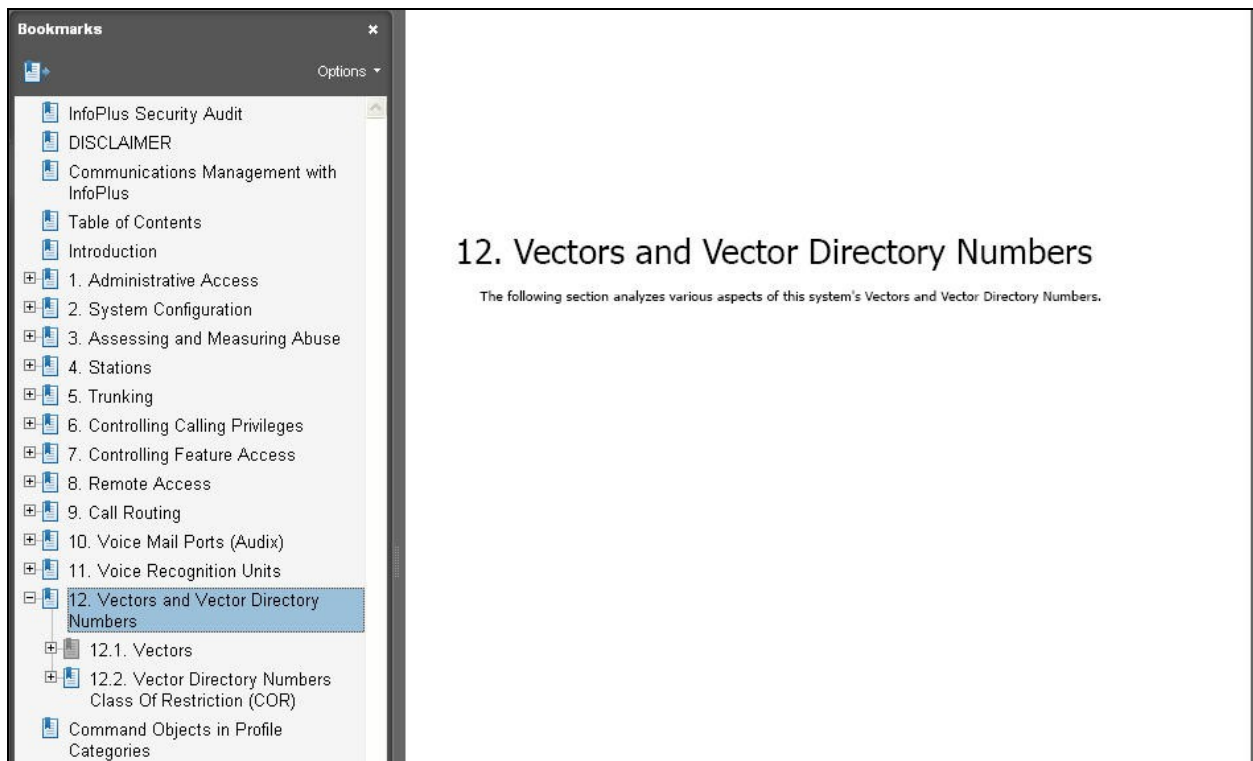
5.12. Review Voice Recognition Units

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.



5.13. 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.



6. 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 the Bristol Capital Security Audit service.

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

All test cases were executed. 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 Time of Day Routing section showed eight empty time of day routing plans when none existed in the system.
- The Digit Manipulation section will interpret route patterns with “0” deleted digits and no inserted digits as a route pattern that manipulated data. Furthermore, special characters in the route pattern inserted digits string were not reflected in the displayed entries.

7. Conclusion

These Application Notes describe the configuration steps required for the Bristol Capital Security Audit service to successfully interoperate with Avaya Aura™ Communication Manager. All test cases were completed successfully with four observations noted in **Section 6**.

8. Additional References

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

1. *Administrator Guide for Avaya Aura™ Communication Manager*, Document 03-300509, Issue 5.0, Release 5.2, May 2009, available at <http://support.avaya.com>.
2. *Avaya Security Audit Demo*, available at <http://www.infoplusonline.com>.

©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.