Avaya Aura® Contact Center

Security Reference Guide

Release 6.4

May 2014

ver. 02.00

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.

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 Web sites 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.

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 Web site: 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.

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 End User a license within the scope of the license types described below. 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 End User. “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. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

Concurrent User License

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.

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.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya®, Avaya Aura®, Avaya™, and Avaya Aura™ are registered trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners.

Downloading Documentation

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

Hardware Support

For full hardware support, please see *Avaya Support Notices for Hardware Documentation*, document number 03–600759 on the Avaya Support Web site, http://support.avaya.com.

Contact Avaya Support

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

Table of Contents

1. Introduction

This document provides an overview of Avaya Aura® Contact Center Release 6.4 security features and considerations. Avaya Aura® Contact Center is a suite of contact center software applications running on the Windows and Linux operating systems. This document provides an overview of the following:

- Avaya Aura® Contact Center server operating system security
- Avaya Aura® Contact Center software security
- Avaya Aura® Contact Center solution security

Avaya Aura® Contact Center provides assisted voice and multimedia customer contact solutions. Avaya Aura® Contact Center supports voice calls on the following voice platforms:

Avaya Aura® Unified Communications platform. Avaya Aura® Contact Center integrates with the Avaya Aura® Unified Communications platform using SIP-enabled technologies. This integration gives Contact Center access to and control of Avaya Aura® Unified Communications platform phones.

Avaya Communication Server 1000. Avaya Aura® Contact Center integrates with Avaya Communication Server 1000 using a propriety Application Module Link (AML) protocol. This integration gives Contact Center access to and control of Avaya Communication Server 1000 phones and Controlled Directory Numbers (CDNs).

Avaya Aura® Contact Center supports multimedia contact types. Contact Center agents can handle multimedia contacts from customers. This offers the customers increased flexibility and choice. Multimedia-enabled agents are more productive, responsive, mobile, and more cost effective compared to voice-only agents. Avaya Aura® Contact Center supports the following multimedia contact types:

1. Email
2. Instant Message (IM)
3. Web communications
4. Outbound
5. SMS text
6. Faxed document
7. Scanned document

8. Voice mail

Avaya Aura® Contact Center requires some additional infrastructure and third-party servers to support these multimedia contact types. For example, an external email server is required to support the email contact type, and an external application server is required to support Web communications.

This document also introduces the Avaya Aura® Contact Center client software, agent desktop computer, Windows domain, and security considerations.

You must consider security when designing, planning, commissioning, and maintaining an Avaya Aura® Contact Center solution. You must consider each component individually, its part in the solution, and the solution as a whole.

For more information about Avaya Aura® Contact Center, see *Avaya Aura® Contact Center Fundamentals and Planning (44400-211)* on the Avaya Support website: http://support.avaya.com.

For more information about Avaya Aura® Contact Center and Avaya Communication Server 1000, see *Avaya Aura® Contact Center Configuration – Avaya CS1000 Integration* (44400-512).

For more information about Avaya Aura® Contact Center and the Avaya Aura® Unified Communications platform, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).

Disclaimer

Avaya has used reasonable commercial efforts to ensure that the information provided here under is accurate at the date of publication. Avaya may change any underlying processes, architecture, product, description or any other information described or contained in this document. Avaya disclaims any intention or obligation to update or revise the book, whether as a result of new information, future events or otherwise. This document is provided “as is,” and Avaya does not provide any warranty of any kind, express or implied.

2. Avaya Aura® Contact Center overview

The Avaya Aura® Contact Center solution needs to be resilient to attacks that can cause service disruption, malfunction, theft of information, or theft of service. The Avaya Aura® Contact Center suite of applications includes the following components:

Contact Center Manager Server (CCMS)

Contact Center Multimedia Server (CCMM)

Contact Center Manager Administrator (CCMA)

Avaya Communication Control Toolkit (CCT)

Contact Center Licence Manager (CCLM)

Avaya Media Server (Windows and Linux)

Orchestration Designer (OD)

Avaya Aura Agent Desktop (AAAD)

3. Avaya Aura® Contact Center Server Security

3.1 Synopsis

This section will cover the common security procedures in place that apply to all of the applications that can co-reside on the Avaya Aura Contact Center Server solution Microsoft Windows 2008 platform. Later sections cover the specific requirements of individual AACC applications.

3.2 Secure by default

The AACC firewall policy opens only those ports necessary for an AACC solution to communicate and function. The policy closes the ports not necessary for AACC to function.

3.3 Listing of ports and transport types

Contact Center Manager Server uses ports for communication between its own components. Most ports do not have implications for external network components like firewalls; however some ports may be used externally and therefore can affect an external firewall.

Third-party applications installed co-resident with Contact Center Manager Server must not use the ports listed in the Port Matrix as this can cause the Contact Center Manager Server to malfunction.

The *Avaya Aura® Contact Center 6.4 Port Matrix document* specifies the port numbers used by Avaya products. This allows you to create effective firewall policies without disrupting contact center communications or opening unnecessary ports into the network.

For more information, see *Avaya Aura® Contact Center 6.4 Avaya Port Matrix* document on *www.avaya.com/support*

For network and port information specific to AACC, refer to the *Avaya Aura® Contact Center Fundamentals and Planning (44400-211). See www.avaya.com/support*

3.4 Firewall policy

Firewall policies monitor, authorize and log data flows and events. They also restrict access using IP addresses, port numbers and application types and sub-types.

The Avaya Aura® Contact Center firewall policy allows Avaya Aura® Contact Center to operate with Windows Firewall switched on. The AACC firewall policy is configured based on the default product install options.

You can download the most recent Avaya Aura® Contact Center Firewall Security policy from www.avaya.com/support.

3.4.1 Reviewing the AACC firewall policy

To review the inbound and outbound rules which are enforced by the supplied Avaya Aura® firewall policy you can open the *Microsoft Windows® Firewall with Advanced Security application* and browse the inbound and outbound rules.

3.4.1.1 Accessing the Microsoft Windows Firewall with Advanced Security application

1. Log on to an AACC server that has the AACC firewall policy installed.
2. Select the ***Start*** button on the main windows desktop
3. Select ***Administrative Tools***
4. Select ***Windows Firewall with Advanced Security***
5. Select the ***Inbound Rules or Outbound Rules*** to view the list of rules, which include applications, services and ports, which now apply to the AACC server once this policy has been implemented.

3.4.2 Backing up your Firewall Policy

Avaya recommends that you export and backup your existing firewall security policy before importing the Avaya Aura® Contact Center Firewall Security policy. You can use this backup policy to roll back the Avaya Aura® Contact Center Firewall Security policy, if you ever need to.

For more information about Avaya Aura® Contact Center Firewall Policy, see *Avaya Aura® Contact Center Fundamentals and Planning (44400-211)*.

3.5 Group Policies

The Avaya Aura® Contact Center (AACC) firewall policy defines the services, network ports, and Windows accounts necessary for secure contact center voice and multimedia functionality. Avaya Aura® Contact Center does not provide or install a group policy.

Domain group policies and security policies can be configured to automate MS Windows updates, server backups, and password expiry rules for local users. These automated features are not supported by AACC. If your group policies or security policies implement these automated features, place the AACC servers in an Active Directory organizational unit (OU) container that protects the servers from these automated features.

If this is not acceptable then the following procedures will have to be undertaken to remove the possibility of a group policy affecting the contact center solution.

If performance or functionality issues are raised to Avaya support personnel as part of the fault diagnosis, you may be asked to place the AACC servers in an Active Directory organizational unit (OU) container that isolates the servers from these automated features.

3.5.1 Working with Avaya Aura® Contact Center

If you plan to apply a corporate or custom group policy to the AACC servers and solution, you must first perform the following:

1. Understand the AACC services, ports, and user account requirements as specified by the AACC firewall. For more information, see *Microsoft Windows Firewall and Advanced Security* on your AACC server to view the inbound/outbound rules.
2. Understand the AACC network ports and transport types. For more information, see the Avaya Aura® Contact Center Port Matrix document available at www.avaya.com/support.
3. Design or modify your group policy to accommodate these existing AACC services, ports, user accounts, and transport type requirements.
4. During an AACC maintenance window, apply and test your group policy. Ensure AACC call control, administration and maintenance capabilities are preserved. Do not apply an untested group policy to a production environment. If necessary, modify your group policy to preserve AACC functionality.
5. After successful testing, place AACC back into production, and continue to monitor the contact center for adverse side effects of your group policy.

In summary, an Avaya Aura® Contact Center solution cannot be changed to accommodate individual corporate group policies, so corporate group policies must accommodate Avaya Aura® Contact Center.

3.5.2 Working with AACC Windows Accounts

The Avaya Aura® Contact Center uses several Microsoft Windows® accounts. The group policy must work in conjunction with the AACC Microsoft firewall policy.

Avaya Aura® Contact Center uses several Windows accounts to communicate and access resources in the solution.

3.5.2.1 Accounts used by Avaya Aura® Contact Center

LocalSystem account

The LocalSystem account is a predefined local account used by the service control manager. This account is not recognized by the security subsystem. It has extensive privileges on the local computer, and acts as the computer on the network.

Several major components of the Avaya Aura® Contact Center solution use this account.

NetworkService Account

The NetworkService account is a predefined local account used by the service control manager. This account is not recognized by the security subsystem. It has minimum privileges on the local computer and acts as the computer on the network.

The Avaya Aura® Contact Center SymposiumWC Service Provider service uses this account.

iceAdmin

The iceAdmin account is a member of the Windows Administrators group, it is used by the Contact Center Manager Administration (CCMA) Active Directory Lightweight Directory Services (AD-LDS) information storage repository.

IUSR_SWC

Member of the IIS_IUSRS and BACKUP_USERS group. The Contact Center Manager Administration (CCMA) application pools in Internet Information Services (IIS) run under this account. This account is also used by Contact Center Multimedia (CCMM) which attach documents to multimedia contacts.

3.6 Anti-Virus considerations

Your security policies may require the installation of antivirus software on AACC servers.

The Avaya Aura® Contact Center supported antivirus products are:

- Symantec Anti-Virus 11.0.5, 11.0.6, or 12
- McAfee 8.8
- Microsoft Forefront 2010

You may deploy antivirus products from other vendors subject to the following guidelines:

- Infected file quarantine policy on the server and client: antivirus software can be configured to clean up the detected virus automatically and files must be quarantined if infected files cannot be cleaned. Contact Avaya to verify whether the quarantine file is part of our product files or dependent system file. If a virus is detected, remove the server from the network immediately during virus eradication to prevent further virus propagation.

- Do not connect a contact center application platform directly to the Internet to download virus definitions or updated files. Furthermore, Avaya recommends that you do not use a contact center application client PC to connect to the Internet. Instead, download virus definitions and updated files to another location on the customer network and manually load them from this interim location onto the contact center application platform.

- Perform the previous steps to download Contact Center application service packs (SP). This method limits access to the Internet, and thus reduces the risk of downloading infected files.

- Scan all SP files, DVD-ROMs, USB drives and floppy disks if present before you upload or install to the server. This practice minimizes any exposure to infected files from outside sources.

- Capacity considerations: running virus scan software can place an additional load on a contact center application platform. The implementation personnel must run the performance monitor tool on the server to gauge CPU usage. If the antivirus software scan causes the platform average CPU usage to exceed the recommended percentage for longer than 20 minutes, the antivirus software must not be loaded onto the contact center application platform.

- Product Support does not provide support on the configuration of antivirus software, but offer guidance where possible. Questions should be directed to the appropriate vendor regarding problems on antivirus software.

- If performance or functionality issues are raised to Avaya support personnel as part of the fault diagnosis, you may be asked to remove third-party utility software or antivirus software.

3.6.1 Folder Exclusion List

Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- F:\Avaya\Contact Center\Database\
- <additional database drive>:\Avaya\Database\
- TSM_OAM log folder location
- D:\Avaya\Contact Center\Manager Server\iccm\bin\data
- D:\Avaya\Contact Center\Manager server\iccm\data
- D:\Avaya\Contact Center\Manager Server\iccm\sdm\log
- OAMContainer*.log located at D:\Avaya\Contact Center\Common Components\CMF
- D:\Avaya\Contact Center\Manager Server\bin\tools2.exe—File access errors occur in the Scan Activity log if you do not exclude this file from scanning.
- D:\Avaya\Contact Center\Manager Server\iccm\logs (SIP logs)
- D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\ (SIP log configuration files)
- D:\Avaya\Contact Center\Common Components\CMF
- The folder where you store Server Packs and patches

For more detail please refer section *Voice and Multimedia Contact Server antivirus software* on the *Planning and Engineering book (44400-210) s*ee www.avaya.com/support

3.7 Domain Considerations

Avaya Aura® Contact Center application platform is designed to work by joining an existing customer network Windows Domain.

3.7.1 Being a Domain member when installing AACC

While it is possible to join a fully configured AACC server to a domain after a software install it is recommended that the server be joined to the domain it will be operating in prior to installing any Avaya Aura Contact Center software.

If Contact Center Multimedia is not part of a Windows domain, additional configuration is required for example. See AACC Fundamentals (44400-220) for further information.

3.7.2 Standalone configuration

If Avaya Aura® Contact Center application platform is configured as a standalone server, all server security policies are controlled by the local server security policy. Security group policy in the customer network domain controller will not be applicable to the Avaya Aura® Contact Center application platform.

3.7.3 Joining a domain (existing or new)

If Avaya Aura® Contact Center application platform is joining an existing customer network domain, you must review any Domain Group Policy that can be applied to the Avaya Aura® Contact. Customers may need to adjust their security group policy or exclude the Avaya Aura® Contact Center platform from the group policy if conflicts are identified.

There are considerations with regard to data replication for Contact Center Manager Administration (CCMA) redundancy. Please refer to Active Directory Lightweight Directory Services (AD-LDS) section.

3.8 Database access security

Database access security is controlled by Cache. Only authorized database user accounts with correct passwords can access the database through pre-assigned access roles. All critical call center configuration information and customer call statistics are stored in the database. Avaya proprietary information is also stored in the database and can only be accessed by the “system administrator” accounts.

Details of these accounts are considered Avaya confidential and, therefore, are not released to any customers. Customers do not need to perform any database access or maintenance operations that require administrative roles access. Instead, customers use other Contact Center Manager Server user accounts to access the database and create custom call statistic reports.

Customers can access the database through the pre-defined “sysadmin” account and other Contact Center Manager Server user accounts created by the Contact Center Manager administrators or supervisors using the Server Utility. The “sysadmin” account and other Contact Center Manager Server user accounts are different from the database administrative role accounts. Customers can change the passwords for all created Contact Center Manager Server user accounts, including the pre-defined “sysadmin” account. In fact, for security purposes, customers should change the default password for the sysadmin account when logging on to Avaya Aura® Contact Center Manager Server for the first time.

Both “sysadmin” and Contact Center Manager Server user accounts have read access only privileges to the database and cannot modify any database content.

3.8.1 Remote backup and restore security

CCMS, CCMM, CCT, and Avaya MS support database backup and restore on a remote network computer that is accessible through the Avaya Server Subnet (formerly known as CLAN). Procedures are provided to setup the proper remote backup location and access account of the remote backup computer on Contact Center Manager Server application server to ensure that only assigned user accounts and privileges are used to access the remote backup location. Customers must exercise proper security measures for the shared remote backup folder on the remote computer to prevent unauthorized access to the Contact Center Manager Server backup files.

Remote backup and restore configuration procedures are documented in Avaya Aura® Contact Center Routine Maintenance (44400-514).

3.9 Software Updates & Microsoft security hot fixes

In the Avaya Aura® Contact Center solution automatic software updates are turned off. Avaya performs a check on any new Microsoft service updates or hot fixes only and updates a document listing the patches that have been passed for installation on the Avaya Aura® Contact Center Windows platform. Avaya does not review non-security hot fixes

For more information about updating, see the *Contact Center Portfolio Service Packs Compatibility and Security Hot fixes Compatibility List* on www.avaya.com/support

Also refer to *Avaya Aura® Contact Center Upgrade and Patches (44400-410),* on www.avaya.com/support, for details on the preparation procedures in applying patches and hot fixes to the servers.

3.9.1 Service updates

Given the number of operating system security service updates and the complexity inherent in any network, create a systematic and accountable process for identifying and applying service updates. To help create such a process, you can follow a series of best practices guidelines, as documented in the National Institute of Standards and Technology (NIST) Special Bulletin 800-40, Procedures for Handling Security Patches.

This bulletin suggests that if an organization has no central group to coordinate the storage, evaluation, and chronicling of security service updates into a library, then system administrators or the contact center administrator must fulfill this role. In addition to these guidelines, whenever possible, follow Microsoft recommendations regarding newly discovered vulnerabilities and ensure that Microsoft security service updates are promptly installed.

Whenever possible, Avaya incorporates the most recent operating system security recommendations and service updates in an integrated solution testing strategy during each test cycle. However, due to the urgent nature of security service updates when vulnerabilities are discovered follow Microsoft guidelines as they are issued, including any Microsoft installation procedures and security service update rollback processes that may be in place.

Finally, before you update the system, you must perform a full system backup to ensure that a rollback is possible, if required. If a Contact Center application does not function properly after you apply a Microsoft security service update, you must remove the service update and revert to the previous version of the application (from the backup you made before applying the service update). For added security, always determine whether Avaya verified the Microsoft service update for compatibility with Avaya Aura® Contact Center.

3.9.2 Service Packs

Avaya has a policy to implement co-residency testing of all new operating system Service Packs for compatibility with the suite of Contact Center applications as soon as they are available. In practice, because a Service Pack can contain a significant amount of new content, Avaya requires that you wait until compatibility testing is complete before you apply the Service Pack.

Note that operating system Service Packs are typically tested with the most recent Contact Center application Service Pack and, therefore, an upgrade to a new Service Pack requires an upgrade to the most recent Avaya Service Pack.

Before you upload a new Service Pack, you must perform a full system backup (for system rollback as in the updating scenario).

For more information about Service Pack compatibility, see the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Compatibility List* on www.avaya.com/support

3.9.3 Backup of Server

Before applying a service pack, plan to perform a backup of server, and then shut down all Contact Center services before applying any Microsoft security hot fixes. Ensure to follow the Microsoft instructions which come with the particular hot fix.

3.9.4 Third-party software requirements

Due to the mission-critical, real-time processing that Contact Center applications perform, you must not install any other application class software on the server. You can install certain utility class software on the server, providing it conforms to the guidelines in this section.

Application class software generally requires a certain amount of system resources and must not be installed on a server running Contact Center applications. The installation of third-party applications can cause Contact Center applications to operate outside of the known engineering limits and can create potential unknown system problems (for example, CPU contentions, increased network traffic loading, disk access degradations).

Certain third-party utility class software applications, such as hardware diagnostics or backup tools, generally require less system resources during the normal operation of Contact Center applications and are permitted. Exceptions are utilities such as screen savers, which can cause

system problems and degrade performance. Antivirus software is classified as a utility and is subject to the generic guidelines in the following section.

3.9.5 Generic guidelines for utility-class software applications

The following are generic guidelines for utility-class software:

- During run-time, the utility must not degrade the contact center application beyond an average percentage of CPU use (see each specific application section in this document for the recommended maximum CPU usage level). Furthermore, the utility must not lower the minimum amount of free hard disk space required by contact center application and the Windows Operating System.

- The utility must not cause improper software shutdowns or out-of-sequence shutdowns.

- The utility must not administer the contact center application.

- If the utility has a database, it must not affect the contact center application database.

- Disk compression utilities must not be used.

- Memory tweaking utilities (for example, WinRAM Turbo, Memory Zipper) used to reclaim memory that is unused by Microsoft must not be used.

- The installation or uninstallation of the third-party software must not impact or conflict with the contact center application (for example, it must not cause DLL conflicts). If such conflicts are discovered, a server rebuild may be necessary.

- The implementation personnel must perform tests to ensure these conditions and recommendations are met before you place the Contact Center application into production. Support personnel may ask for the results of the testing during fault diagnosis. As part of fault diagnosis, Avaya Support may ask for third-party software to be removed.

4.0 Virtualization and security

Virtualization supports security and fault isolation by running in separate software environments via sandboxing. Environmental isolation allows multiple operating systems to run on the same machine due to the fact that a virtual machine cannot access the underlying host resources directly. The use of virtualization allows the applications to run on the same physical machine while isolating the servers from one another because they are running on separate virtual machines.

4.0.1 Performance impact consideration

While virtualization offers these forms of isolation, virtualization environments do not provide performance isolation. The behavior of one virtual machine can adversely affect the performance of another virtual machine on the same host. Most modern virtualization environments provide mechanisms that you can use to detect and reduce performance interference. You must carefully engineer your virtualized contact center solution to avoid performance interference.

Deploy Avaya Aura® Contact Center on an enterprise-grade virtual environment with the most recent hardware that supports hardware-assisted virtualization. Avaya recommends that you apply virtualization planning, engineering, and deployment with full organizational support for virtualization rather than organically growing a virtualization infrastructure.

Schedule backups and virus scanning programs in virtual machines to run at off-peak hours and do not schedule them to run simultaneously in multiple virtual machines on the same host.

4.0.2 VMware Snapshot considerations

VMware snapshots save the current state of the virtual machine, so you can return to it at any time. Snapshots are useful when you need to revert a virtual machine repeatedly to the same state, but you don't want to create multiple virtual machines.

When restoring snapshots, carefully consider the possible impact from out-of-date antivirus definitions, missed Microsoft Windows OS and security updates, and lapsed domain accounts on the contact center. Isolate the restored virtual machine until these issues are resolved.

For additional snapshot considerations, see the *Planning and Engineering Guide (44400-210)* on www.avaya.com/support

4.1 Communication Control Toolkit

4.1.1 Communication Control Toolkit application security layer

Communication Control Toolkit application security layer includes built-in security functions that protect critical Communication Control Toolkit call information and system resources from unauthorized access.

4.1.2 Secure transport

The communication between the Communication Control Toolkit application server and Communication Control Toolkit client application is implemented using a secure Microsoft Windows Communication Foundation (WCF) transport with Windows authentication. NetTCPBinding with Reliable Session is used to establish a secured TCP transport channel between the Communication Control Toolkit server and client.

4.1.3 Resources control

The Communication Control Toolkit application includes built-in security functions that protect Communication Control Toolkit resources from unauthorized access. All Communication Control Toolkit resources are configured and assigned with authorized users who must be a valid Windows user (local or domain). The Communication Control Toolkit users are validated before any of the assigned resources are accessed.

4.2 Avaya Contact Center Manager Administration

4.2.1 User access security

An Avaya Contact Center Manager Administration desktop PC user can connect only to the Contact Center Manager Administration application server by logging on with a valid Contact Center Manager Administration user account and password in the initial Web page connection. Each Contact Center Manager Administration user can have his or her own access and partition permissions that restrict which Contact Center Manager Administration services the user can access.

These same permissions can limit the list of Contact Center Manager Server items (for example, the list of connected servers in Contact Center Manager Server, Agents, Skillsets, CDN etc.) that the Contact Center Manager Administration user can access. A default “webadmin” Contact Center Manager Administration user is created during the Contact Center Manager Administration installation.

Customers cannot delete this default account, and Avaya recommends customers change the default “webadmin” account password immediately after the initial logon.

All Contact Center Manager Administration user information including its password in an encrypted format is saved in the local Active Directory Lightweight Directory Services (AD-LDS) database on the Contact Center Manager Administration application server. The Contact Center Manager Administration user password is encrypted by using SHA-1 hashing algorithm with 256 bits encryption and a key of 32 characters length. All actual Contact Center Manager Server user information (for example, Contact Center Manager Server supervisor and agent accounts) is stored in the database on the Contact Center Manager Server and is not available on the Contact Center Manager Administration application server.

No actual Contact Center Manager Server user account and password information is transmitted between the Contact Center Manager Administration desktop application and Contact Center Manager Server.

A security option is included in Contact Center Manager Administration to integrate with the Security Framework to provide the following user access security enhancements:

- Single sign-on with customer network user accounts
- Enforce password and account policies and auditing
- Support authentication of users against Active Directory including across domain configuration

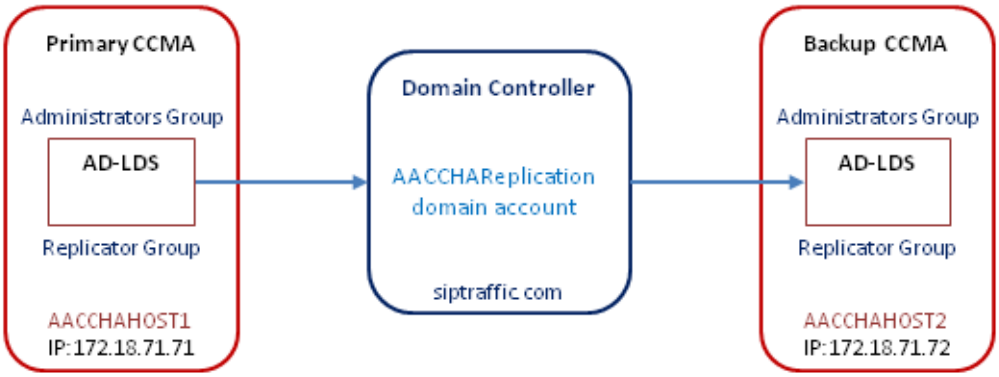
4.2.2 Contact Center Manager Administration Redundancy

Contact Center Manager Administration (CCMA) redundancy is provided by the addition of a replication or standby CCMA server. The replication of the data is enabled by Active Directory Lightweight Directory Services.

4.2.2.1 Active Directory Lightweight Directory Services (AD-LDS)

CCMA stores configuration data in a Microsoft Active Directory - Lightweight Directory Services (AD-LDS) data store. The standby CCMA replicates the AD-LDS on the primary CCMA. The standby CCMA uses AD-LDS replication to maintain a copy of the primary CCMA configuration data. If the active CCMA fails, no loss of configuration data occurs because the standby CCMA replicates the data stored in AD-LDS.

The primary CCMA server and the standby replication CCMA server must both be in the same Windows domain for AD-LDS replication to work. AD-LDS replication uses a common windows account, used by both CCMA servers, to copy or replicate configuration data from the primary CCMA AD-LDS to the standby CCMA AD-LDS.



The siptraffic\AACCHAReplication domain user account is a member of the Administrators Group and the Replicator Group on both CCMA servers. This AACCHAReplication account is used to replicate CCMA data.

4.2.2.2 Domain environments

Perform the following steps to create the AD-LDS Replication account:

• Ask your Systems Administrator to create a domain user account for use by AD-LDS Replication, for example "siptraffic\AACCHAReplication".

• Assign this domain user account to the local Administrators and local Replicator groups on both CCMA servers.

4.2.2.3 AD-LDS Accounts

These account details, necessary for AACC HA, must be kept secure, as they cannot be changed after installing AACC. The account password must not expire because changing it is not supported by AACC.

Whilst this will be seen as a vulnerability in security scans it is a requirement for a HA deployment.

4.2.3 Internet Information Service configuration

Avaya Aura® Contact Center Manager Administration and Contact Center Multimedia/Outbound applications require that Internet Information Service (IIS) be installed on the application platform. The Internet Information Service security strategy includes a set of default IIS security settings and configurations that help to minimize the exposure of IIS on the application server to potential attackers.

4.2.3.1 Securing CCMA Web Site

To secure communication when using CCMA the following steps need to be performed to enable https: and Secure Sockets Layer (SSL) for the website. Please refer to *Avaya Aura® Contact Center Commissioning* guide *(44400-312)* from www.avaya.com/support

4.2.3.2 Enabling HTTPS security for CCMA

1. Click Start > Administrative Tools > Internet Information Services (IIS) Manager.
2. On the tree view under the server node, from the list of Sites, select the Default Web Site.
3. On the Actions pane on the right, select Bindings.
4. On the Site Bindings window, click Add.
5. In the Add Site Binding window, from the Type list, select https.
6. In the Port box, type the SSL port number. The default port is 443.
7. From the SSL Certificate list, select the installed signed certificate, using the certificate friendly name.
8. Select OK.
9. Select Close.
10. On the tree view under the server node, from the list of Sites, select the Default Web Site.
11. On the center list view, double-click SSL Settings.
12. Select Require SSL.
13. Select Ignore.
14. On the Actions pane, select Apply.

4.2.3.3 Enabling communications with CCMA server components

Enable secure communications with CCMA server components such as Orchestration Designer and Open Interfaces Web Services. Use the Contact Center “wcApplyChanges” utility to configure Orchestration Designer and Open Interfaces Web Services to work when CCMA uses HTTPS security.

Log on to Contact Center Manager Administration.

Click Start > Run.

In the Open box, enter cmd.

At the command prompt, enter *wcApplyChanges -i*.

4.3 Avaya Media Server

Avaya Media Server can operate as a single standalone entity on a separate server, which is Linux based or in certain configurations it can co-reside on the Avaya Aura® Contact Center server which is Microsoft Windows based.

4.3.1 Windows based Media Server considerations

Avaya Media Server co-resident on the AACC Windows server is subject to the AACC Windows firewall policy. Please see section on Firewall policy

4.3.2 Linux based Media Server considerations

4.3.2.1 Linux firewall

As with Microsoft Windows, Avaya Media Server on Linux utilizes a firewall via iptables. iptables are the tables provided by the Linux kernel firewall and the chains and rules it stores. Upon installation an iptable is provided. Restart the Linux firewall using the following command: service iptables start

4.4 Contact Center Multimedia (CCMM)

Contact Center Multimedia interacts with an external email system and enables agents to send attachment files from their computers to the Contact Center Multimedia server. Both methods of retrieving data are potential sources of software infection.

4.4.1 Antivirus software considerations

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Contact Center Multimedia server do not have a virus. Contact Center Multimedia does not block specific attachment file types. Third-party antivirus software must be installed on the Portal Server according to guidelines in this document for such utilities.
- Exclude the Contact Center Multimedia partition from being scanned.

Warning:

Running a Virus Scan on the Contact Center Multimedia attachment folder, which contains thousands of files, can use significant CPU time on a server and can cause drastic slowdown in agent's response times. Avaya recommends that you run scans, if necessary, during off-peak hours.

4.4.2 Firewall considerations

If a firewall is enabled on the Agent Desktop computer, the Report Listener may be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.

You must not enable the Microsoft Updater to Auto-Run on the CCMM server. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

4.4.3 Spam Filter

You must install and actively manage a spam filter to remove spam messages from all contact center mailboxes. Unsolicited bulk spam messages to your Contact Center, if not filtered out, may impact performance or may cause damage to your contact center solution.

4.4.4 Enabling secure communication on Email Manager

` By default, CCMM will communicate with the Email Server over plain text. This communication channel is used for the mailbox login, email retrieval and sending using POP3/SMTP protocol.

` Normally, both the AACC Multimedia server and the Email Server will be within your corporate intranet. However, for additional security, you can use POP3/SMTP over SSL. A setting that may be required by your mail server.

For additional details please refer to section *Enabling SSL on the Email Manager* on the *Avaya Aura® Contact Center Server Administration* guide *(44400-610)* from www.avaya.com/support

4.4.5 SSL support for Multimedia and Outbound administration

It must be noted that on a fully co-res system, SSL is not supported. Sites should deploy a standalone AACC-Multimedia server if they want SSL enabled for CCMA.

4.5.6 Address Book Service connecting to the LDAP server over SSL

AACC-Multimedia supports an address book populated from a corporate LDAP directory. The Address Book Service is capable of connecting to the LDAP server over SSL. To enabled, check the Use SSL checkbox when adding/editing the LDAP Server as described in the *Avaya Aura® Contact Center Server Administration* guide *(44400-610)* from www.avaya.com/support

4.5.7 Email retrieval over POP3 or IMAP

AACC-Multimedia supports email retrieval over POP3 or IMAP. Either of these protocols can be secured over SSL or TLS, provided your mail server supports it. Using TLS sends the *STARTTLS* command to the mail server.

STARTTLS is an extension to plain text communication protocols, which offers a way to upgrade a plain text connection to an encrypted (TLS or SSL) connection instead of using a separate port for encrypted communication.

For additional information on STARTTLS please refer to http://www.ietf.org/rfc/rfc2487.txt

4.5 Service-oriented architecture (SOA) Open Interface (OI)

SOA OI uses the standard java keystore in JKS-format to store X.509 certificates for establishing trust and RSA public/private keys used to establish secure TLS connections. At the time of writing the size of the RSA keys generated by the CCT Console configuration utility are 1024-bit.

For more information regarding the keytool command please see
http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html

For configuring the CCT Server to use TLS please use the CCT Console. The CCT Console can generate certificate signing requests and will create the keystore automatically from the user interface so that they keytool command line interface (CLI) command doesn't have to be used directly. The CCT Console will also configure SOA OI web services to be reachable via HTTPS. The CCT Console utility will also store the password for accessing the keystore in an encrypted format in the same directory as the keystore can be found. More information can be found in the SOA OI SDK Documentation.

4.6 Avaya Aura® Contact Center Security Framework Server

This server, when installed will provide identity management, authorization, and single sign-on (SSO) authentication for contact center solution users. Security Framework provides session management and integrates with your directory services infrastructure (AD) to reduce administrative costs and eliminate the redundant user information associated with application solutions.

4.6.1 Security Framework deployments

If you plan to use a single security domain for single sign-on for multiple applications in your network, you must determine and configure all applications to access the primary security server. The following list describes where to host the primary security server based on the deployed applications:

- Avaya Communication Server 1000.

  If the Avaya Communication Server 1000 application is on your network, it must host the primary security server.

- Contact Center.

  If a Contact Center application is on your network with no Avaya Communication Server 1000 application, use the Contact Center application to host the primary security server.

- Avaya Media Server (AMS) or NMC.

  For example, if your network uses Avaya Communication Server 1000 and you want to enable the single sign-on feature for all applications including Contact Center and AMS, you must configure Avaya Communication Server 1000 to host the primary security server, or security domain in your network. If you do not want to configure your application as part of the single security domain, follow the documentation for your specific application to configure the security server for the application.

  If you configure a backup security server in your network configuration, use the same configuration as described for the primary security application. Security Framework is not supported co-resident with Avaya Media Server.

4.6.2 Remote support access tool

You must configure a remote support access tool on the server to provide remote support for the Security Framework. You can use LogMeIn Rescue from LogMeIn (www.logmein.com).

LogMeIn Rescue supports remote systems over the Web without installing software. Please refer to the LogMeIn Rescue Connection guide on how to setup connectivity to a server. LogMeIn Rescue Connection Guide

You can use the Remote Desktop Connection feature in Windows as an alternative for remote support access tool instead of LogMeIn Rescue. Remote Desktop Connection is supported in console or admin mode only. Refer to the Microsoft Web site for details about how to verify that you are connected to the console/admin session (session 0).

4.7 Remote support access

Avaya requires you to install an Avaya Secure Access Link (SAL) server to provide remote support. You use the remote desktop service feature in Windows along with the SAL to gain remote access to the AACC server.

4.7.1 Avaya Secure Access Link (SAL)

Avaya Aura® Contact Center supports Avaya Secure Access Link (SAL). SAL is a remote access architecture that provides simplified network management and increased support options for greater security, reliability and flexibility. SAL gives you complete control of when and how Avaya, or any other service partner, can access your equipment. You can take advantage of channel-neutral support by enabling self-service, Avaya, and/or business-partner support of your networks.

Secure Access Link offers security, reliability, and flexibility for network connections. Secure Access Link also helps you optimize network communications by opening the door to a suite of Avaya services and tools that enable faster issue resolution and increased communications uptime.

Avaya Secure Access Link architecture includes several software-driven components, two of which reside in your network.

For more information about Avaya Secure Access Link, see www.avaya.com/support

4.7.2 Microsoft Windows® Remote Desktop

In conjunction with SAL, you must connect to the remote server using Microsoft Windows® remote desktop service. This service must be turned on. Please refer to Microsoft Windows Remote Desktop for information on enabling the remote desktop service.

4.8 Configurable Security

The Avaya Aura Contact Center solution out of the box requires secure SIP signaling between the contact center server and Avaya Enablement Services (AES) server. Signed security certificates are used to secure the link between the CCMS and the AES. SIP provides a standard means to establish sessions, negotiate capabilities, and invoke applications.

The solution supports Transport Layer Security (TLS) to secure the signaling between SIP endpoints. It uses OpenSSL technology to negotiate and establish these connections.

Please refer to *Avaya Aura® Contact Center Commissioning guide (44400-312)* Chapter 12 Contact Center Manager Server certificate commissioning.

4.8.1 Transport Layer Security (TLS)

TLS is a public key encryption cryptographic protocol that helps secure a communications channel, providing privacy and safety. With public key cryptography, two keys are created, one public and one private. Anything encrypted with either key can be decrypted only with the corresponding key. Thus if a message is encrypted with the server's private key, it can be decrypted only using its corresponding public key, ensuring that the data must have come from the server.

4.8.2 Digital Certificate Management

Avaya Aura® AACC Server utilizes digital certificates to set up a trust with other SIP endpoints. Avaya follows the industry standards on the application and use of digital certificates. It utilizes a standard java key store in JKS-format to store X.509 certificates for establishing trust and RSA public/private keys used to establish secure TLS connections.

4.8.3 Digital Certificate template version support

SIP enabled AACC supports version 1, 2 and 3 security templates.

4.8.4 Digital Certificate template key length support

Certificate Manager, SOA OI supports 2048 Key length digital certificates and is backward compatible with 1024 key length digital certificates, but note that use of such digital certificates are deemed insecure since January 2011 and should not be used.

While the Aura solution can support lesser key lengths, 1024 for example, it is advised that if an in-house Certificate Authority is being used to sign security certificates, to ensure that is has the ability to sign RSA 2048 key length security certificates.

4.8.5 SHA256 encryption support

In release 6.4 any application that generates Certificate Signing Requests (CSR) and negotiates with digital signing requests will be able to do so in SHA256 encryption level.

4.8.6 Backward computability with older SHA1 encryption

To ensure that existing installations can continue to operate, especially if they have an in-house certificate authority and no desire to change its configuration to sign SHA256 CSR's then Certificate Manager and SOA OI will allow the selection of SHA1 encryption.

Note:

Selection of SHA1 will result in a visual warning message which advises that the selection of this encryption level is not deemed secure anymore. The administrator who configures this level of encryption does so at their own volition.

4.8.7 Default passwords

Several components of the solution come with default passwords. It is recommended that once initial commissioning has been completed, these passwords are changed and that a record of them is placed in a secure location off the server(s).

4.8.8 Certificate Manager

Maintenance of the digital certificates in use by the server is facilitated by the Certificate Manager. This application allows the customer to generate certificate signing requests (CSR), add, remove, export and view PKCS#12, signed and root digital certificates being used.

4.8.8.1 Certificate Manager Security

Access to the Certificate Manager application is password protected and encrypted.

Note: The default password that comes with the application when installed should be changed and a record of it should be stored off server for cases where it is forgotten as the password while stored on the server itself is encrypted and not human readable.

4.9 Configuring Data Execution Prevention (DEP)

Configure the Data Execution Prevention (DEP) hardware and software to perform additional checks on memory that protect the Avaya Aura® Contact Center server against malicious code exploitation and prevent certain exploits that store code via a buffer overflow.

Please refer to Changing Data Execution Prevention settings

5.0 Server Message Block Signing (SMB)

SMB signing is available in all currently supported versions of Windows, but it's only enabled by default on Domain Controllers. While SMB signing can be configured for the Workstation service and for the Server service, where the workstation service is used for outgoing connections and the Server service is used for incoming connections, Avaya Aura Contact Center 6.4 has been tested with the default settings that are set when the Windows operating system is installed.

Avaya Aura Contact Center 6.4 has not been tested with any other SMB signing configuration changes that deviate from the default settings.

6.0 PCI DSS (Payment_Card_Industry_Data_Security_Standard)

Avaya Aura Contact Center 6.4 makes no claim of PCI compliant for voice or Multi Media transactions.

AACC may form part of a PCI compliant solution subject to detailed requirements, implementation and validation. For example an IVR may be used in tandem with AACC to solely collect PCI information on voice calls. In that way AACC does not handle the PCI data at all. Solutions for other contact types such as email may also be designed such that AACC would not handle the PCI written information.

Definitions

AACC	- Avaya Aura® Contact Center
CCMM	- Contact Center Multimedia Server
CCMA	- Contact Center Manager Administrator
CCT	- Communication Control Toolkit
CCLM	- Contact Center License Manager
AMS	- Avaya Media Server (Windows and Linux)
CS 1000	- Communication Server 1000
CCMA	- Contact Center Manager Administration
AD-LDS	- Active Directory Lightweight Directory Services
CLAN	- Customer Local Area Network
NIST	- National Institute of Standards and Technology
CPU	- Central Processing Unit
VM	- Virtual Machine
DEP	- Data Execution Prevention
CCT	- Communication Control Toolkit
TCP	- Transmission Control Protocol
TLS	- Transport Layer Security
WCF	- Windows Communication Foundation
IIS	- Internet Information Services
http	- Hypertext Transfer Protocol
https	- Hypertext Transfer Protocol Secure
SSL	- Secure Sockets Layer
Email	- Electronic Mail
SOA	- Service-Oriented Architecture

OI	- Open Interface
CLI	- Command-Line Interface
SSO	- Single Sign On
NMC	- Nortel Multimedia Conferencing
SAL	- Secure Access Link
JKS	- Java KeyStore
RSA	- Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman Algorithm for public-key cryptography