Avaya Aura® Contact Center and Avaya Contact Center Select

Security Reference Guide

Release 7.1.0.3

July 2020

ver. 07.00

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 (AACC) and Avaya Contact Center Select (ACCS) Release 7.1.0 security features and considerations. Avaya Aura® Contact Center and Select 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 Contact Center Select (ACCS) is derived from Avaya Aura® Contact Center and supports a subset of its APIs, namely Web Communications Web services, Email Open Interfaces, CCT .Net API, Real-time Data API, Real-time Statistics Multicast API and Host Data Exchange API.

- Avaya Aura® Contact Center (AACC) and Select (ACCS) server operating system security.
- Avaya Aura® Contact Center (AACC) and Select (ACCS) software security.
- Avaya Aura® Contact Center (AACC) and Select (ACCS) solution security.

AACC and ACCS provide 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 Contact Center Select supports voice calls on the following voice platforms:

IP Office™ Platform. Avaya Contact Center Select integrates with the IP Office™ platform. This integration gives Supports skill-based routing, call treatments, reporting and unified agent management.

Avaya Aura® Contact Center and Avaya Contact Center Select 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. The Contact Center supports the following multimedia contact types:

1. Email

2. Routed Instant Message (IM)

   [Peer to Peer IM only on ACCS]

3. Web communications
4. Outbound
5. SMS text
6. Faxed document
7. Scanned document
8. Voice mail
9. Agent controls browser application
10. Video

Both solutions require 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 Contact Center client software, agent desktop computer, Windows domain, and security considerations.

You must consider security when designing, planning, commissioning, and maintaining an Avaya 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 Overview and Specification* 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* and *Avaya Communication Server 1000 Integration*.

For more information about Avaya Aura® Contact Center and the Avaya Aura® Unified Communications platform, see *Avaya Aura® Contact and Avaya Aura® Unified Communications Integration.*

1.1 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 and Avaya Contact Center Select overview

The Avaya Aura® Contact Center and Avaya Contact Center Select solutions needs to be resilient to attacks that can cause service disruption, malfunction, theft of information, or theft of service.

The solutions suite of applications includes the following components:

Contact Center Manager Server (CCMS)

Contact Center Multimedia Server (CCMM)

Contact Center Manager Administration (CCMA)

Avaya Communication Control Toolkit (CCT)

Contact Center Licence Manager (CCLM)

Avaya Aura Media Server (AAMS) (Red Hat Linux)

Orchestration Designer (OD)

Avaya Agent Desktop (AAD)

Agent controls browser application

Workspaces (WS)

3. 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 2012/Windows 2016 platform. Later sections cover the specific requirements of individual AACC applications.

3.2 Contact Center firewall Installed by default

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

3.3 Listing of ports and transport types

The Contact Center 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 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 and Avaya Contact Center Select 7.1.0 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 and Avaya Contact Center Select 7.1.0 Port Matrix* document on *www.avaya.com/support*

For network and port information specific to AACC, refer to the *Avaya Aura® Contact Center* Overview and Specification*. See www.avaya.com/support*

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 Contact Center firewall policy allows Avaya Aura® Contact Center and Avaya Contact Center Select to operate with Windows Firewall switched on. The AACC/ACCS firewall policy is configured based on the default product install options and the one firewall policy covers both solutions.

The firewall is automatically applied upon installation of the contact centre installation process and can be viewed on the server after installation.

4.1 Reviewing the AACC/ACCS firewall policy

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

4.2 Accessing the Microsoft Windows Firewall with Advanced Security application

1. Log on to an AACC/ACCS server that has the Avaya 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 /ACCS server once this policy has been implemented.

4.3 Backing up your Firewall Policy

Avaya recommends that you export and backup your existing firewall security policy before importing the Avaya 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 Overview and Specification.*

5. Group Policies

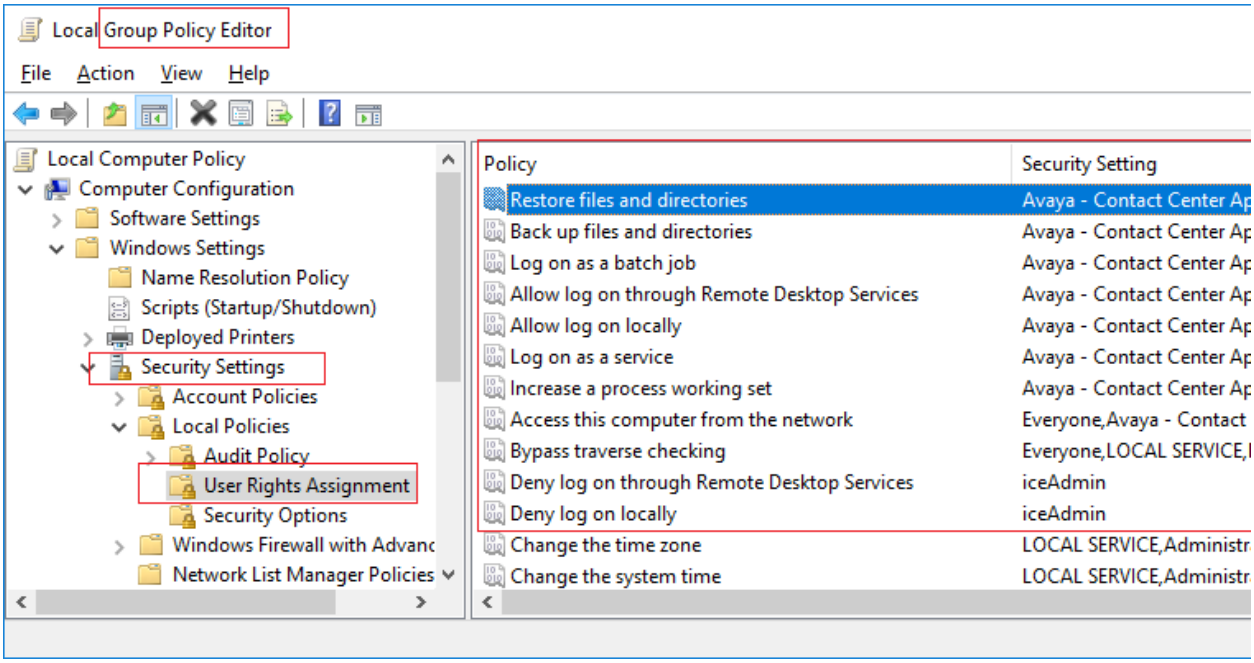
The Avaya contact center firewall policy defines the services, network ports, and Windows accounts necessary for secure Contact Center voice and multimedia functionality. Avaya Aura® Contact Center or Avaya Contact Server Select does not provide or install a group policy.

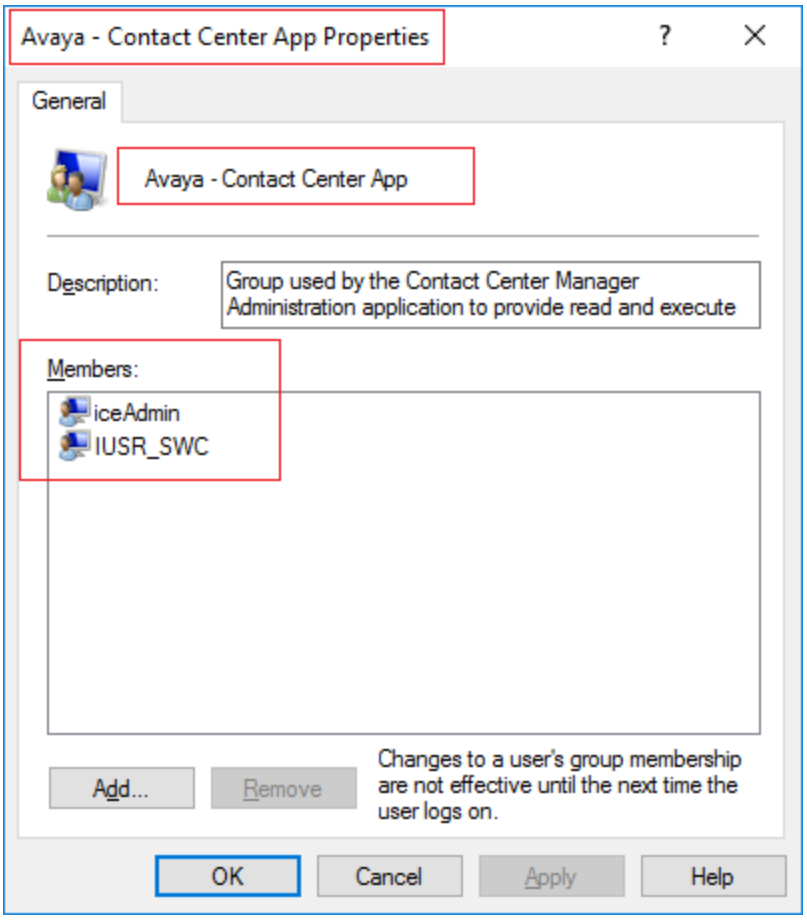
Domain group policies and security policies can be configured to automate MS Windows updates, server backups, and password expiry rules for local users. These automated features are not supported by AACC/ACCS. If your group policies or security policies implement these automated features, place the AACC/ACCS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

Contact Center App group and iceAdmin user applied to the following security policies.
The Avaya - Contact Center App group contains of two users, iceAdmin and IUSR_SWC.





If AACC/ACCS servers join domain server and domain policy has changes with these policies, CCMA may not be functional.

5.1 Working with Avaya Aura® Contact Center/Avaya Contact Server Select

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

1. Understand the AACC/ACCS 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 and Avaya Contact Center Select 7.1 Port Matrix document available at www.avaya.com/support.

3. Design or modify your group policy to accommodate these existing AACC/ACCS services, ports, user accounts, and transport type requirements.
4. During an AACC maintenance window, apply and test your group policy. Ensure AACC/ACCS 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/ACCS functionality.
5. After successful testing, place AACC/ACCS 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 or Avaya Contact Center Server solution cannot be changed to accommodate individual corporate group policies, so corporate group policies must accommodate the Avaya contact center solutions, AACC or ACCS.

5.2 Working with AACC/ACCS Windows Accounts

The contact center uses several Microsoft Windows® accounts. The group policy must work in conjunction with the AACC/ACCS Microsoft firewall policy.

The Contact Center uses several Windows accounts to communicate and access resources in the solution.

5.2.1 Accounts used by Avaya Aura® Contact Center/Avaya Contact Center Select

5.2.1.1 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.

5.2.1.2 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.

5.2.1.3 iceAdmin

The iceAdmin account is a member of a Avaya - Contact Center App group; it is used by the Contact Center Manager Administration (CCMA)

5.2.1.4 IUSR_SWC

Member of the Avaya - Contact Center App 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 attaches documents to multimedia contacts.

6. Default services and privileges installed by Operating system

The standard Windows 2012/ Windows 2016 installation has several services which are enabled and on by default. Some of these services, such as Remote Desktop (Terminal Services), have default user accounts with rights to log onto the system.

Avaya does not explicitly remove accounts or disable services that are installed and enabled during the operating system installation as each customer has specific criteria on what is required and enabled and what is not. But the following section will describe how to disable such services which may pose a security threat

6.1 Network Level Authentication (Terminal Services)

Currently Terminal Services on the AACC/ACCS server is enabled by default. This is to facilitate remote support and configuration of the server. It is understood that, dependent on each individual company's policies, this may not be desirable.

Any account with the right to log on through Remote Desktop Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, malicious users might download and run software that elevates their user rights.

The following section describes two options available to the customer dependent on their particular security policies to either disable terminal services or to leave on but add an additional security aspect when accessing the server from a remote location.

6.1.1 Disabling Terminal Services

If having terminal services enabled on the AACC/ACCS server does not meet specific security requirements it can be disabled.

Note:

Disabling terminal services will prevent any support personnel or remote configuration / patch installation from being possible. It is up the customer to determine if turning on terminal services meets their security policies to accommodate the aforementioned remote services.

To disable Terminal Services connections

Select System Manager (Search system manager and launch)

Select Remote settings

On the Remote tab, clear the *Allow users to connect remotely to your computer* check box, and then click OK.

The terminal server no longer accepts new connections, but existing connections are maintained until closed by the users. This allows administrators to shut down a terminal server gradually.

Notes

You must be logged on as Administrator or a member of the Administrators group to disable Terminal Services connections.

6.1.2 Limit users to access Network Level Authentication (NLA) for Terminal Services

If disabling Terminal services is not acceptable and remote access to the server is required for services relevant to company network policies then the following can be added to remote desktop access to enhance security accessing the server.

By default local administrator credentials are set to be able to use NLA and therefore access the server remotely. This is a standard Microsoft Windows installation configuration setting and as such if one server or account using remote desktop is compromised then in theory if no changes are made to other servers then they are also compromised. Removing or customizing the users that have access to remote desktop will prevent such a situation.

6.1.3 Network Level Authentication

Network Level Authentication used in Remote Desktop Services (Server) or Remote Desktop Connection (Client) that requires the connecting user to authenticate before a session is established with the server.

NLA prevents this automatic establishment of a session with the server and prompts the user to authenticate before establishing any session on the server.

This is a more secure authentication method that can help protect the remote computer from malicious users and malicious software.

This is on by default on AACC/ACCS 7.1, but to further limit access to the server one can add specific users and remove users that can use NLA and access the server

6.1.3.1 Requirements to use NLA

Before setting up NLA the following must be considered.

The client computer must be using at least Remote Desktop Connection 6.0.

The client computer must be using an operating system, such as Windows 8.1, Windows 8, Windows 7, Windows Vista, or Windows XP with Service Pack 3, which supports the Credential Security Support Provider (CredSSP) protocol.

The Remote Desktop Session Host "server" must be running Windows Client: Vista or newer (Vista, 7, 8, 8.1)

6.1.3.2 Adding/Removing users that can use NLA for Terminal Services

Select System Manager (Search system manager and launch)

Select Remote settings

On the Remote tab, if not set already, check *Allow remote connections only from computers running Remote Desktop with Network Level Authentication (recommended)*

Select the *Select Users …* button and add, or remove as required, users that can access the server using NLA.

6.2 SMB v1 disabled

In this release SMB v1 has been disabled on the server due to the Wannacry ransomware attack where it actively uses vulnerability in SMB v1 to instigate a man in the middle attack.

This may impact legacy operating systems and Linux when attempting to mount a drive on the server. If this is required and SMB v2/3 cannot be used in its stead then the following Powershell cmdlet can be used to re-enable SMB v1

Windows Server 2012 introduces the new Set-SMBServerConfiguration Windows PowerShell cmdlet. The cmdlet enables you to enable or disable the SMBv1, SMBv2, and SMBv3 protocols on the server component.

To obtain the current state of the SMB server protocol configuration, run the following cmdlet:

```
Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol
```

To disable SMBv1 on the SMB server, run the following cmdlet:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

To enable SMBv1 on the SMB server, run the following cmdlet:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $true
```

6.3 Server Message Block (SMB) Signing

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol. The Microsoft SMB Protocol is a client-server implementation and consists of a set of data packets, each containing a request sent by the client or a response sent by the server.

Server Message Block security has two main components: user-level and share-level. The first is for accessing servers, and the second is for accessing files, folders, and printers if share-level authentication has been configured on the server.

6.3.1 SMB Signing

SMB signing places a digital “tag” into each server message block. This signature or tag is used by both SMB clients and servers to prevent so-called “man-in-the-middle” attacks and guarantee

that SMB communications are not altered. SMB signing is off by default on standard Windows installations. In release 7.0.1 SMB signing will be on by default.

6.3.1.1 SMB Signing settings enabled by default

AACC and ACCS have enabled the following settings for SMB signing.

Policy Name	Enabled/Disabled
Microsoft network Server: Digitally sign communications (Always)	Enabled
Microsoft network Client: Digitally sign communications (always)	Enabled

6.3.2 To turn off SMB signing if required

If for any reason SMB signing is not acceptable on the network it can be disabled.

6.3.3 Group Policy settings

The recommended method is by using the local group policy settings on the server.

Open Windows Group Policy application (gpedit.msc from the command prompt if preferable).

Navigate in the left pane's tree to

Computer Configuration

Windows Settings

Security Settings

Local Policies

Security Options.

Scroll down to find the section of policies that begin with Microsoft network client or Microsoft network Server.

There are several elements in this list, the ones that are required to be turned off are:

Policy Name	Enabled/Disabled
Microsoft network Server: Digitally sign communications (If server agrees)	Disable
Microsoft network Server: Digitally sign communications (always)	Disable

6.3.4 SMB Encryption

In Windows 2012 R2 in SMB 3.0 is available in the Windows 8 client and Windows Server 2012. A new algorithm is used for SMB signing. SMB 2.x uses HMAC-SHA256. SMB 3.0 uses AES-CMAC. CMAC is based on a symmetric key block cipher (AES), whereas HMAC is based on a hash function (SHA)

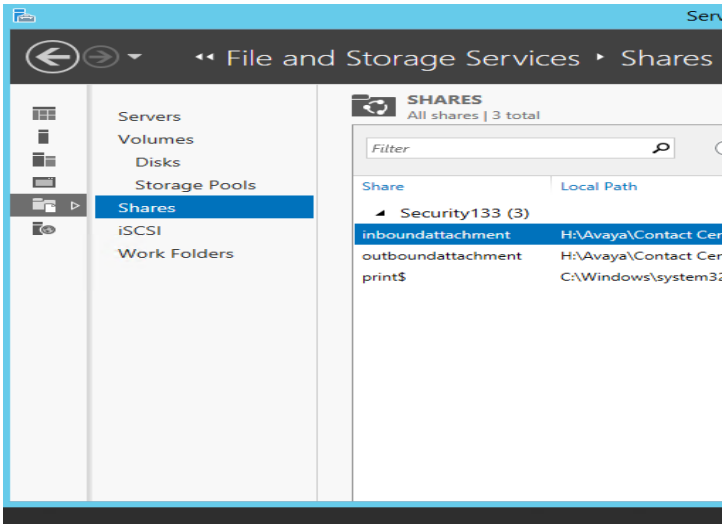
In SMB 3.0 there is the ability to encrypt the SMB data while it's in transit. Encryption in transit protects the communications from eavesdropping if intercepted as it passes through the network.

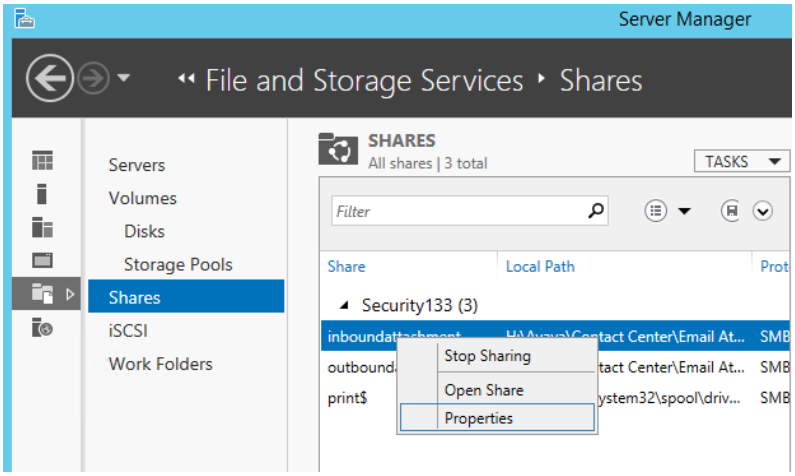
Specific shares can use this encryption in Server 2012 via the File and Storage Services in Server Manager. This can be done on existing shares on the AACC/ACCS server.

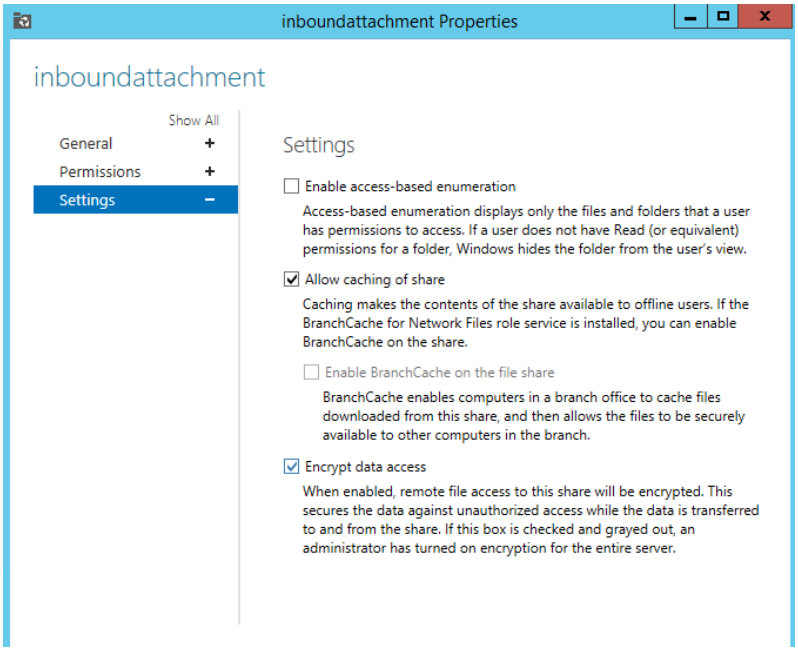
Select the share

Right click and select properties

Check the Encrypt data access option


File and Storage Services ▸ Shares
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
SHARES
All shares | 3 total
Filter
Share
Local Path
Security133 (3)
inboundattachment
H:\Avaya\Contact Cer
outboundattachment
H:\Avaya\Contact Cer
print$
C:\Windows\system32


Server Manager
File and Storage Services ▸ Shares
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
SHARES
All shares | 3 total
TASKS
Filter
Share
Local Path
Prot
Security133 (3)
Stop Sharing
Open Share
Properties
SMB


inboundattachment Properties
inboundattachment
Show All
General
Permissions
Settings
Settings
Enable access-based enumeration
Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.
Allow caching of share
Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.
Enable BranchCache on the file share
BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.
Encrypt data access
When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

6.4 Restricting NT LAN Manager (NTLM) authentication

In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. The protocol continues to be supported in Windows operating systems but has been replaced by Microsoft Kerberos as the default/standard.

6.4.1 Default setting on AACC/ACCS servers

On AACC/ACCS installations there are no modifications made that would restrict or audit NTLM authentication. This is due to the fact that each target network has their own rules and group policies and by forcing NTLM authentication restrictions onto the server may not adhere to local policies and therefore the decision to restrict, or audit, NTLM is left to the local administrator to apply.

6.4.2 Why restrict NTLM authentication

While NTLM is not the default standard it is still an option to be used if Kerberos authentication cannot be established with the major reason is to maintain compatibility with older systems.

Microsoft does not recommend its use as an authentication mechanism due to various well known vulnerabilities which can be exploited, such as “pass the hash” attack (reflection attack).

6.4.3 Decision to restrict or audit NTLM

For every policy to restrict NTLM there are alternative policies audit NTLM traffic rather than restrict. These permit the administrator to capture and analyze authentication activity between clients and member servers or within a domain before restricting the traffic and potentially causing service interruptions.

Based on the target network policies auditing may be more acceptable and if not then restrictions can then be applied.

6.4.4 Restricting NTLM traffic

If restrictions on NTLM is the decision made then an extensive plan and audit of its usage in the network needs to be executed before applying changes. Setting the policy Restrict *NTLM: NTLM authentication in this domain* without performing an impact assessment first might cause service outage for those applications and users still using NTLM authentication.

The three points at which to restrict NTLM traffic are:

NTLM traffic within a domain from a domain controller

NTLM traffic outbound from a remote server

NTLM traffic from a client computer to connected remote server

6.4.4.1 Using Security Policies

This document can only point out the main points on how to restrict NTLM, Microsoft has various articles detailing on the various steps to execute before finally restricting NTLM in your domain that should be adhered to.

Please refer to:

Assessing NTLM usage

https://technet.microsoft.com/en-us/library/jj865670.aspx

Restrict NTML usage

https://technet.microsoft.com/en-us/library/jj865676.aspx

Using security policies to restrict NTLM traffic

https://technet.microsoft.com/en-us/library/jj865668.aspx

6.4.4.2 Where to find Security policies

Open Windows Group Policy application (gpedit.msc from the command prompt if preferable).

Navigate in the left pane's tree to

Computer Configuration

Windows Settings

Security Settings

Local Policies

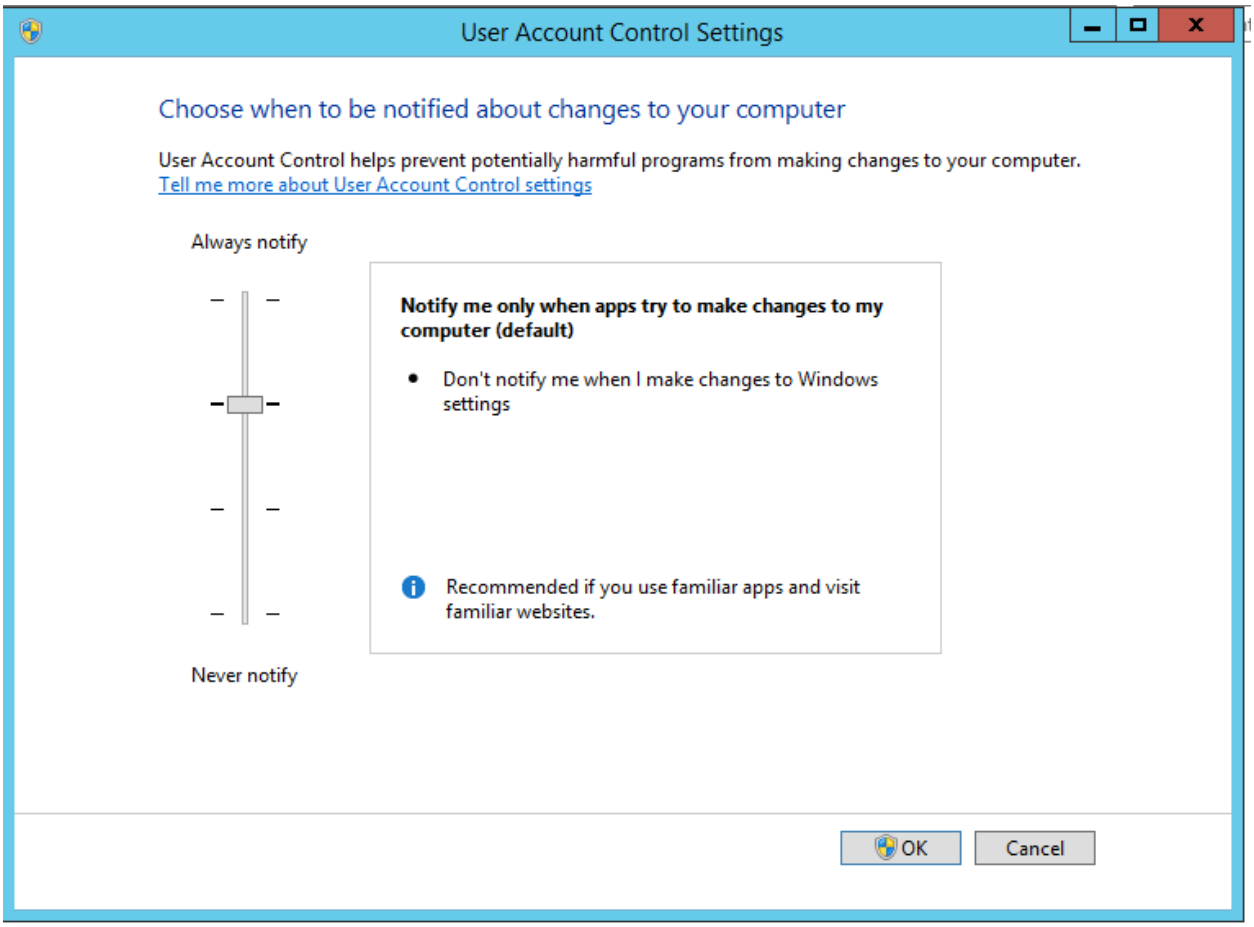
Security Options.

Search for Network Security: Restrict NTLM ….. Entries.

6.5 User Access Control

User Access Control ensures applications and services can't take administrator-level permission without consent. When changes need to be made to the computer a prompt will request permission to do so, requiring an administrator-level account to allow. If the logged on user is not at the administrator level, an administrator or equivalent is required to unlock the requesting function. The intent is to prevent malicious software from being installed or to make changes to the computer.

The default setting on Windows 2012 R2/ Windows 2016 is the third level “Notify me only when apps try to make changes to my computer (default)”. See screen shot below for reference



Currently AACC and ACCS can operate at this level. It cannot work at the highest level without impacting functionality.

6.6 SNMPv1 – SNMPv2 ports closed

In AACC-ACCS 7.1.0 release the UDP ports 161 and 162 which are typically used by SNMPv1/SNMPv2 are now actively blocked, turned off, by the AACC-ACCS firewall policy.

This is to tighten lock down and remove vulnerabilities known to use SNMP and these ports.

If these ports are required to be re-opened for any other reason, they are not required for the solution, then the firewall policy will have to be modified and a backup of the previous one be made. Responsibility then falls to the customer if they are reopened.

7. Role-based access control

Standard Windows operating system creates several local user groups in which user accounts can be added or removed. The following section will propose the creation of custom groups with a specific purpose which will allow the customer to control access to the resources on the system.

System Administrator Group

A read-write access to system parameters e.g. IP addresses, upgrade software. Any user assigned to this group would have the ability to start and stop services, and modify, assign, or define other roles and read/write access to create and modify logins.

Windows Sever 2012 R2/ Windows Sever 2016 has a built in *Administrators* group. Any user specifically created to operate as a System Administrator as defined above, should be added to this group. This user will then be granted the necessary permissions to operate at this elevated level.

Standard Windows Server Operating System installation places the built in *Administrators* users group in the Security Tab of all folders created on the server. This gives this group access to all areas of the server, any user added to this group would have total access to all areas of the server and should be planned carefully on what users are added to this group.

Auditor Group:

A read-only role for observing the system. The auditor is a user assigned to the Auditor group that has read only access to logs, security logs, configuration information and audit files. The user assigned to the Auditor role is not allowed to execute any command that may allow them to access another host.

Avaya Services Administrator Group

This role has read/write access to all operations and resources including the ability to start and stop services, and services diagnostic capabilities and can only be assigned to services accounts.

This role is required by Avaya services to effectively and efficiently troubleshoot system problems reported by alarms or by the customer.

The customer has full control on when this group is to be created. Access to the system by Avaya support personnel is a planned event and as such the customer dictates when the scheduled event is to take place and therefore when they deem to create this group to allow the Avaya support personnel to access to the system. This is in conjunction with a strictly defined access protocol agreed by and with the customer and Avaya support personnel.

Avaya Services Maintenance and Support roles

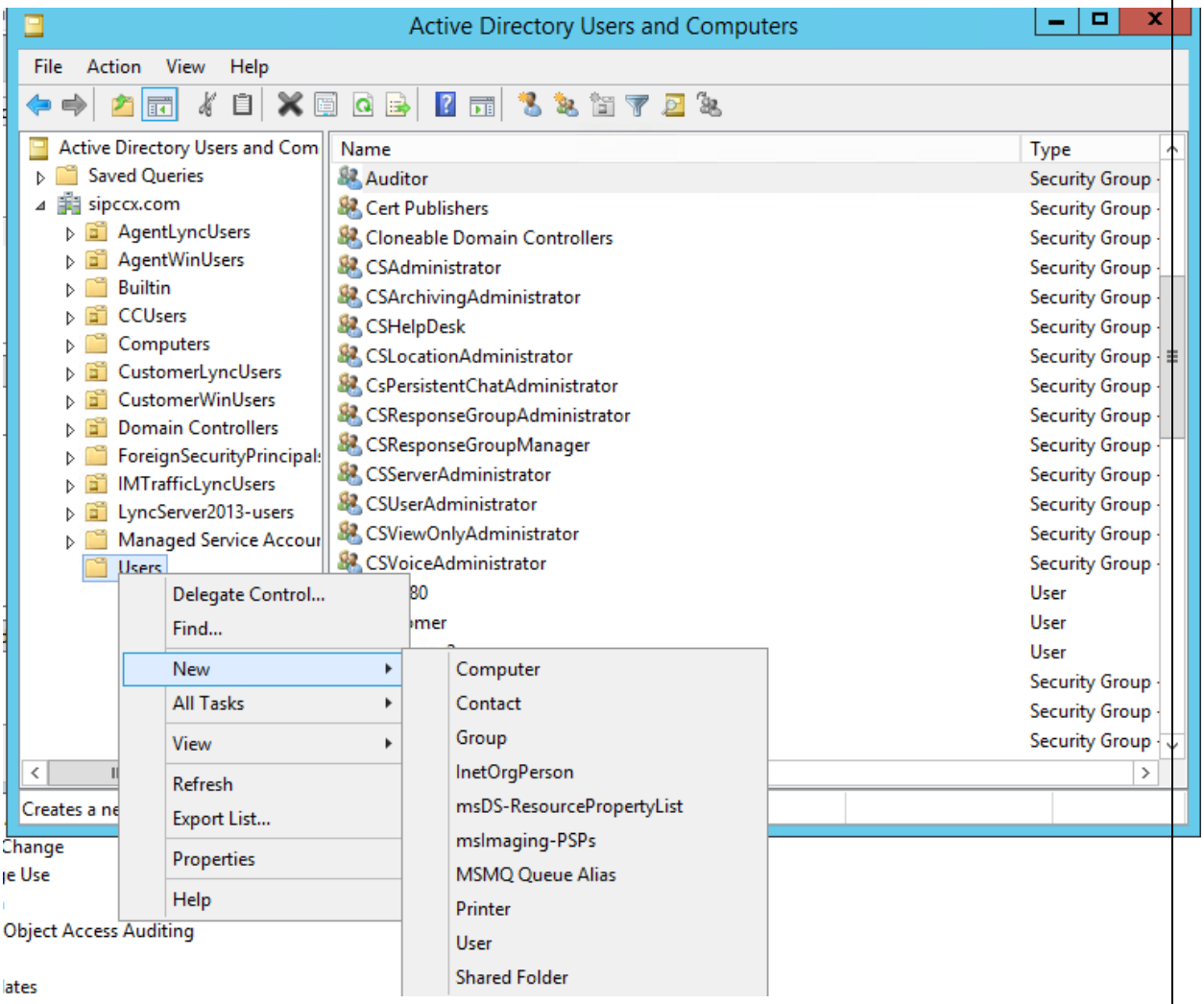
This role has read only access to maintenance logs, the ability to run diagnostics and view the output of diagnostics tools. The user assigned to the Avaya Services and Maintenance role is not allowed to execute any command that may allow them to access another host - host containment.

7.1 Creating a group

Open Active Directory Users and Computers which can be accessed from the start menu or search for Users and Computers and select the Active Directory Users and Computers suggestion listed below the search list.

Expand the tree on the left and select Users folder

Right select the folder and select New and Group to create a new group.



Name the group, see suggestions above, and select Ok.

The new group will be present in the right hand pane.

7.2 Adding members to the group

Double select the new group and select the Members tab

Hit the Add button

Enter in the user accounts you wish to use in this group

Hit Ok button

7.3 Assigning the group to a particular file or folder

Browse to the target file or folder and go to Properties and then Security tab

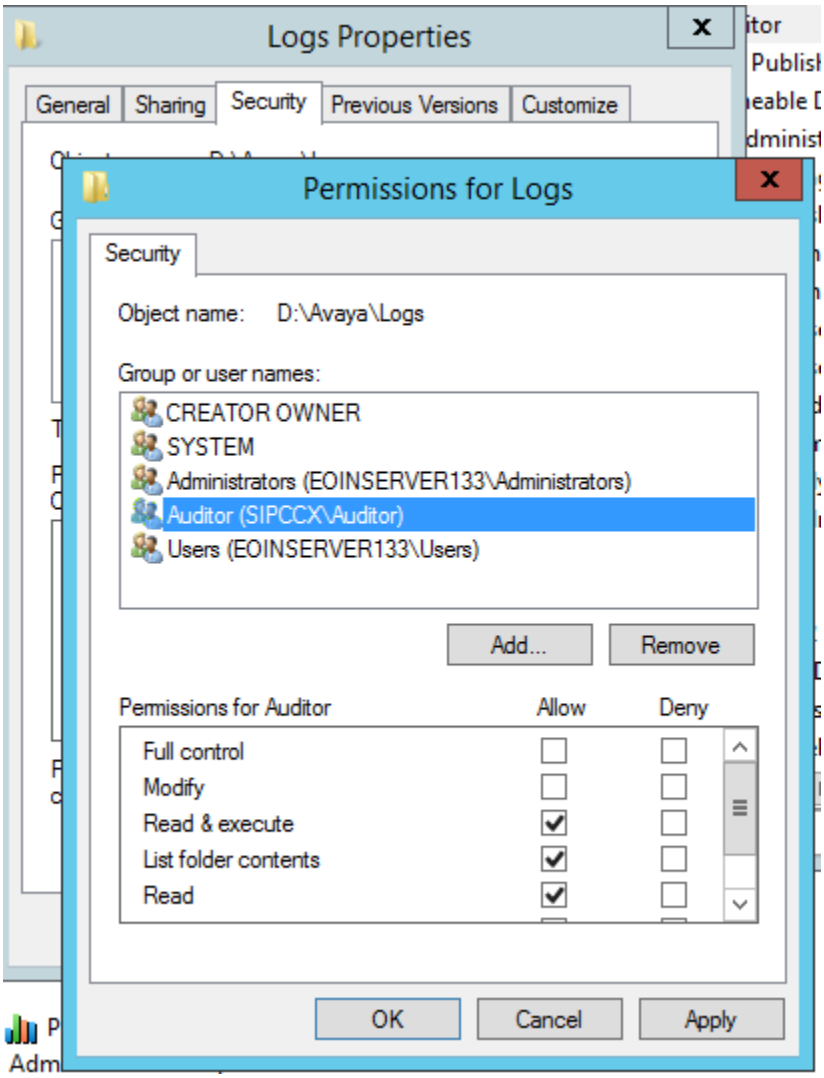
Select Edit

Then Add

Type in new group or groups created

7.4 Modifying the Permissions of this group on the folder

Once the group(s) has been added to a particular file or folder then permissions on that object can be modified to suit the group's level of permissions allowed



7.5 Work with Auditing

See Section 8 Configuring monitoring and Auditing AACC/ACCS Server (optional) for additional settings in relation to auditing actions on the objects that the group has been assigned to

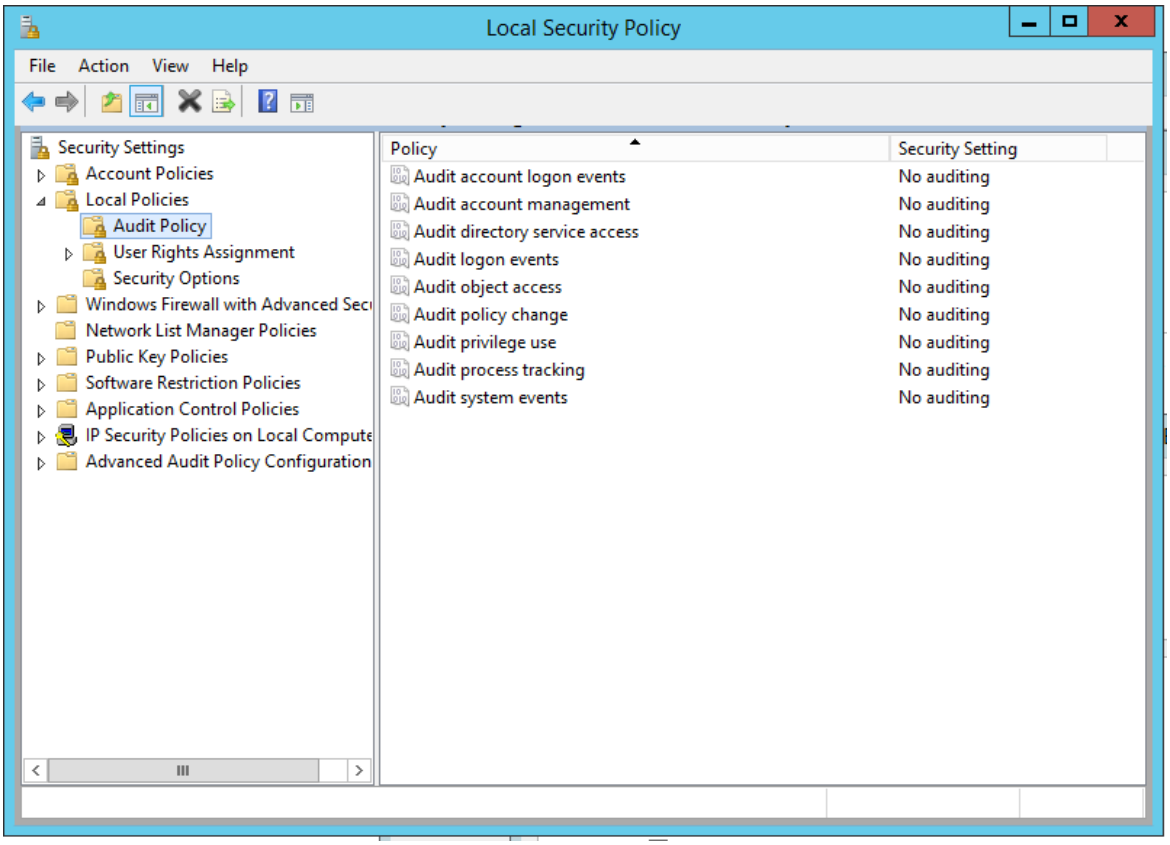
8. Configuring monitoring and Auditing AACC/ACCS Server

The standard installation of Microsoft Windows 2012 R2/ Microsoft Windows 2016 server has an extensive array of monitoring and auditing capabilities; these are not enabled by default but can be enabled to work in conjunction with the bespoke groups outlined in Role-based access control section to monitor the state of the system.

This section is only to identify the location of these audits and monitoring capabilities, Avaya Contact Center does not enable any of these during the suite installation process. Each can be enabled based on each customer's organizations security policies.

8.1 Standard Audit capabilities

Since Windows 2000 the standard audit capabilities have been available and are located in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policies node and are shown in the screen shot below



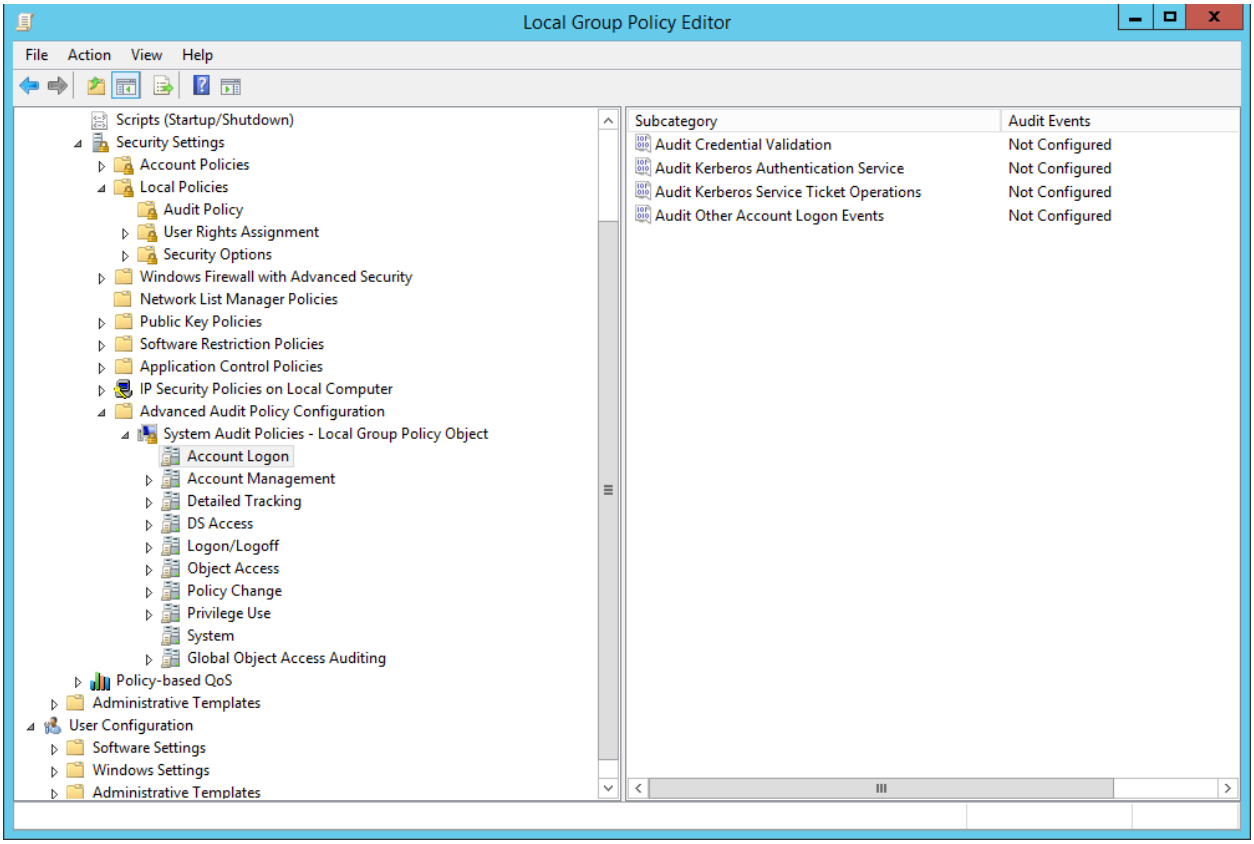
While these can be turned on they do not have the granular approach when they capture actions and events on the server and can record information that is not necessary relevant to your needs.

8.2 Advanced Audit policies

The goal here is to reduce the amount of data recorded and of the data that is captured, is to ensure that it dual needs of being easy to analyze while at the same time containing the relevant information to make a decision quickly.

Windows has an advanced audit policy which will allow it to be more specific to what you wish to audit. This is, as well, disabled by default, but can be enabled as you see fit.

It is located in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policies node, see screen shot below



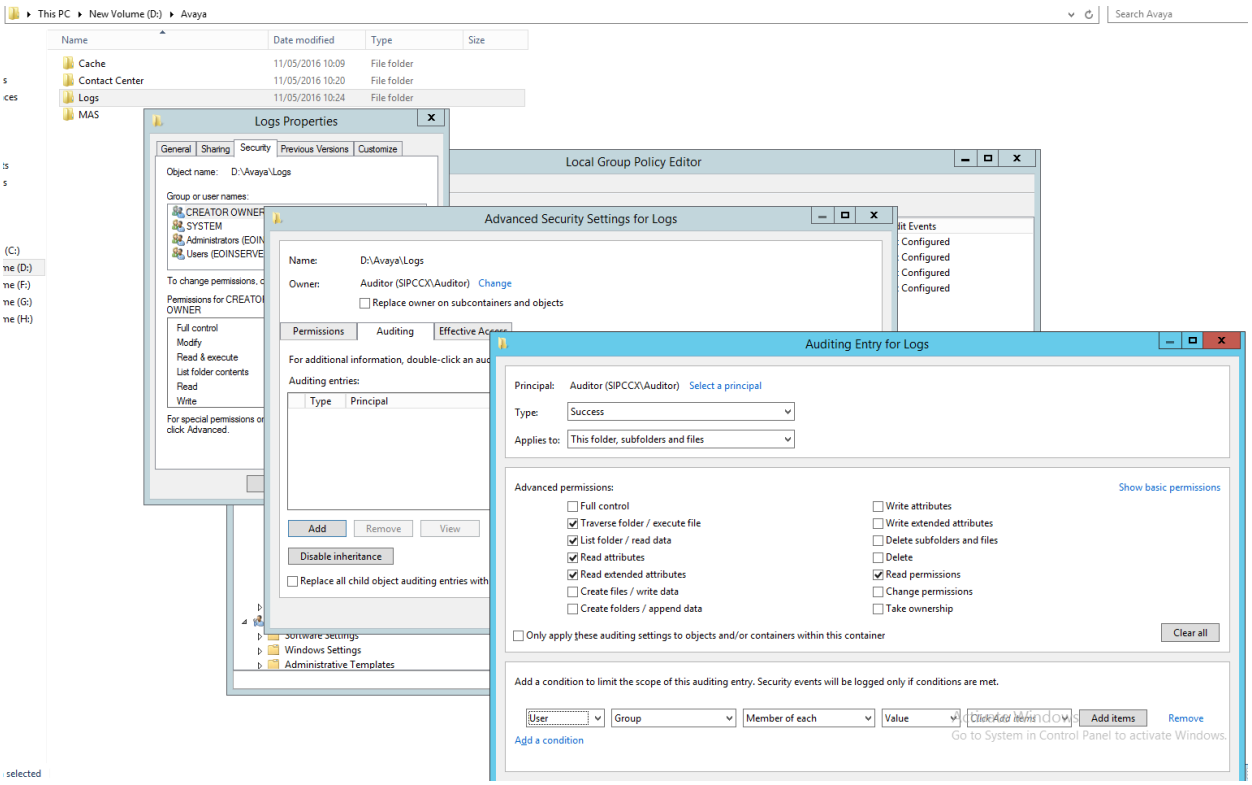
8.3 Groups and Auditing

So once your groups have been defined, it is a case of what activities that will trap and event written and recorded. An example is where say, a member of the Auditor group, accesses a file. This not only allows control of who has access to this file but when and what action was performed on it.

8.3.1 File and folder auditing

The level of granularity available in the auditing infrastructure on Microsoft Windows 2012 R2/ Microsoft Windows 2016 allows auditing on an individual file or folder. To access this all that needs to be done is through the *advanced* button on a file or folders properties Security tab.

In the example below you will see that the Auditor group has been added as the Principal group and the relevant permissions to be audited on the users in that particular group on the Avaya Logs folder.



Based on your particular needs auditing and creation of groups can be used to enhance the security and traceability of the Contact Center server. What level this is implemented will be dictated by the environment and policies dictated by the customer, Avaya does not implement

or enable the auditing detailed above to ensure it does not infringe in any local rules and policies.

9. Anti-Virus considerations

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

The Avaya Aura® Contact Center supported antivirus products are:

- Symantec Anti-Virus
- McAfee
- Microsoft Forefront

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.

9.1 Folder Exclusion List

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

- F:\Avaya\Contact Center\Databases\
- <additional database drive>:\Avaya\Contact Center\Databases
- TSM_OAM log folder location
- D:\Avaya\Contact Center\ and all folders under this parent
  - 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
  - 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
  - D:\Avaya\Contact Center\Workspaces
- The folder where you store Server Packs and patches

For more detail please refer section *Voice and Multimedia Contact Server antivirus software* on the *Avaya Aura Contact Center Overview and Specification* see www.avaya.com/support

10. Domain Considerations

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

10.1 Being a Domain member when installing AACC/ACCS

While it is possible to join a fully configured AACC/ACCS 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 *Avaya Aura Contact Center Overview and Specification* for further information.

10.2 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.

10.3 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.

11. 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.

11.1 Remote backup and restore security

CCMS, CCMM, CCT, CCMA 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 Maintaining Avaya Aura® Contact Center.

12. 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

An email is sent periodically by a dedicated Avaya resource listing all of the security patches that have been tested on a particular release. You can subscribe to this distribution list by emailing jamesca1@avaya.com .

Also refer to *Upgrading and patching Avaya Aura® Contact Center* on www.avaya.com/support, for details on the preparation procedures in applying patches and hot fixes to the servers.

12.1 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.

12.2 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

12.3 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.

12.4 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.

12.5 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.

13. 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.

13.1 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.

13.2 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

14. Communication Control Toolkit

14.1 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.

14.2 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.

14.3 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.

15. Avaya Contact Center Manager Administration

15.1 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 their own access and partition permissions that restrict which Contact Center Manager Administration components the user can access.

These same access and partitioning 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, CDNs etc.) that the Contact Center Manager Administration user can access. For AACC a default Contact Center Manager Administration user account named “webadmin” 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. This account is only relevant to AACC.

For ACCS, the default account created is named “Administrator”, the same principle applies to this account as it does to the AACC “webadmin” account regarding deletion and password changing.

All Contact Center Manager Administration user information including its password is saved in the Cache database on the Contact Center Manager Administration application server. 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.

15.1.1 Account Lockout

If the account lockout feature is enabled in CCMA then if the configured number of failed login attempts is reached by a user then that user will be locked out of the application for a predefined length of time. The new CCMA Security Settings dialog allows this lockout feature to be enabled and the lockout duration to be configured. The number of failed login attempts a user is allowed before being locked out is configurable, also in the CCMA Security Settings dialog. This feature is turned off by default.

15.1.2 Password Ageing

A password ageing feature is available in CCMA. If the amount of time elapsed from the password last modified date exceeds the maximum password age then the user is redirected to the Change Password page and informed that their password has expired. The maximum

password age is a value in days configured in the CCMA Security Settings dialog. A warning period time can also be configured in the CCMA Security Settings dialog. When specified this value is used to display a warning message to a user that their password is about to expire. This feature is turned off by default.

15.1.3 Force Password Change on First Login

Using this feature it is possible to force a user to change their password on their first login. This feature is configured in the CCMA Security Settings dialog. This feature is turned off by default.

15.2 Domain environments

15.2.1 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.

15.2.2 Securing CCMA Web Site outside the Security Manager Security Setting

On a new AACC/ACCS installation CCMA uses https by default if the Ignition Wizard security configuration has created and populated the AACC security store. IIS, if required can be configured manually outside the secure by default setting in Security Manager. But note that once Security Manager is used to remove or add a binding onto IIS there may be a mismatch with what was performed manually to what the automated securing of IIS performs and thus may require additional manual checks or tidying up to ensure that the state of IIS remains in a state you expect.

Please refer to *Section 22 Use of secure protocols by default upon installation* for additional details.

15.2.2.1 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.

15.2.2.2 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.

1. Log on to Contact Center Manager Administration.
2. Click Start > Run.
3. In the Open box, enter cmd.
4. At the command prompt, enter *wcApplyChanges -i*.

16. Avaya Aura Media Server

Avaya Aura Media Server runs on Red Hat Linux Operating System. It can operate as a single standalone entity on a separate server (or a VMWare OVA), can co-reside on the Avaya Aura® Contact Center server running as a Hyper-V virtual machine.

16.1 Red Hat Linux based Avaya Aura Media Server considerations

16.1.1 Linux firewall

As with Microsoft Windows, Avaya Aura 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. For Virtual Machines, the firewall policy is installed as part of the deployment. For AAMS installations on Customer obtained Red Hat Servers, an iptable file is provided. Restart the Linux firewall using the following command: service iptables start

17. 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.

17.1 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.

17.2 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.

17.3 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.

17.4 Enabling secure communication on Email Manager

` By default, CCMM will communicate with the Email Server over clear-text (i.e., no encryption). This communication channel is used for the mailbox login, email retrieval using POP3 or IMAP, and sending using 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 TLS. Such a configuration may be required by your mail server.

For additional details please refer to the following relevant sections in the *Avaya Aura® Contact Center Server Administration* guide *(44400-610)* from www.avaya.com/support

- *Configuring the email server names*
- *Adding an email server*
- *Adding a certificate for use with TLS email connections*

17.5 Email retrieval over POP3 or IMAP

AACC/ACCS-Multimedia supports email retrieval over POP3 or IMAP. Either of these protocols can be secured over TLS, provided your mail server supports it. AACC/ACCS-Multimedia Email Manager supports three distinct email retrieval configurations:

- Clear-Text
  - *No encryption.*
- STARTTLS
  - *TLS-secured communications initiated/negotiated over a clear-text connection.*
- TLS
  - *All client / server interaction over secured channel*
  - Note: *Some email servers may refer to this configuration as "SSL" depending on their level of backward compatibility support for the deprecated precursor of TLS.*

STARTTLS is an extension to clear-text communication protocols, which offers a way to upgrade a clear-text connection to an encrypted (TLS) 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

17.6 Address Book Service connecting to the LDAP server over TLS

AACC/ACCS-Multimedia supports an address book populated from a corporate LDAP directory. The Address Book Service is capable of connecting to the LDAP server over TLS. To enable, check the **Use TLS** checkbox when adding/editing the LDAP Server.

For additional details please refer to the following relevant sections in the *Avaya Aura® Contact Center Server Administration* guide *(44400-610)* from www.avaya.com/support

- *Configuring a Directory LDAP server*

17.7 Configuring Attachment Upload Location

The locations used for storing attachments received via customer emails (Inbound) as well as attachments to be sent on behalf of agents can be configured via the CCMM Administration interface.

For additional details please refer to the following relevant sections in the *Avaya Aura® Contact Center Server Administration* guide *(44400-610)* from www.avaya.com/support

- *Configuring the email settings*

17.8 Preventing Execution of Uploaded Attachments

CCMM web services are hosted on IIS. The IIS web server's behavior is controlled by a configuration file (`web.config`). There can be a version of this file for each web application folder under IIS. Settings in the current folder take precedence over settings inherited from a parent folder.

For security purposes the `accessPolicy` specified for folders where content can be uploaded should be restricted to prevent execution of (potentially malicious) uploaded content.

The recommended `web.config` for an attachments directory is shown in the left pane of Table 1. There is no `"Script"` entry in `accessPolicy` so IIS will not run script content (e.g., ASP, PHP) uploaded to this location. For CCMM outbound attachments the only required `accessPolicy` is `"Read"` as shown on the left of Table 1. This is the recommended configuration for folders to which users can upload content onto the CCMM server.

Directory browsing should also be disabled by setting the `directoryBrowse` for these locations as shown on the left.

Table 1

Recommended:

- ✓ Only *Read* accessPolicy
- ✓ Directory browsing disabled

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <handlers accessPolicy="Read" />
    <directoryBrowse enabled="false" />
  </system.webServer>
</configuration>
```

Note: accessPolicy values are case sensitive.

Not Recommended – Insecure Configuration:

- ✗ Including *Script* accessPolicy
- ✗ Directory browsing enabled

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <handlers accessPolicy="Read, Script" />
    <directoryBrowse enabled="true" />
  </system.webServer>
</configuration>
```

These settings can be controlled from the command line using the IIS `appcmd` utility,

```
appcmd set config "Default Web Site/outboundattachment" /section:handlers
/accessPolicy:"Read"

appcmd set config "Default Web Site/outboundattachment" /section:directoryBrowse
/enabled:"false"
```

The `appcmd` utility is installed as part of IIS: location `C:\Windows\System32\inetsrv` – note that this location is not on the `PATH` by default. The above commands can be executed from the `inetsrv` folder.

Note: These settings should be re-applied if the attachment location is changed via CCMM Admin as per section **Error! Reference source not found.**.

For further information on IIS handler configuration and `appcmd` usage please refer to the following 3rd party resources,

- IIS handlers: https://www.iis.net/configreference/system.webserver/handlers
- IIS appcmd: https://technet.microsoft.com/en-us/library/jj635852.aspx

18. Agent Greeting Recorder

The Agent Greeting recorder (AG) application is hosted on the Apache Tomcat instance included with Contact Center Manager Server installations. This Tomcat instance (and consequently the applications it hosts) relies upon the java keystore that is delivered with AACC/ACCS and administered via the Security Manager tool, for identity keys to accept inbound TLS connections.

The Agent Greeting recorder application also utilizes the same key store for trusted CA certificates needed to establish outbound TLS connections to other systems. The application interacts on the following communication channels, each of which may or may not utilize TLS secured connections depending upon system configuration:

- **SIP Inbound** – from Avaya Session Manager. Agents dial into the recorder application on a designated phone number which routes to the AG application through SM. By default, this connection utilizes the TCP protocol, but can be configured to use TLS connectivity through updating of the agentgreeting.properties file in the Tomcat conf directory and appropriate configuration of the Entity Link(s) defined in Session Manager routing. Ports 5080 (TCP) or 5081 (TLS) are listened on by default for this connection.
- **HTTP Outbound** – to CCMA REST web services. AG uses these to fetch basic application configuration from CCMA and also to query and update agent profiles when greeting recordings are captured or when agents change their AG password. Per default AG configuration, the use of TLS connectivity on this link falls in line with the enablement or otherwise of web services security for AACC/ACCS as set via the Security Manager tool. Ports 80 (TCP) or 443 (TLS) are used to connect to CCMA.
- **HTTP Outbound** – to AMS REST Web UserAgent endpoint. This link is used to anchor agent calls into the recorder application to AAMS and launch the recorder application dialog there. As above, the use of TLS connectivity for this link is, by default, pursuant to the overall web services security level for AACC/ACCS. Ports 7150 (TCP) or 7151 (TLS) are used to connect to the AAMS REST Web UserAgent.
- **HTTP Inbound** – from AAMS for fetching VXML dialogs and from web browsers for some configuration and basic troubleshooting tasks. The AACC/ACCS Tomcat service is configured with Connectors on ports 8081 and 8445 for inbound HTTP and HTTPS traffic respectively. When web services security is enabled on AACC/ACCS, the connector on port 8081 is disabled and hence non-TLS connections are not accepted accordingly.

19. 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/8/docs/technotes/tools/windows/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.

20. Avaya Aura® Contact Center System Manager Server

This server, when installed will provide identity management, authorization, and single sign-on (SSO) authentication for contact center solution users. System Manager 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.

20.1 System Manager 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 Aura Media Server (AAMS) 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 AAMS, 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.

20.2 Remote support access tool

You must configure a remote support access tool on the server to provide remote support for the System Manager. 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).

21. 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/ACCS server.

21.1 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

21.2 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 section 6.1 Network Level Authentication (Terminal Services) and the options available.

22. Use of secure protocols by default upon installation

In release 7.0 an initiative was put in place to secure a range of Contact Center Web Services and access to administrative applications by setting the communication type as HTTPS only, this is what is called *secure by default*.

After the installation, the following Web services accept only HTTPS requests from clients, and do not accept HTTP requests. This impacts the following connections:

- CCMA
- CCMM Administration
- Agent Desktop
- Multimedia Services
- Orchestration Designer
- Outbound Campaign Management Tool
- Contact Center Web Services
- CCT Web Administration.

This secure by default was continued in 7.1 release.

22.1 From 7.0.3 release – Removal of default OTB Security Store

A new initiative was implemented where the default out of the box (OTB) contact center security store was removed from new installs and therefore the installation of the solution may not be secure by default if the customer does not create and populate a security store for the server using the new Ignition Wizard Security configuration sections.

Removal of this OTB means that for AACC and ACCS there is no ready-made security store with security certificates available on new installations of the product and thus the customer will have to manually, through Ignition Wizard security configuration during the initial installation of the product or Security Manager after the installation and initial configuration process has been completed, create and populate the contact center security store to establish a working and secure solution.

22.1.1 AACC specific notes on removal of OTB store

By removing the default OTB store from new installations, if AACC customers do not configure and populate a security store then the SIP-CTI link to AES which requires mandatory TLS communication will be down and all features associated with this will not be available.

The system will be insecure without proper provision of the store.

22.1.2 ACCS specific notes on OTB store

By removing the default OTB store from new installations, if ACCS customers do not configure and populate a security store and they have not configured IPO to communicate over TCP then then the TAPID link to IPO will be down and all features associated with this will not be available.

In 7.1.0 there is now the option to set the transport type for communication to IPO on ACCS. Default is TLS but it can be set to TCP, this also requires configuration on IPO to facilitate TCP communication.

The system will be insecure without proper provision of the store.

22.2 TLS v1.2 now the default TLSv1 level

In previous releases TLS v1.0 was the default level of TLS on all AACC/ACCS services which could secure communications using TLS. From 7.1 this has now changed where TLS v1.2 is the default level of TLS to use and TLS v1.0 is disabled by default.

22.2.1 Fresh Installs and Migrations

In this release TLS v1.2 will now be the minimum TLS level supported when a fresh installation or migration is executed. This encompasses the services listed above in Section 22 *Use of secure protocols by default installation* plus also the SIP traffic when secured. When secure by default is set or selected by the customer TLS v1.2 is the only option when TLS negotiation is instigated.

TLS v1.0 and TLS v1.1 are actively disabled on the server in AACC/ACCS 7.1.

22.2.2 Upgrades

For upgrades or application of feature packs, the TLS level currently set on the underlying operating system will remain the same and will not be forced to use TLS v1.2.

This particular decision is to maintain functionality as much as possible when moving from a 7.0 system which may have legacy system in the solution that still require the lower levels of TLS.

While the installation of 7.1 will not modify the TLS level, as it does with a fresh installation, on an operating system level, which covers CCMA and the rest of Microsoft based technology applications as well as the application or service which wishes to access the server over a secure connection, it does not have control over all aspects of setting the TLS levels.

SIP traffic and Event Broker Web Services (EBWS) will be still set to TLS v1.2 upon installation and so if there is a need to move or reset these back to a lower level of TLS then please refer Security Manager where by launching this application and going to the security tab and selecting the appropriate TLS levels relating to the services mentioned above, will set the TLS levels required to maintain functionality.

22.3 Remote Desktop from Windows 7 clients

When TLS v1.2 is the default TLSv1 level set on AACC/ACCS server, specifically on the CCMA-Multimedia web service level, then on remote client machines who don't have installed a specific Microsoft patch will not be able to remote into the AACC/ACCS server.

This is due to the fact that client machines without this Microsoft patch can only connect over TLS v1.0 and if this is disabled on the AACC/ACCS server, via the setting mentioned above, they will fail to connect successfully.

The Microsoft patch provides support for Transport Layer Security (TLS) 1.1 and TLS 1.2 in Windows 7 Service Pack 1 (SP1) or Windows Server 2008 R2 SP1 for Remote Desktop Services (RDS).

Please refer to the following location and apply the update on any client machines that are required to connect to the AACC/ACCS server remotely

https://support.microsoft.com/en-us/kb/3080079

This is only required for client machines that are needed to remote to the AACC/ACCS server, otherwise this update is not required.

The other option is lowering the TLS v1 level on the CCMA-Multimedia web service level to TLS v1.0 and not update is required on any client machine to connect to the AACC/ACCS server. But note that this means that the CCMA application and Multimedia web services will now have the option to use TLS v1.0 and TLS v1.1 as well as TLS v1.2 when negotiating a secure connection.

22.4 Backward compatibility

Due to support for previous releases of applications and services which still require the lower levels of TLS v1, AACC/ACCS has the ability to allow the customer to select a lower level of TLS v1 protocol to suit their particular deployment.

22.4.1 SIP Signaling

AACC has a permanent secure link with AES (SIP-CTI) and with previous release of AACC. AACC 7.1 supports older versions of AES which can only support lower levels of TLS v1 and so below is a list of the AES versions and what level of TLS v1 they support and how AACC can be modified to change their TLS v1 level to ensure continued connectivity.

In addition to AES, Session Manager and Avaya Aura Media Server are two other endpoints typically used in a deployment that can also be secured using TLS, a matrix is also listed below for these also.

Note

This is not an extensive compatibility matrix please review appropriate documentation on the other applications and release to get details

22.4.1.1 AES releases and TLS v1 level support

AES Release	TLS v1.0 support	TLS v1.1 support	TLS v1.2 support	Options
6.3.3	YES	NO	NO	Would require SIP Signaling TLS v1 level to be lowered on AACC via Security Manager GUI
7.x	YES	YES	YES	
7.0.1	NO	NO	YES (default)	TLS v1.0 and TLS v1.1 can be enabled AES OAM/Admin Interface
8.1	YES	YES	YES (default)	TLS v1.0 and TLS v1.1 can be enabled AES OAM/Admin Interface

22.4.1.2 Session Manager Releases and TLS v1 level support

SM Release	TLS v1.0 support	TLS v1.1 support	TLS v1.2 support	Options
7.0.1	YES	YES	YES	
7.1	NO	NO	YES (Green Field sites only)	Minimum TLS version in SM R7.1 will be inherited from the release upgrading from The 7.1 SM EM running on SMGR will set the network global default to TLS 1.2 if it sees no SMs administered in the DB
8.1	NO	NO	YES	

22.4.1.3 AMS Releases and TLS v1 level support

AMS Release	TLS v1.0 support	TLS v1.1 support	TLS v1.2 support	Options
7.7 FP1	NO	NO	YES	Configurable (via Element Manager) TLSv1.0 or TLSv1.1 can be set instead if required.
8.0	NO	NO	YES	Configurable (via Element Manager) TLSv1.0 or TLSv1.1 can be set instead if required.

22.4.2 CCMA – Multimedia Web Service and Event Broker Web Service

The other services which can be set to a lower level of TLS to accommodate legacy application that either use or consume services are the CCMA application and Multimedia Web Services.

These can be changed from the Security Configuration tab on Security Manager, but what must be noted is that this change is made from a Windows operating system perspective and whatever TLSv1 level is set here basically covers the AACC/ACCS server from a Windows technology perspective. For AACC/ACCS this is IIS but any other Microsoft application that leverages TLS will be influenced by this setting.

This secures the AACC/ACCS server with this setting.

22.4.3 Skype for Business Server 2015 and AAD

The previous section outlines the impact of setting TLSv1 for CCMA- MM web services on Microsoft technology based applications.

AACC supports Skype for Business Server and incorporates Microsoft SDK to integrate Instant Messaging features into Agent Desktop application.

In its current implementation AAD can operate at TLS v1.2 level.

While running AAD on the AAAC server is not supported, if it was then the TLSv1 level set by CCMA- MM WS on AACC will have an impact on being able to log into Skype for Business Server 2015 if the TLSv1 level was set higher then TLS v1.0.

22.4.4 Event Broker Web Service

The other service which has the ability to set it TLSv1 level is Event Broker web service.

22.4.5 Security Manager Security Tab

As with the secure by default feature introduced in release 7.0, Security Manager Security tab has been expanded to give the customer a means to change the level of TLS v1 for the following services

SIP Signaling

CCMA – Multimedia Web Service

Event Broker Web Service

Each of these services can be changed to a lower level than the default TLS v1 level set (TLS v1.2)

They work in conjunction with the Security ON/OFF feature in that they are not used when Security is OFF, but once it is turned ON then the levels set, once the server has been rebooted, will be the TLS v1 levels available for TLS negotiation.

TLSv1 Level Set	**TLS v1.0**	**TLS v1.1**	**TLS v1.2**
1.0	**ON (min level)**	**Available**	**Available**
1.1	**Disabled**	**ON (min level)**	**Available**
1.2	**Disabled**	**Disabled**	**ON (min level)**

22.5 Contact Center Server Security Store

Not all of the services and applications that are available on the Contact Center server use this security level switching mechanisms that is about to be described and fall outside its influence and therefore the Contact Center server has several individual certificate stores.

The store, which we will call from this point, Contact Center Security Store, which is used by the applications and services to enable secure communications and is configured via Ignition Wizard upon installation and modified by Security Manager post install was traditionally only used to secure SIP traffic (to AES, SM, AMS, etc.).

In 7.0 this store influence has been expanded to now provide security certificates for the applications and services listed in *Section 20 Use of secure protocols by default upon installation* above.

22.5.1 Combining Stores

To minimize the amount of configuration required to secure the applications and services with this new secure by default feature several certificate stores which existed for individual applications were eliminated and brought into a single store. This resulted into the Contact Center Security Store.

This one store now provides a security certificates for all of the applications that fall under the new secure by default feature.

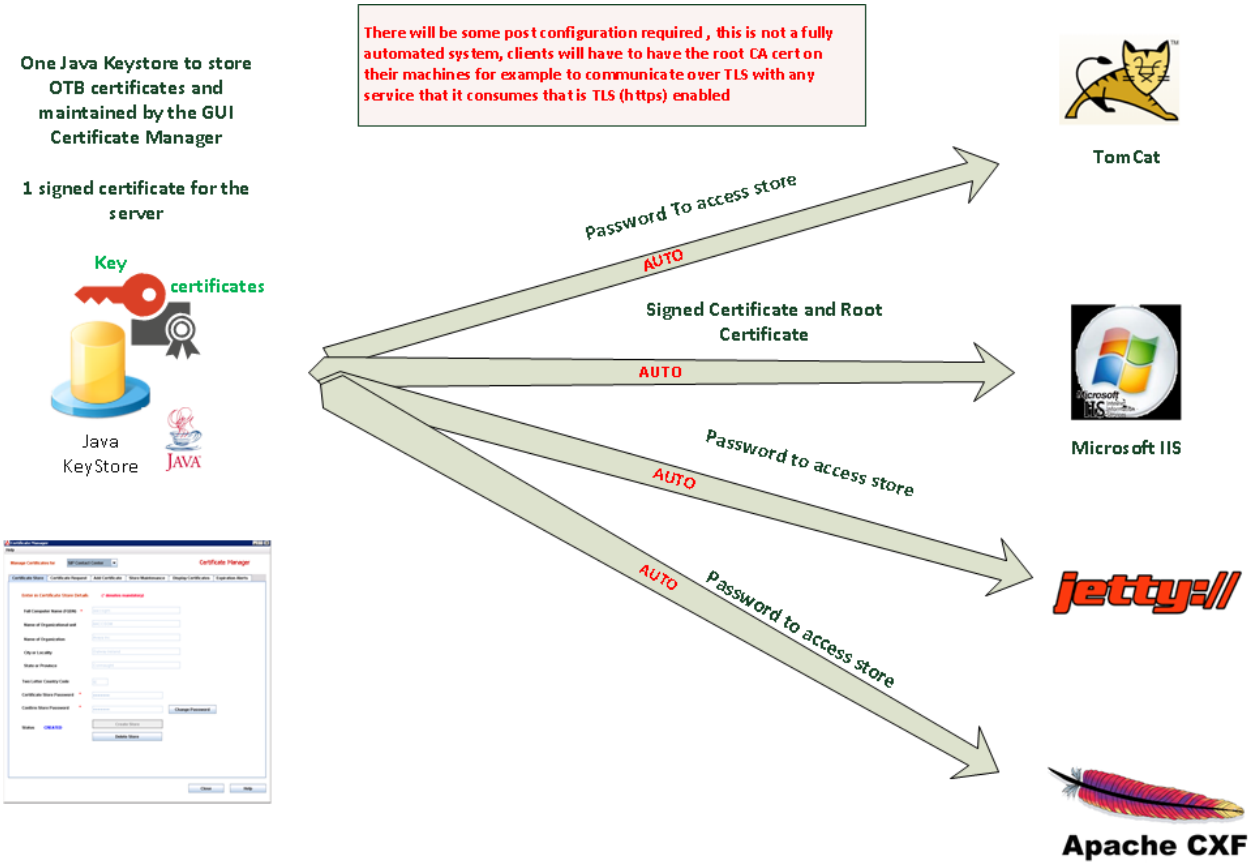
22.5.2 Implications of using a single store

Using a single store has several benefits, but it also has some drawbacks, one being that if the certificates are changed in the store then the changes have to propagate to all of the applications and services that use this store.

For the secure by default feature this propagation of certificates is automated to a point for the applications and services which this feature encapsulates.

For the SIP traffic connections, if the Certificate Authority is changed for example, then that root CA security certificate would have to be placed on any TLS enabled endpoint that communicates with the Contact Center server. This would be a manual step.

22.5.3 Single Store and security on by default (diagram)



22.6 Deployment requirement for root CA security certificates

While the majority of securing the services and applications are automated to a point where all web servers which host the applications are configured automatically without any customer intervention to use the security certificate setup on the Contact Center Certificate Store, there is one manual step which is not automated, the Certificate Authority (CA) root security certificate has to be deployed to any client machine which any contact center application, who will be accessing the contact center server over a secure connection, resides on.

General access to the contact center features out of the box is not possible without some additional configuration to the solution.

Generally it will be the distribution of the root certificate authority security certificate on client machines which will allow the TLS negotiation to be possible without warnings or errors

22.6.1 Where to get the Certificate Authority (CA) root security certificate

While obtaining the root CA security certificate is relatively straightforward, there are a couple of possible configuration decisions that determine where it can be sourced. See *Appendix A How to get the Root Security Certificate From Security Manager*

22.6.1.1 Maintaining an in-house Certificate Authority

If the customer decides to create their own Certificate Authority (CA) server inside their network then this root security certificate can be obtained from that server at any time as they effectively control their own Certificate Authority.

But note that this configuration means that the customer are maintaining their own CA and while it is trusted inside their own network infrastructure the same cannot be said of machines residing outside their network.

22.6.1.2 Purchasing from a 3rd Party Certificate Authority

If the customer decide to purchase a signed security certificate from an outside source, such as recognized Certificate Authority, then the root CA security certificate can be obtain from them.

The benefits of picking a recognized Certificate Authority is that the Windows Operating Systems tend to have prepackaged trust relationships with these CA's and therefore deployment of these root security certificates may not be required. Picking the appropriate vendor is important to achieve this automatic trust relationship.

22.6.1.3 Storing the Certificate Authority (CA) root security certificate

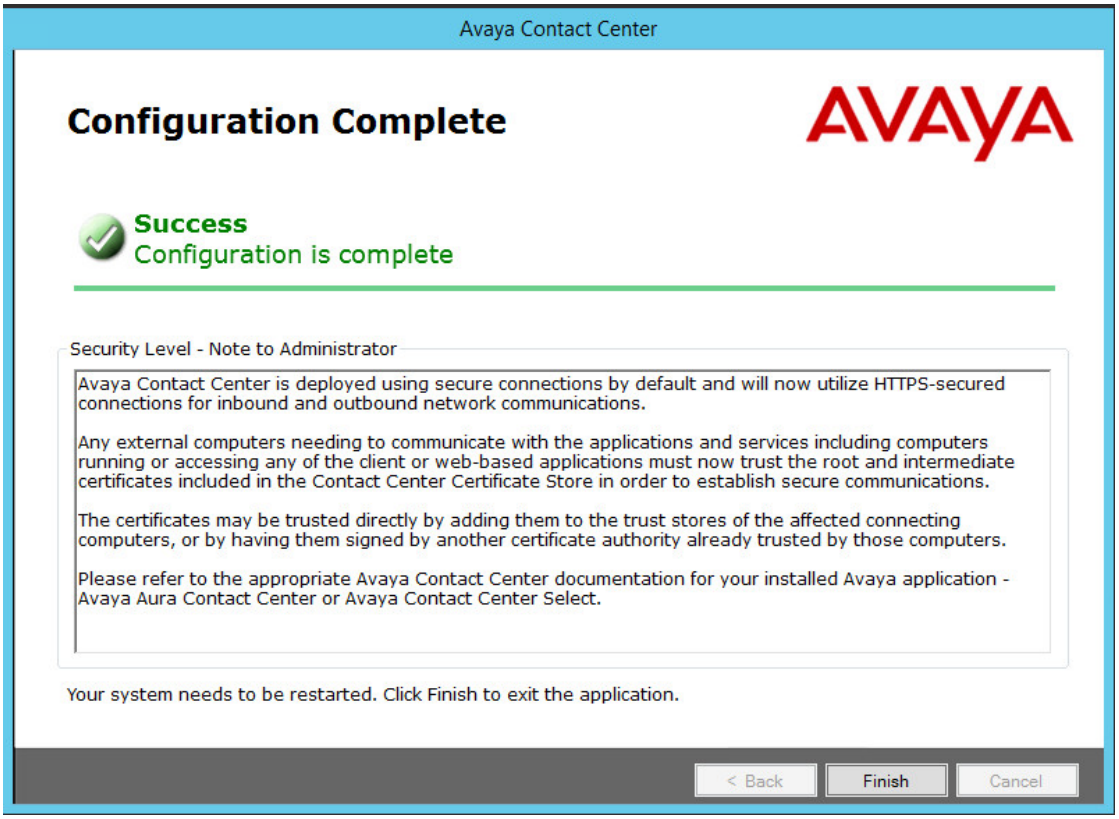
In both cases, the root CA certificate can be stored in the Contact Center Certificate Store which is used to provide the security certificates to establish secure connections for the various services. Importing the root CA certificate is very straightforward by using the Security Manager application which is available on the Contact Center server.

22.7 How it works

There are two separate applications used when setting secure communications for the range of web services and applications.

22.7.1 Ignition Wizard (Mandatory)

During the installation process, Ignition Wizard will execute a series of commands to secure the various web servers residing on the contact center server. Tomcat, CXF, JMX and IIS are all automatically configured to disable use of HTTP and enable HTTPS only if the customer completes fully the security configuration section of Ignition Wizard, which is introduced in 7.0.3 to facilitate the creation and population of the contact center security store. Once Ignition wizard has completed it will display an informational message indicating that the changes have been made and will list the services impacted by the changes.



22.7.1.1 Access to features after Ignition Wizard

After the installation has been completed the customer will have to access applications and services using the HTTPS protocol if they have completed the security configuration element of Ignition Wizard, otherwise the system will be unsecure and access can be performed through the HTTP protocol.

If any application resides outside the Contact Center server then the customer will have to distribute the Certificate Authority root security certificate to those clients to successfully access services over a secure connection.

If the root Certificate Authority security certificate is not present then access will be denied. Please refer to *Section 19.1.1 Where to get this Certificate Authority (CA) root security certificate* for details.

22.7.1.2 Ignition Wizard: Once Only and On Only

Execution of securing the Web servers is mandatory and it cannot be changed. Ignition Wizard is only designed to enable secure communications.

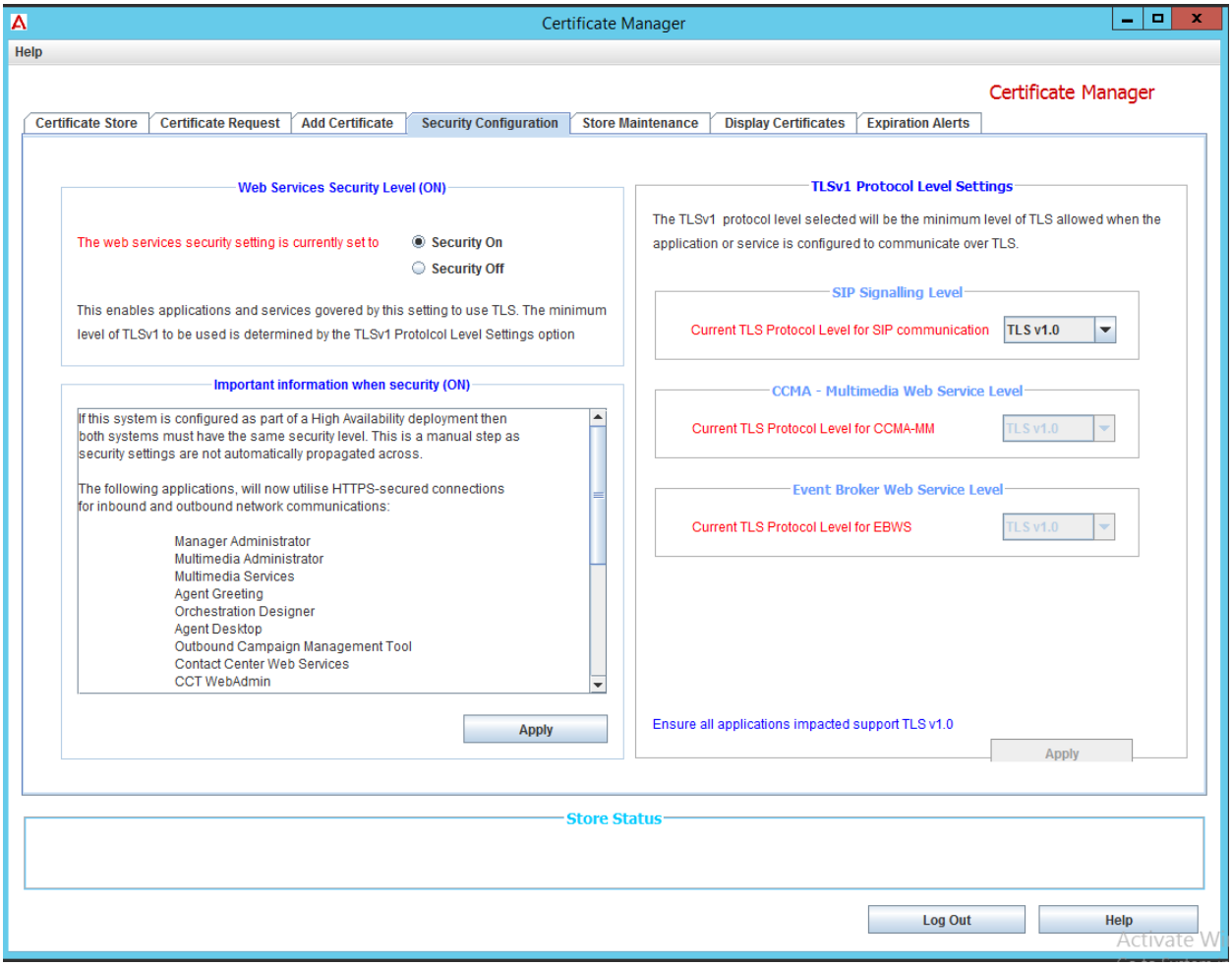
This is only executed once, upon subsequent launches of Ignition Wizard this sequence of setting security settings is not executed only if the customer has completed the security configuration section of the Ignition Wizard process.

If this security configuration section has not been fully completed at this stage then none of the commands will be executed and the system will be unsecure when restarted and can only then be secured by using the Security Manager application to create and populate this security store.

22.7.2 Security Manager (turning on security)

Security Manager (previously Certificate Manager) is a GUI based interface which allows the customer to maintain the Contact Center server security store which contains the security certificates for enabling secure access to the services and applications mentioned in *Section 19 Use of secure protocols by default upon installation.*

Security Manager has a new tab which allows the user to turn on the security for the aforementioned services and applications. See below



22.8 Changes implemented when turning on security

When the Ignition Wizard and/or Security Manager turns on secure communication for the services and applications listed several settings are enforced on the onboard Web Servers that the Contact Center server uses to host the services and applications.

These Web servers include: Apache Tomcat, Internet Information Services (IIS), Apache CXF and Jetty.

During the turning on process HTTP is disabled and HTTPS is enabled causing any services or applications that reside on these Web servers to use secure access only.

22.8.1 IIS changes

For IIS, the turning on process passes the signed security certificate and root certificate authority certificate to IIS and adds then to the Windows certificate store automatically.

It also creates a binding to port 443 with the imported signed certificate and enables *Require SSL* on the site.

22.8.1.1 Exceptions

To allow *Click Once* applications to be downloadable over HTTP the following folders on IIS have the *Require SSL* check unchecked.

Agentdesktop

ADMIN

OCMT

Dashboard

This allows initial download of these applications without distributing the root CA certificate to the client. But it must be noted that access to the features will still require a secure connection and therefore the CA root certificate on the client.

22.8.2 Apache Tomcat, Apache CXF, Jetty

For these web servers/services access to the Contact Center certificate store which contains the security certificates to enable secure connection is enabled.

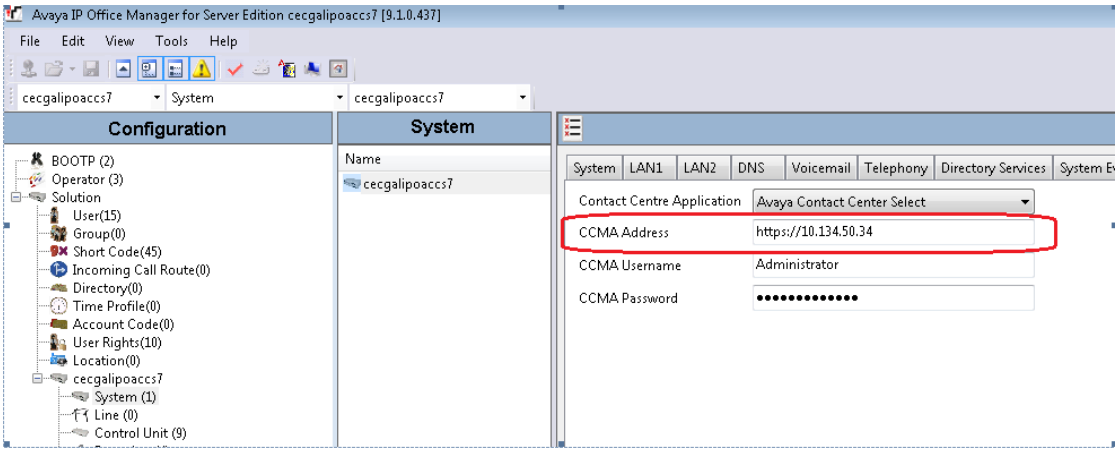
22.8.3 Restart required

To pick up any changes made to the store, such as new certificates added or different password entered to access the store a message is displayed to the customer that a restart of the server or all services is required.

Not all changes require this restart but for completeness sake a restart is required so ensure all services and applications will receive any changes made to the store.

22.8.4 IP Office Configuration when security is On (ACCS specific)

IP Office makes web service calls to CCMA to synchronize the agent information between the two systems. By default, these calls are made over http. Once https is enabled, these calls will fail until the CCMA details are updated manually on the IP Office manager interface. The name of the CCMA server as configured on IP Office manager must be pre-pended by https.



22.9 Turning off security

Not all deployments will require HTTPS secure communication and therefore there is the ability to turn off the security for the applications and services.

22.9.1 Implications

Turning off the security level for applications and services reverses the changes made to the Web servers (Tomcat, CXF, Jetty and IIS) that were performed when Ignition Wizard enabled security during the installation of the solution.

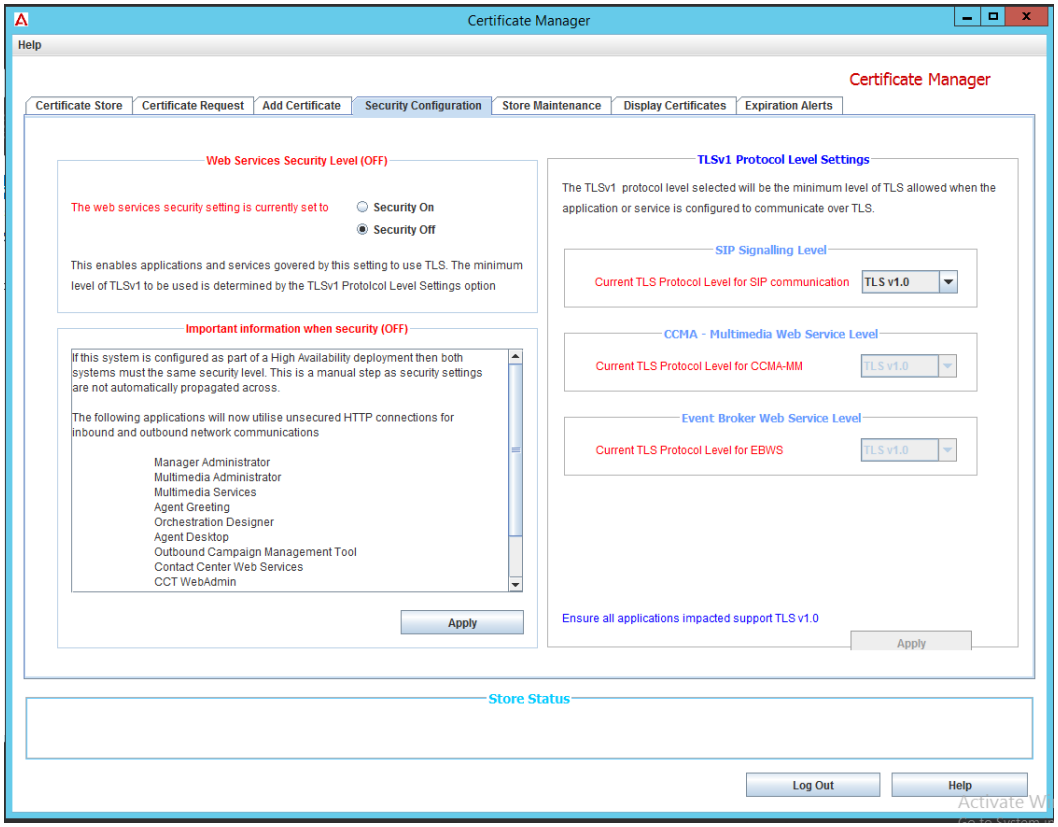
By switching off the security on the applications and services the customer will then be communicating over an unsecure channel (HTTP) and implications of doing so.

22.9.2 How to turn off security

There is only one method of turning off security for the applications and services that utilize this particular security feature.

22.9.2.1 Security Manager (turning off security)

Security Manager is the only application on the contact center that will revert all changes to the web servers influenced by this feature. The mechanism is similar to turning it on as described in heading *19.2.2 Security Manager (turning on security).*



Basically the customer can select the Security Off option and hit apply and all the changes will be made automatically, a reboot of the server is required to ensure all changes are propagated correctly.

22.9.2.2 Exceptions

While most of the changes are reverted back to use HTTP, On IIS the security certificate and binding to that certificate remains in place, as you can see in the information message in the screen shot above. This is to accommodate Agent Controls Browser App which must communicate over HTTPS.

> *The agent controls application is new to CC 7.0. It is a browser based application that allows the agent to carry out basic contact center functionality including logging in and out, setting not ready reason codes, and going ready, setting activity codes and after call work codes. This application works in conjunction with a desk top phone and does not provide call control.*

So this basically re-enables use of HTTP and leave HTTPS enabled and configured with a server security certificate. So application and services can revert to HTTP, while the Agent Controls Browser App can use HTTPS.

22.9.3 Changing the security level post installation

The Security Configuration tab in Security Manager gives the customer the ability to change the security level at any time. Security Manager can be used to turn on and off security for the applications and services.

Every change will require a restart of services so all changes can be propagated throughout the server.

For more details on how to change the security level using Security Manager then see *Appendix B – How to Change the Security Level using Security Manager*

23. Digital Security Certificates in AACC/ACCS

The Contact Center solution in 7.0 has been automatically set to use secure protocols in a range of web services and applications and as such require additional configuration to establish the secure connections.

Along with the aforementioned web services and applications, there still is the requirement to have a secure SIP connection to the Avaya Enablement Services (AES). Other SIP endpoints are configurable but can communicate over TCP as well as TLS and so unless there is a need to secure all endpoints these TCP enabled endpoints require no additional configuration.

All of the above is provisionally configured by using the default security store or also known as the Out-of-The-Box (OTB) security certificates. These certificates are provided for use in a lab or pre-production environment and are not designed to be used in a production deployment.

So removal of the OTB security store and replaced with the customer own security store is paramount before the Contact Center is deployed.

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

For the web servers it enables secure transmission over HTTPS (using TLS). It uses the various web server technologies to establish these connections.

Please refer to *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* chapter on Contact Center Manager Server certificate commissioning.

23.1 Chained Certificates support

Chained Certificates are supported since 7.0.3 (post installation via Security Manager) and 7.1 (at installation time via Ignition Wizard).

23.2 Default Test Security Certificates (Out Of the Box)

The Contact Center solution up to release 7.0.1.1, contains a prepackaged java keystore (JKS) which contains a signed security server certificate and root security certificates. The purpose of providing this pre-populated security certificate store is to allow the commissioning and testing of the contact center prior to going into a live production environment

While these certificates allow Ignition Wizard to set up all of the host web servers in the solution with appropriate security certificates, these certificates are not industry standard and should only be used to get initial configuration in place and be replaced with custom security certificates either signed in-house or purchased with a 3rd party vendor before entering production.

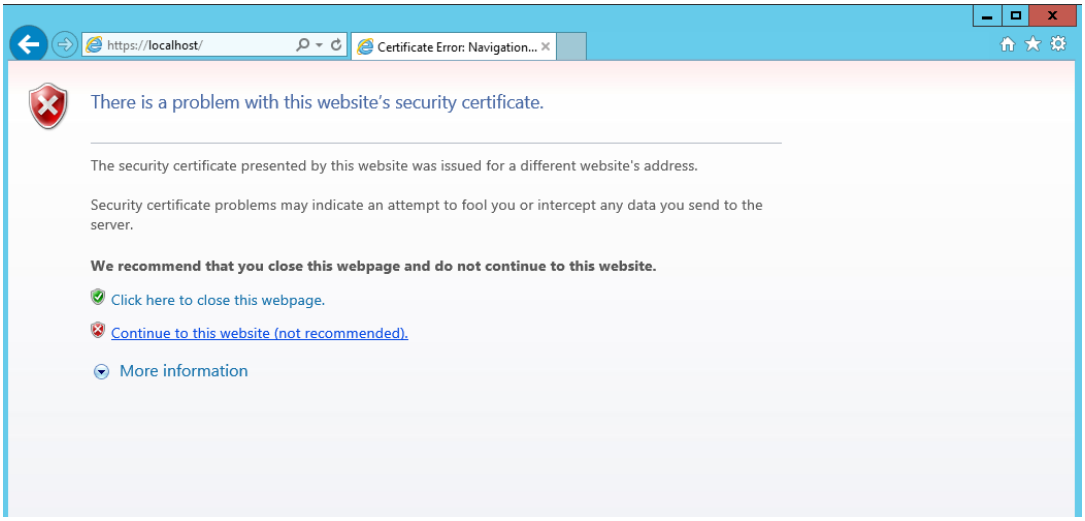
It is recommended that this store be replaced at the earliest convenience to reduce additional configuration later on.

These are for **test** or **pre-production** only.

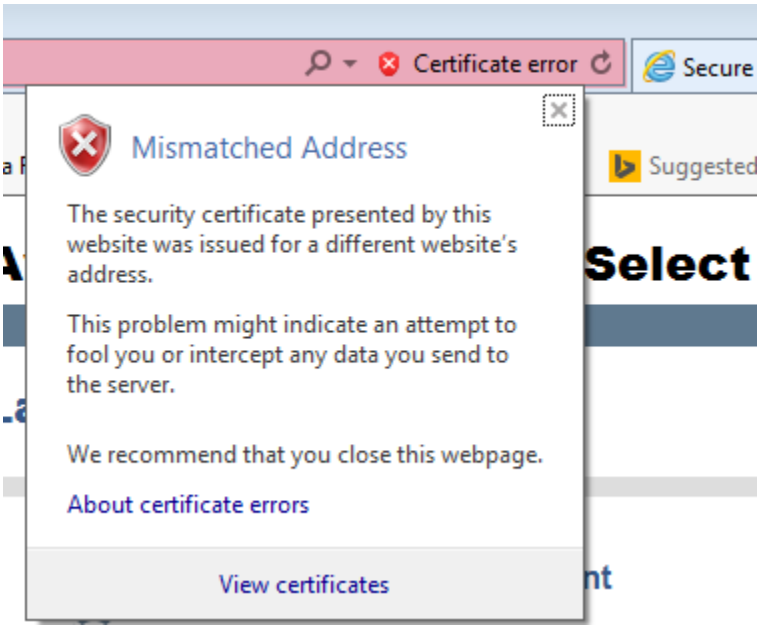
23.2.1 Known Limitations with the OTB Certificate Store

While the security certificates in the OTB store will allow applications and services to establish a secure connection over TLS there are known issues that will be noticed when you use these to establish connections. This is due to the generic nature of the security certificates used in the store, the certificate name or unique name is set to AACCSGM60 and this does not match the actual machine name which is unique within a network and thus will result in warnings in browsers that state as much. See below for examples

Typical Warning when using non custom certificates over HTTPS



For CCMA for example, even when using the name of the computer the OTB signed certificate will have a different name and thus this warning. While it displays a warning the connection is secure but will always display the mismatched address.



23.2.1.1 Realtime Dashboard

The Realtime Dashboard will not work with the default cert as it is not able to ignore this error. The dashboard will only work with a proper signed cert having a matching name and trusted root cert installed.

23.2.1.2 Excel Configuration Tool

The Excel Configuration Tool will work with the default cert.

23.2.2 Warning notification about use of Out Of the Box (OTB) Security Certificates

Until the OTB store is removed from the contact center, Security Manager will display a warning message about the continued use of the default store.

23.2.3 Basic steps required to replace the default store on AACC/ACCS

The end user is encouraged to remove the OTB store and replace it with their own that matches the server on which it resides on before it enters production to avoid warnings described in heading : *21.1.1Known Limitations with the OTB Certificate Store.*

To change from the provided OTB store, the following basic steps should be followed to introduce a new custom security store with your own provides security certificates.

Backup the existing store (using Security Manager Application)

- Create a new store (using Security Manager application)
- A Certificate Signing Request (CSR) is generated when the store is created, it is this CSR that is sent to Certificate Authority (CA) , either yours or a 3rd party one.
- The resulting signed security certificate and root certificate authority are then imported back into the new store on AACC/ACCS (using Security Manager application)
- The root CA security certificate is distributed to all clients which need to communicate to AACC/ACCS services over TLS
- It is placed into the local trusted certificate authority section on the client machine.
- Restart services

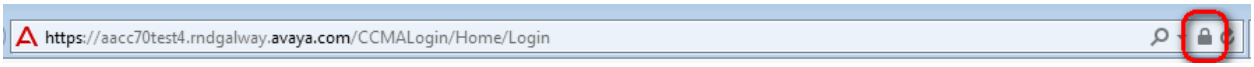
For more detail please see *Appendix C - Replacing the OTB Store*

23.2.3.1 When Custom Certificates installed on the Contact Center

When the official signed certificate is installed the server name in the URL should match the name to which the cert was issued. This is usually the FQDN for the server.

e.g. https://acc7server.domain.com

The root cert for the CA that was used to sign the server certificate must be installed as a the Trusted Root Cert on every client that will be running CCMA. Once this is in place and the official cert is installed, the browser should show the site as being fully secured.



23.3 Digital Security Certificate Management

Avaya Aura® AACC/ACCS 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.

23.3.1 Identity Certificate Template requirements

While the contact center does not sign digital certificates it does generate a Certificate Signing Request (CSR). The CSR is sent to the desired Certificate Authority (CA) to be signed and generate an Identity certificate. This CSR has to be signed using a template with Client and Server Authorization attributes. Please check that the CA chosen has a Client/Server authentication template and it is used when signing the CSR from the contact center.

If the Client/Server authentication template does not exist then it can be created on the CA by basing it off an existing template and adding the appropriate attribute to make a Client/Server Authentication template.

Failure to sign the CSR with this type of template may result in the SIP-CTI link not establishing a secure connection with AES.

23.3.2 Digital Certificate template version support

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

23.3.3 Digital Certificate template key length support

Security 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.

23.3.4 SHA256 encryption support

In release 7.0 any application that generates Certificate Signing Requests (CSR) and negotiates with digital signing requests will be able to do so in SHA256 encryption level.

23.3.5 Backward compatibility 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 Security 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.

23.3.6 Security Manager

Maintenance of the digital certificates in use by the server is facilitated by the Security 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.

24. SSLv3: Removal of support

In this release support for Secure Socket Layer (SSL) has been removed from the Contact Center server as a means to encrypt a secure connection to any other endpoint in the solution.

The changes implemented were:

24.1 Windows operating system

The changes to eliminate SSLv3 on the OS level are server wide and impact any Windows based application that reside on the Contact Center server. This covers, for the Contact Center, Internet Information Services (IIS) which hosts several applications and services and Internet Explorer (IE).

Details of the changes made can be gotten from the following link under the heading *Disable SSL 3.0 in Windows for Server Software.*

https://technet.microsoft.com/en-us/library/security/3009008.aspx

24.2 OpenSSL

OpenSSL is used to establish TLS connections between the Contact Center Server and other endpoints for SIP Traffic. An upgrade to the latest OpenSSL version removes the fallback mechanism to pick SSLv3, the flaw which POODLE exploited which forced a protocol downgrade.

24.3 Tomcat Server

The Contact Center solution leverages Apache Tomcat to host several applications and services. Modification to the connectors and an upgrade to the latest version have removed Tomcat's support of SSLv3.

Details can be found from the following link

http://wiki.apache.org/tomcat/Security/POODLE

25. Default passwords

Several components of the solution come with default passwords. Since 7.0.X upon first login the customer is forced to change the default to one of their choosing. Ensure that the password chosen is safeguarded as some applications do not have a reset facility.

26. 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

27. PCI DSS (Payment_Card_Industry_Data_Security_Standard)

Avaya Aura Contact Center 7.0 makes no claim of being PCI compliant for voice or Multi Media transactions.

AACC/ACCS 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/ACCS to solely collect PCI information on voice calls. In that way AACC/ACCS does not handle the PCI data at all. Solutions for other contact types such as email may also be designed such that AACC/ACCS would not handle the PCI written information.

28. GDPR (General Data Protection Regulation) Support

Avaya Aura Contact Center 7.0 makes no claim of being GDPR compliant for voice or Multi Media transactions.

GDPR regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU. Therefore, from a Contact Center perspective, this can apply to not only customer personal data but also to Agent/Supervisor personal data.

AACC/ACCS provides tools to support customers to achieve compliance and may form part of a GDPR compliant solution subject to detailed requirements, implementation and validation. Some of the tools provided to support GDPR directives are shown in below table:

GDPR Directive	AACC/ACCS Tools	Documentation Reference
Privacy by Design – Encryption of data at rest	Security Manager – Database Encryption tab CCMM Administration – Store attachments in database	**AACC Document**: Avaya Aura® Contact Center Server Administration **ACCS Document**: Avaya Contact Center Select Advanced Administration **Relevant sections:** Database encryption administration Configuring the email settings
Right to information and access to one's own data	CCMM Data Management – Privacy tab	**AACC Document**: Avaya Aura® Contact Center Server Administration **ACCS Document**: Avaya Contact Center Select Advanced Administration **Relevant section:** Data Management – customer privacy
Right of erasure (the right to be forgotten)	CCMM Data Management – Privacy tab	**AACC Document**: Avaya Aura® Contact Center Server Administration **ACCS Document**: Avaya Contact Center Select Advanced Administration **Relevant section:** Data Management – customer privacy
Right to object to processing	Avaya Agent Desktop – Restricted flag	**AACC Document**: Using Agent Desktop for Avaya Aura® Contact Center **ACCS Document**: Using Agent Desktop for Avaya Contact Center Select

		Relevant section: Customer and contact details

28.1 Data Privacy Controls Addendum

28.1.1 Data Categories Containing Personal Data (PD)

Multiple PD items maybe present depending on use of product. Refer to "Contact Center Performance Management Data Dictionary" for details.

28.1.2 PD Human Access Controls

Administrator, Agent, Supervisor configuration refer to customer documentation Avaya Aura® Contact Center Client/Administration and Administering Avaya Contact Center Select available from support.avaya.com

Full GDPR compliance is achieved with access controls for Administrator, Agent & Supervisor roles with the additional use of partitions that supports departmentalisation of customers PD for groups of agents and supervisors based on their assigned skillsets. Customer PD is required for business operation of the contact center.

28.1.3 PD Programmatic/API Access Controls

Multiple interfaces available through ODBC, JDBC, Web Services and SDKs. These all require password authentication. For further details refer to Contact Center Performance Management Data Dictionary and Avaya Aura Contact Center SDKs available from DevConnect

https://www.devconnectprogram.com/site/global/downloads/index.gsp?item=3de9a6f6-8586-443a-a42c-f8807795cf5d

28.1.4 PD "at Rest" Encryption Controls

Database Encryption using Advanced Encryption Standard with a 256-bit Cipher Security Level. Full GDPR compliance requires that Database Encryption is enabled by default at installation/upgrade time. However, Database Encryption is currently disabled at installation/upgrade time to allow customers to manage their encryption keys when they enable this security feature. It is the responsibility of the AACC/ACCS customer to enable Database Encryption immediately after installation/upgrade and prior to handling customer contact transactions.

28.1.5 PD "in Transit" Encryption Controls

TLS 1.2 supported between clients, e.g. Avaya Agent Desktop and AACC/ACCS Server.

28.1.6 PD Retention Period Controls

This is a function of product user. Minimum moving window period you can set to automatically remove data is 1 month from OFFLINE database.

Full GDPR compliance requires a retention period of zero days. However, the business operation of the contact center would be adversely affected if the data retention period were to be reduced from the minimum moving window period of 30 days/1 month to zero days. The default retention period must remain at 30 days. It is the responsibility of AACC/ACCS product customers to clearly request explicit consent from their customers at the beginning of every contact transaction to store their PD.

28.1.7 PD Export Controls and Procedures

High-level solution provided to customer to configure retention period on data. This is configured through CCMM Data Management and CCMA->Configuration->Historical->Statistics

28.1.8 PD View, Modify, Delete Controls and Procedures

CCMM Data Management provides interface to delete PD for a customer. Avaya Agent Desktop provides interface to modify customers PD.

Full GDPR compliance requires a mechanism to re-delete a customers PD after a Database Restore procedure has restored a Database Backup image taken prior to deleting a customers PD. AACC/ACCS product customers should maintain a log of customers who have requested their PD to be deleted. The Deleting Customer History procedure should be used to re-delete the customers PD - refer to customer documentation Avaya Aura® Contact Center Server Administration and Avaya Contact Center Select Advanced Administration available from support.avaya.com

28.1.9 PD Pseudonymization Operations Statement

Encryption of PD in database.

29. Secure Shadowing

29.1 Introduction

InterSystems Cache *shadowing* is used by AACC/ACCS high availability configurations. *Shadowing* enables standby nodes maintain a shadow copy of the database on the active. By continually transferring journal information from the active to the standby, *shadowing* enables recovery to a system which is typically within only a few transactions of the source. The communication between the active and standby servers uses a Cache *shadowing* communication channel. Currently, this channel is not secured.

In 7.1.0.0, the shadowing communication channel is secured when security is enabled using Security Manager. If security is not enabled, the channel is not secure. Secure shadowing applies to both AACC and ACCS.

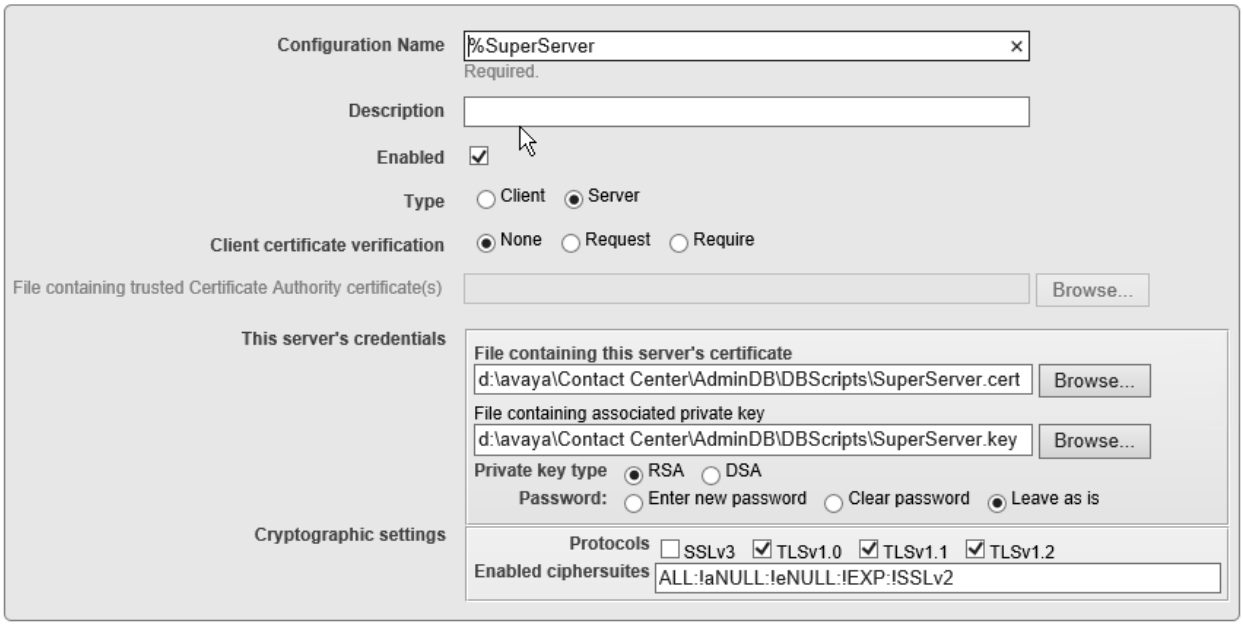
29.2 Secure Shadowing

The shadowing communications channel is secured by introducing and using new Cache SSL/TLS Configuration. The new SSL configurations are created during 7.1.0.0 install or upgrade to 7.1.0.0. The configurations enable the secure communication between the active and standby nodes. The new SSL Configurations:

29.2.1 %SuperServer

In order to secure communications in Cache, the Cache **%SuperServer** is created and configured for TLS communication.

In 7.1.0.0, the **%SuperServer** is automatically created and configured during the install / upgrade processes.



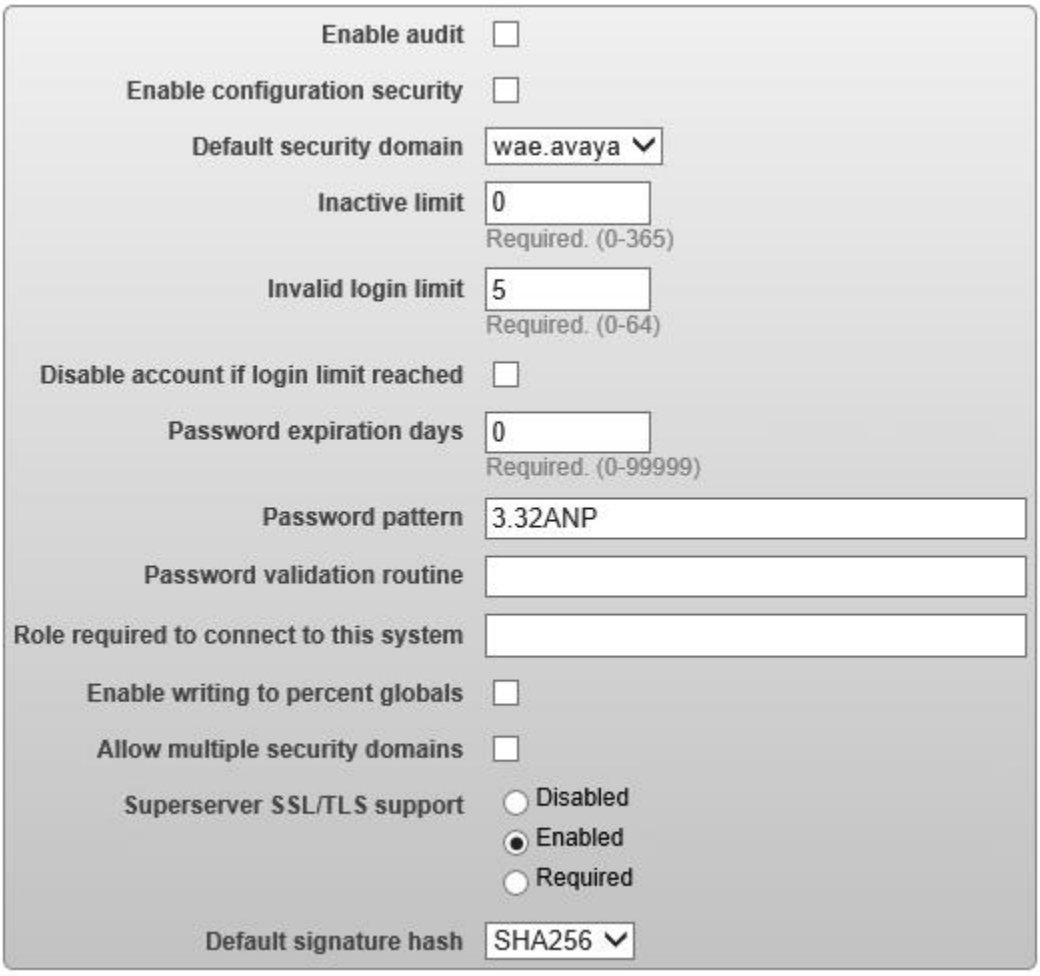
The TLS security is enabled using new security credentials automatically created during the install / upgrade processes.

Certificate File	d:\avaya\Contact Center\AdminDB\DBScripts**SuperServer.cert**
Private Key	d:\avaya\Contact Center\AdminDB\DBScripts**SuperServer.key**

In addition to the %SuperServer creation and configuration, Superserver SSL/TLS support must be enabled as a system wide security feature. The configuration is done automatically during the install / upgrade processes.

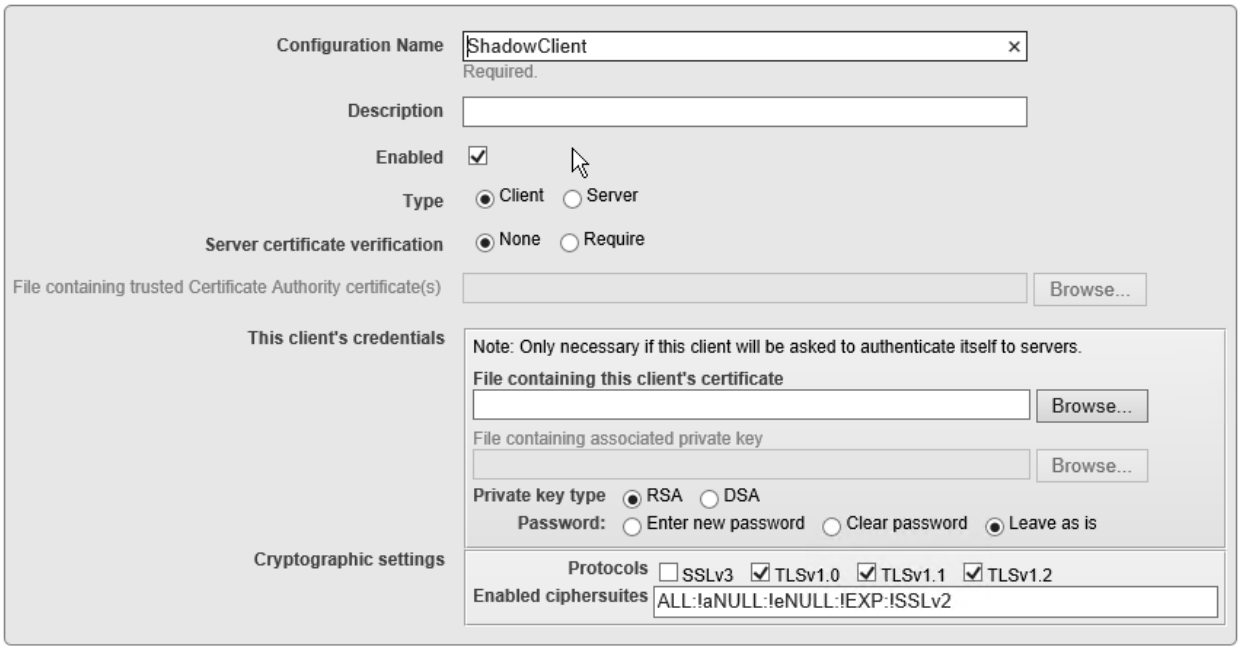
System-wide Security Parameters...

System Administration > Security > SSL/TLS Configurations



29.2.2 ShadowClient

A new client SSLConfiguration called **ShadowClient** is created automatically during the install / upgrade processes.


Configuration Name
ShadowClient
Required.
Description
Enabled
Type
Client
Server
Server certificate verification
None
Require
File containing trusted Certificate Authority certificate(s)
Browse...
This client's credentials
Note: Only necessary if this client will be asked to authenticate itself to servers.
File containing this client's certificate
Browse...
File containing associated private key
Browse...
Private key type
RSA
DSA
Password:
Enter new password
Clear password
Leave as is
Cryptographic settings
Protocols
SSLv3
TLSv1.0
TLSv1.1
TLSv1.2
Enabled ciphersuites
ALL:!aNULL:!eNULL:!EXP:!SSLv2

30. JMX vulnerability port protection

30.1 Introduction

During the latest security scan, some unsecured port vulnerabilities were found.

A Java JMX agent running on the remote host is configured without SSL client and password authentication. An unauthenticated, remote attacker can connect to the JMX agent and monitor and manage the Java application that has enabled the agent.

This vulnerability affects three JMX ports: 1099, 8100, 8200.

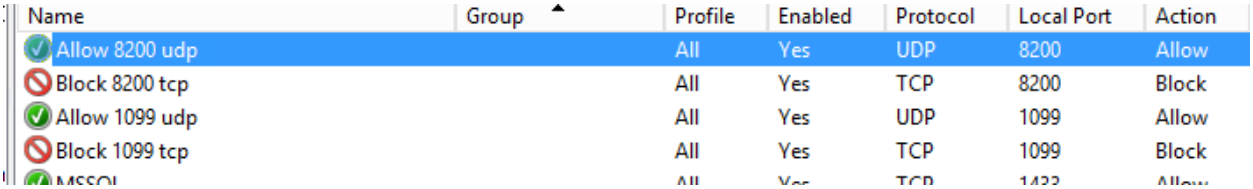
To protect these ports, the security authentication will be introduced in the next release 7.2.

For rel 7.0.3 and 7.1 rel need to apply the following configuration changes:

30.2 Secure port 1099

The 1099 port should be blocked at MS Windows Firewall.

1. Go to Control Panel->Windows Firewall-> Advanced settings->Inbound riles
2. Create a rule to block inbound TCP connections to port 1099
3. Create a rule to allow inbound UDP connections to port 1099
4. If firewall rule controlled by domain group policy, new rules should be applied to actual domain rules to take effect.



Name	Group	Profile	Enabled	Protocol	Local Port	Action
Allow 8200 udp		All	Yes	UDP	8200	Allow
Block 8200 tcp		All	Yes	TCP	8200	Block
Allow 1099 udp		All	Yes	UDP	1099	Allow
Block 1099 tcp		All	Yes	TCP	1099	Block
MSSQL		All	Yes	TCP	1433	Allow

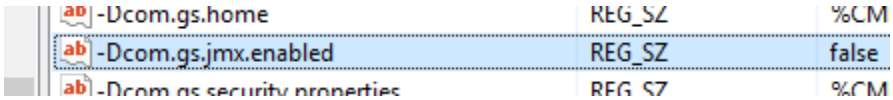
30.3 Secure port 8100

The 8100 port can't be closed as port above, as this port belongs to CMF and a lot of communication is going to-from this port even at standalone configuration. Also, it used to communication between nodes at HA setup.

To protect this port, need to disable JMX for this port only.

The following actions should be performed:

1. Run the "regedit" command at the windows command line with admin rights.
2. Go to HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\CCMS_SIP_Service\Parameters\JVMOptions
3. Add registry key as String Value -Dcom.gs.jmx.enabled=false



4. SIP Service restart is required

Note: As a side effect of these changes the SGM Management Client stops working at all. Usually, the SGM Management Client used by the customer-admins to verify established connections. Recommended applying changes above only after setup configured.

30.4 Secure port 8200

8100 Port Used for UDP exchange by Emergency Help feature. Disabling TCP should not affect the functionality.

The 8200 port should be blocked at MS Windows Firewall.

1. Go to Control Panel->Windows Firewall-> Advanced settings->Inbound riles
2. Create a rule to block inbound TCP connections to port 8200
3. Create a rule to allow inbound UDP connections to port 8200
4. If firewall rule controlled by domain group policy, new rules should be applied to actual domain rules to take effect

31. Enabling Agent Security for Avaya IX™ Workspaces

31.1 Introduction

The new option was introduced to secure connection from the Workspace client side. The **Agent Security** option can be enabled from **CCMM Admin -> Workspaces Configuration -> Server Settings -> Agent Security.**

Once the **Agent Securi**ty option enabled, the Workspace client URI can be reached only through secure **https** connection with specified **FQDN** name.

31.2 Create Certificate

Before you begin, need to obtain a security certificate and associated key file from a trusted Certificate Authority (CA).

If you use SMGR as CA, you can create a ***.p12** certificate with specified CN.

e.g.

From created certificate, need to extract client certificate and private key. OpenSSL command or specific tools (like KeyStore Explorer) can be used to extract client certificate and private key.

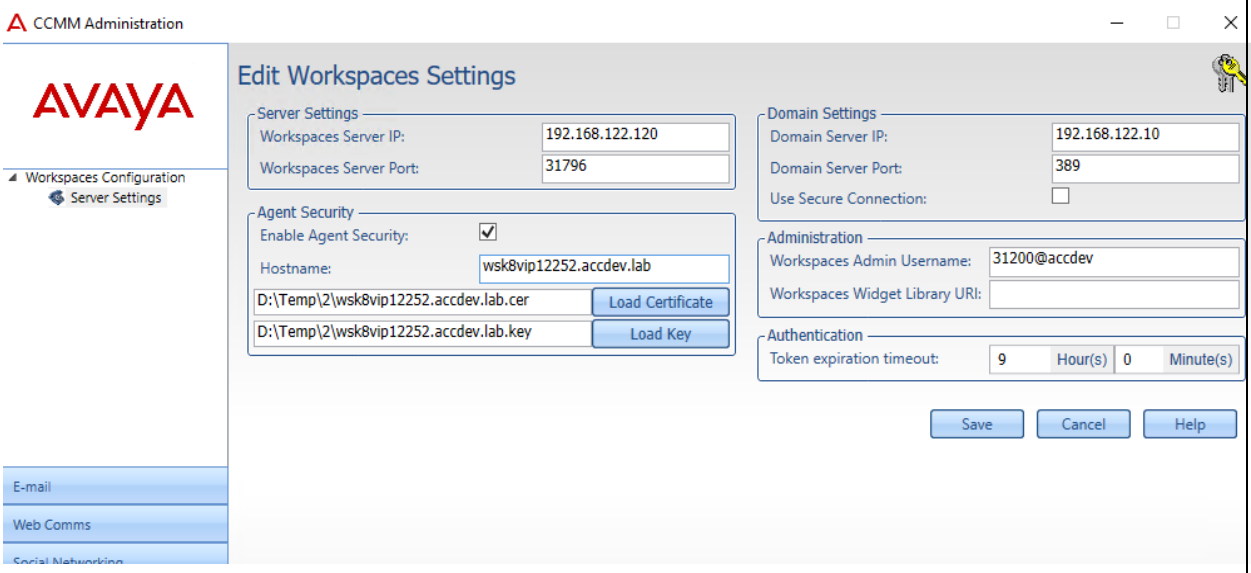
31.3 Steps to enable Agent Security for Avaya Workspaces

1. Open CCMM Admin -> Workspaces Configuration -> Server Settings -> Agent Security.
2. On the **Edit Workspaces Settings** screen, under **Agent Security**, select the **Enable Agent Security** checkbox.
3. Click **Load Certificate**, browse to the desired directory, and select an HTTPS certificate file.
4. Click **Load Key**, browse to the desired directory, and select a key file.
5. In the **Hostname** field, enter the hostname you want to use to access Avaya IX™ Workspaces. Use the same FQDN configured in the client certificate at 31.2
   Important: Need to use the full FQDN name (like **hostname.domain**). The short hostname options is not allowed. It is 7.1.0.3 limitation.
6. Click **Save.**

Important: You must ensure that this hostname matches the hostname used when creating the security certificate. You must also ensure that all Avaya IX™ Workspaces client computers can resolve this hostname to the IP address of the Avaya IX™ Workspaces cluster.

Important: After you saved the changes in the Agent Security settings, you must wait for not less than five minutes for the changes to take effect. It is important that you don't change any Agent Security settings within this five-minute period.

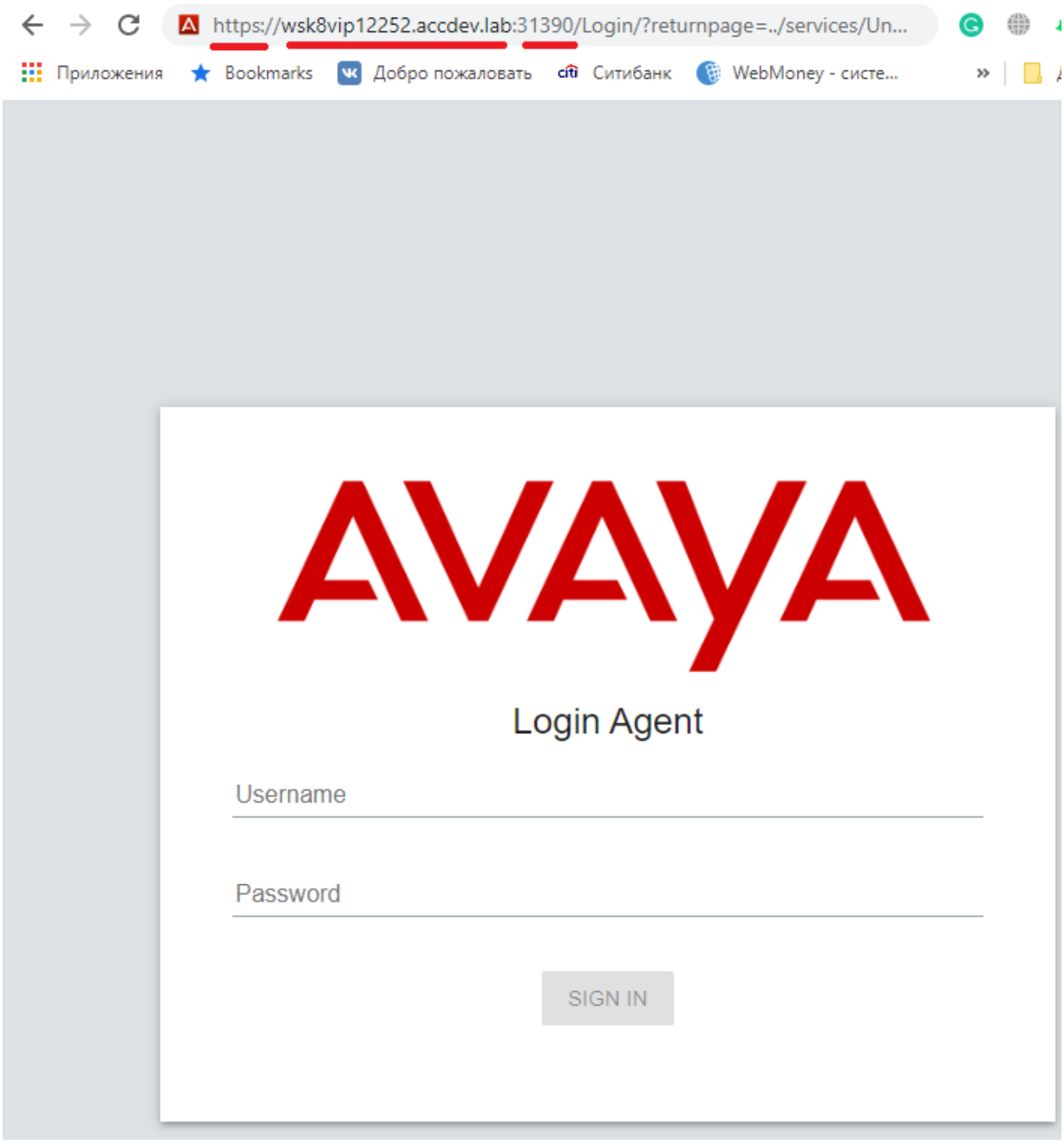
e.g.



Once all configuration settings applied, the Workspace client can be reached through https secure protocol only.

Important:

- Secure protocol - **https**
- Secure https port – **31390**
- Use **FQDN** configured in certificate
  Refer screenshot below.


https://wsk8vip12252.accdev.lab:31390/Login/?returnpage=../services/Un...
Приложения
Bookmarks
Добро пожаловать
Ситибанк
WebMoney - систе...
AVAYA
Login Agent
Username
Password
SIGN IN

Definitions

AACC	- Avaya Aura® Contact Center
AD-LDS	- Active Directory Lightweight Directory Services
ACCS	- Avaya Contact Center Select
AAMS	- Avaya Aura Media Server
CCMM	- Contact Center Multimedia Server
CCMA	- Contact Center Manager Administrator
CCT	- Communication Control Toolkit
CCLM	- Contact Center License Manager
CS 1000	- Communication Server 1000 (a.k.a. CS1K)
CLAN	- Customer Local Area Network
CPU	- Central Processing Unit
CLI	- Command-Line Interface
DEP	- Data Execution Prevention
Email	- Electronic Mail
http	- Hypertext Transfer Protocol
https	- Hypertext Transfer Protocol Secure
IIS	- Internet Information Services
JKS	- Java KeyStore
NIST	- National Institute of Standards and Technology
NMC	- Nortel Multimedia Conferencing
OI	- Open Interface
RSA	- Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman Algorithm for public-key cryptography

SSL	- Secure Sockets Layer
SOA	- Service-Oriented Architecture
SSO	- Single Sign On
SAL	- Secure Access Link
TCP	- Transmission Control Protocol
TLS	- Transport Layer Security
VM	- Virtual Machine
WCF	- Windows Communication Foundation

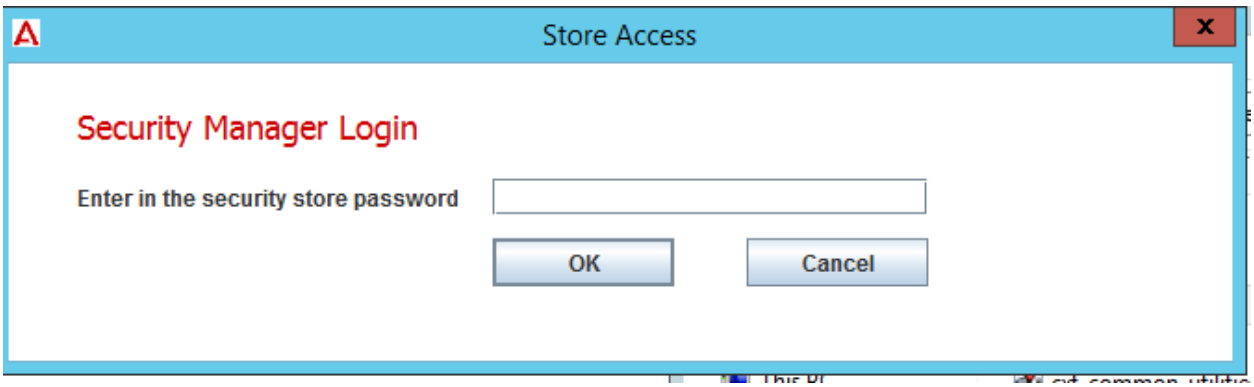
Appendix A - How to get the Root Security Certificate from Security Manager

Security Manager application provides all of the services for the end user to maintain the contact center certificate store and one of these services is an export facility where the user can select the root certificate authority and export it out of the secure store and place it in a location of their choosing and then distribute this to their client machines.

1. Launch Security Manager
   In the screen shot example it is a shortcut that has been created on the server. The menu system exists to access the Security Manager application.

2. Enter in default password (initial login only)
   Initial login will present the user with the password screen seen below. Enter in the default password "__avaya" (two underscores).

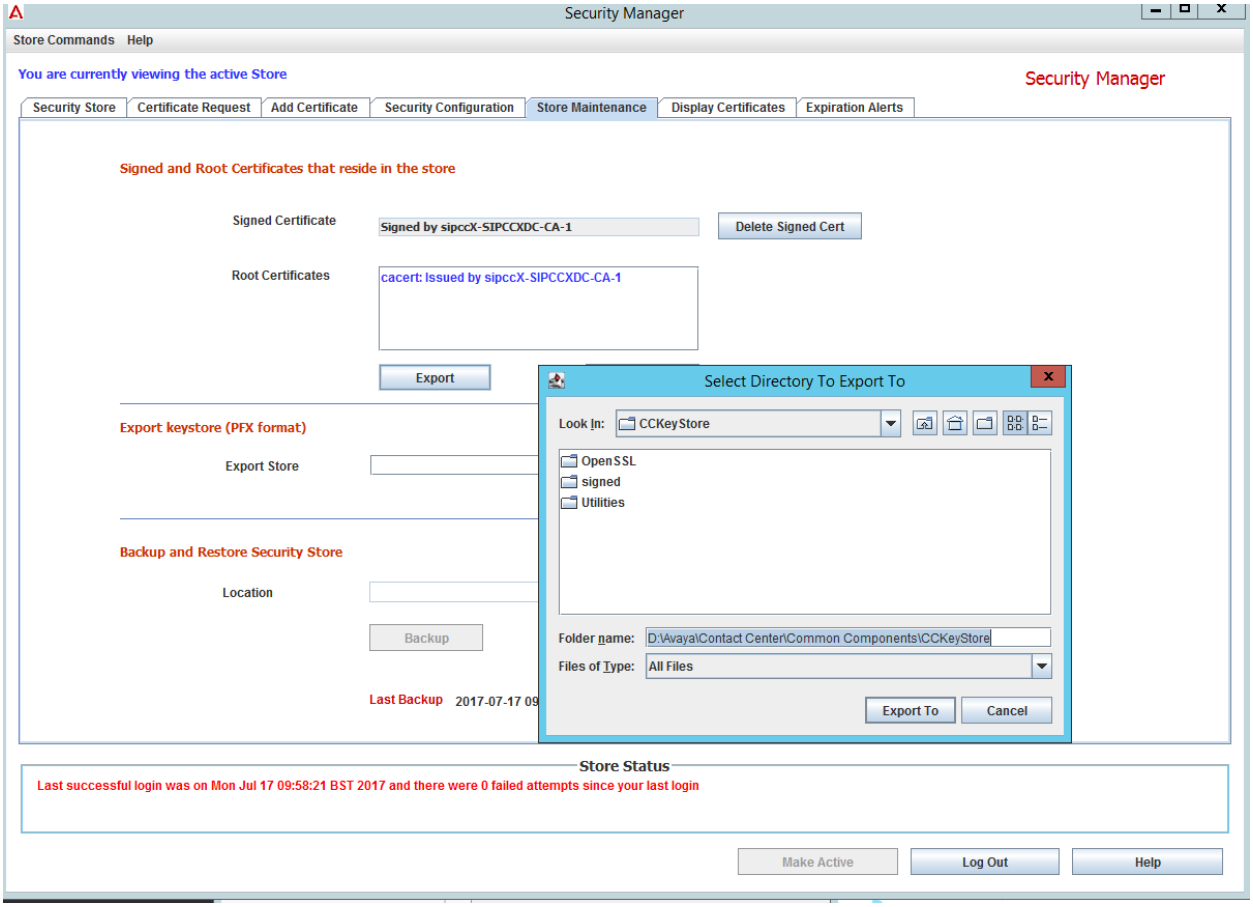
Note: You have three attempts to get it right otherwise you will be locked out of the application for 30 minutes (default)



Once you have entered in the password successfully you will be asked to change the default password, please remember the new password as it is encrypted and cannot be retrieved anywhere on the server in plain text.

3. Once the Security Manager has been successfully launched , select the Store Maintenance tab

Select the root certificate "*caCert2:Issued by SIP Product Certificate Authority*" and the Export button will be enabled , select your location and export.



4. Go to that location , copy the file and place on the client machines,

   To place apply the certificate onto the client machine you do the following

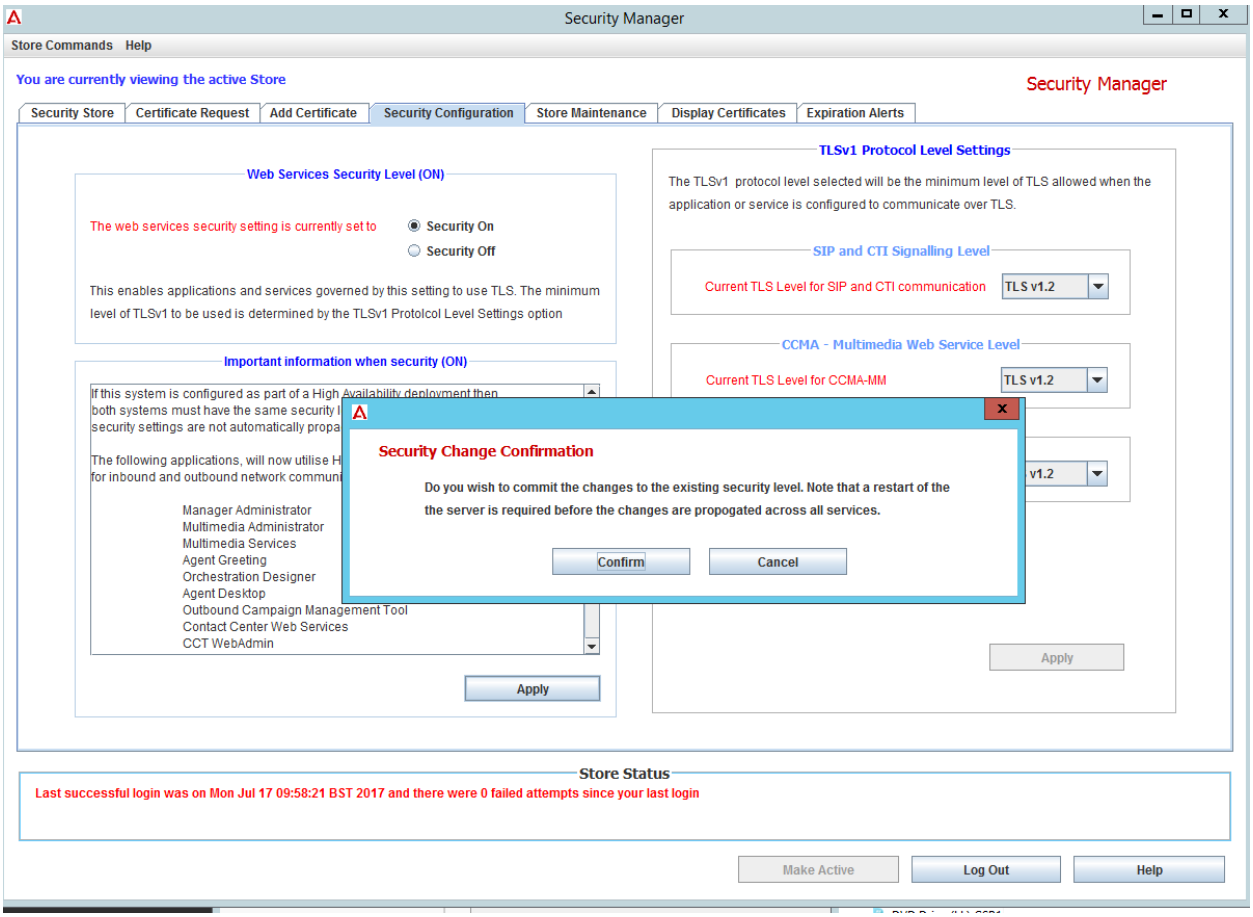
   a. Start→Run→MMC
   b. File Add/Remove Snap-In
   c. Select Certificates from the list to Add over to Selected Snap-In's
   d. Select Computer account , Next
   e. Leave default setting
   f. Finish.
   g. Hit Ok on the main screen
   h. Expand Console Root tree, Expand trusted Root Certificate Authority
   i. On the Certificates folder Right select for menu
   j. Select All Tasks and Import
   k. Hit Next on the next screen and browse to your certificate
   l. Leave the default setting and hit Next
   m. Finish

5. That will now import the root CA certificate onto the client machine and allow the application on that client to accept the signed certificate sent by AACC/ACCS services and establish a secure connection.

Appendix B - How to Change the Security Level using Security Manager

1. Launch Security Manager
2. Go to the Security Configuration tab
3. Note the current security level
4. Select the new level you wish to apply
5. The information screen will display the services and applications that Are impacted by the change, review and understand the changes about to be made.

6. Hit the Apply button
7. The decision dialog will ask you to either confirm the changes or back out.
8. Once you confirm the changes, which may take up to one minute dependant on the speed of the machine, a message will be displayed indicating that the server must be restarted.

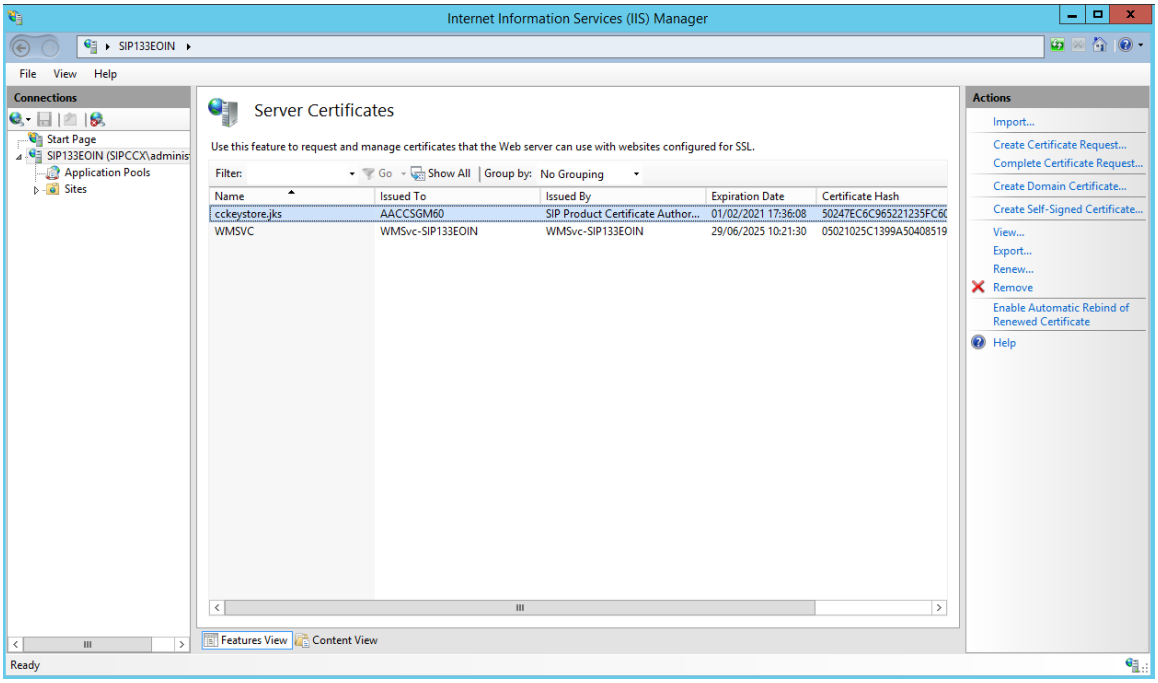


TURNING SECURITY LEVEL TO ON

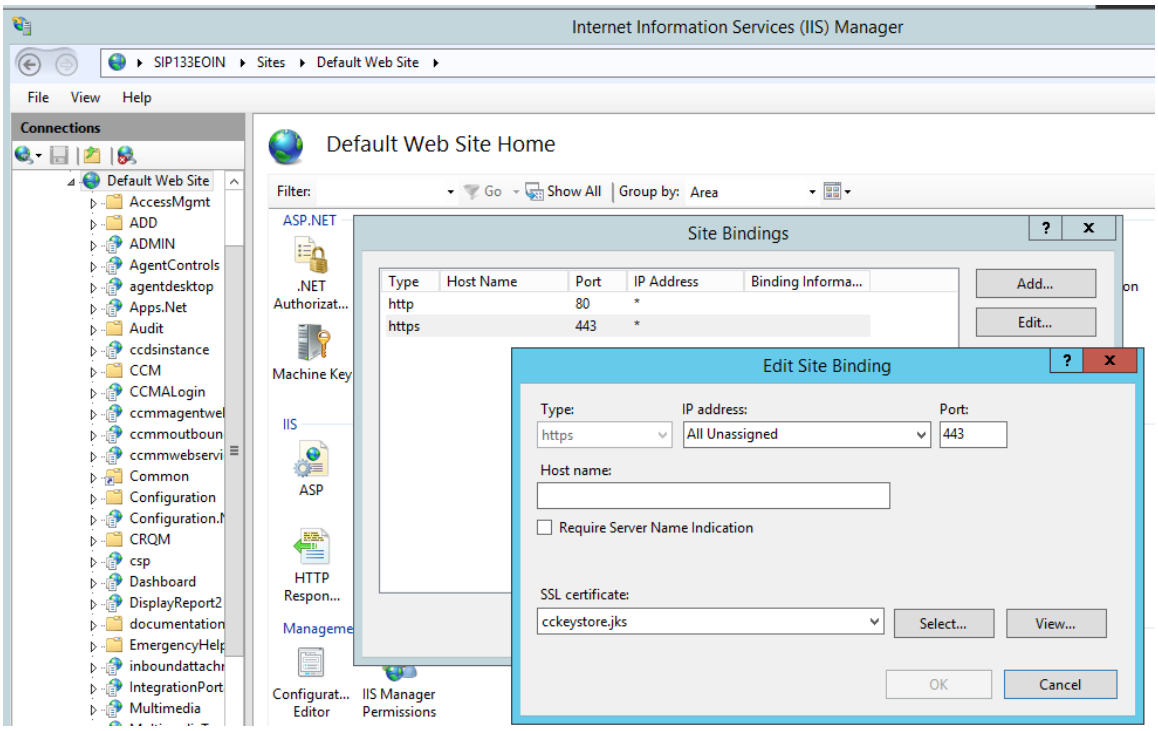
When the security level is set to **On** the following operations happen “silently” behind the scenes and are fully automated. Note the following steps are for informational purposes only and there are no manual steps required to implement what is shown over the next pages.

Internet Information Services

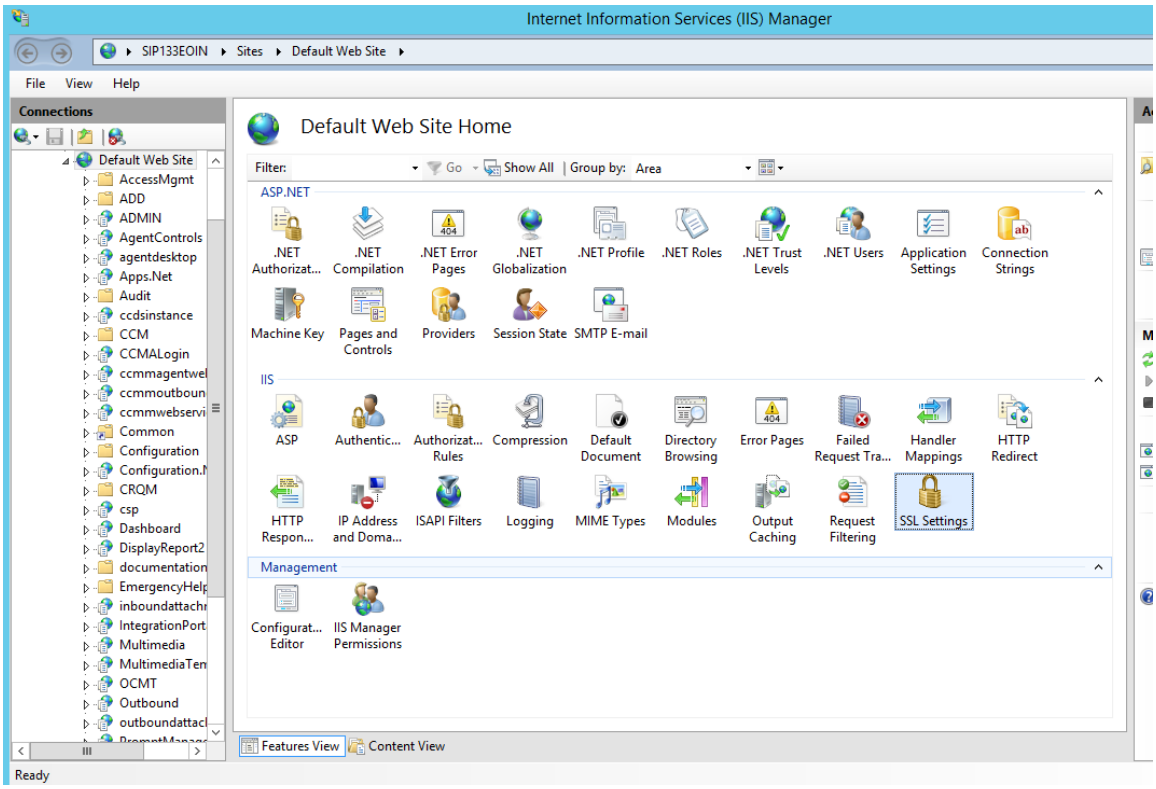
The signed server certificate that resides in the store is placed into the server certificates location in IIS. This can be viewed in the IIS Manager under the friendly name of “cckeystore.jks”



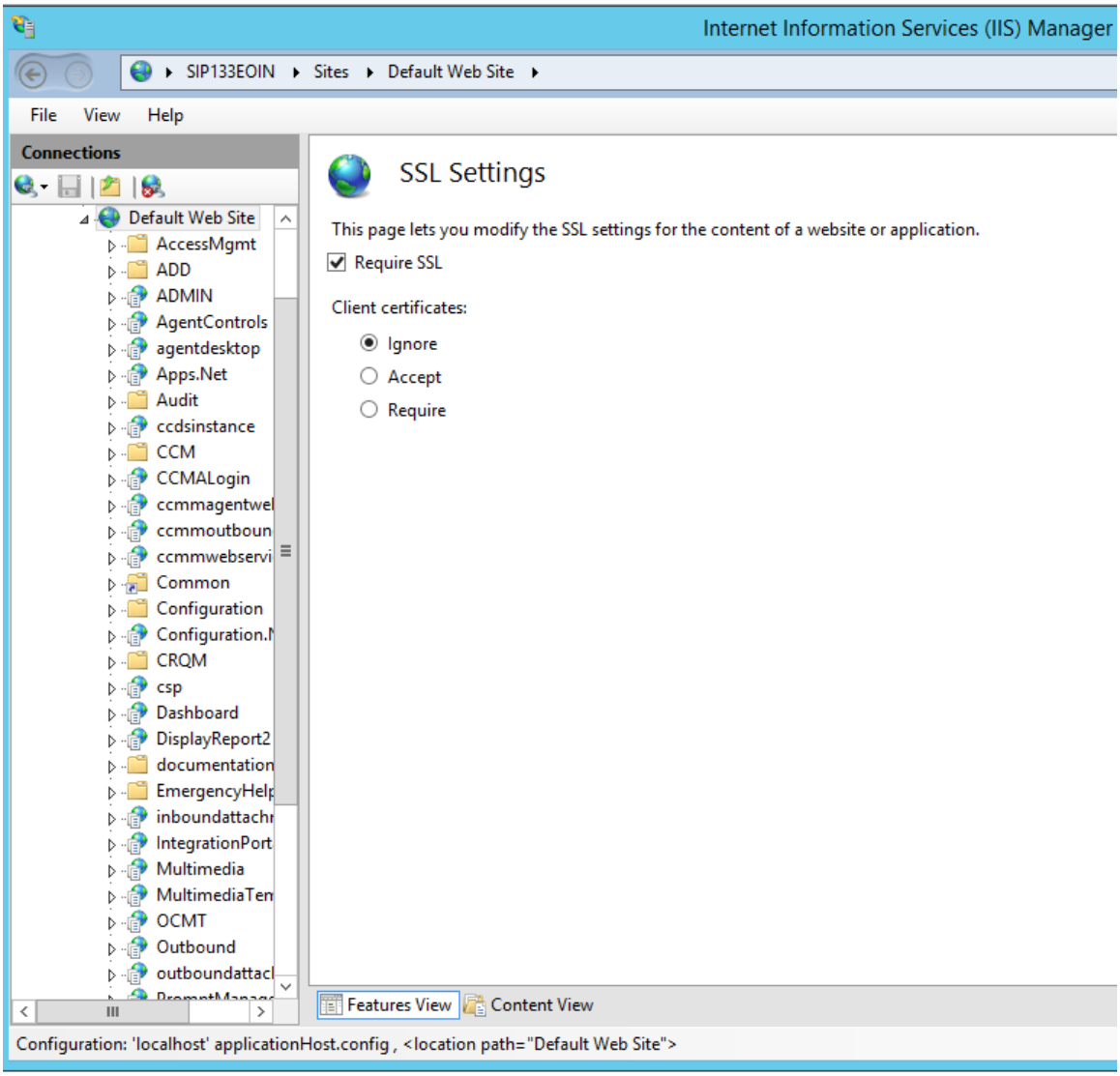
It then applies a binding to https with port 443 and associates that signed certificate with that binding.



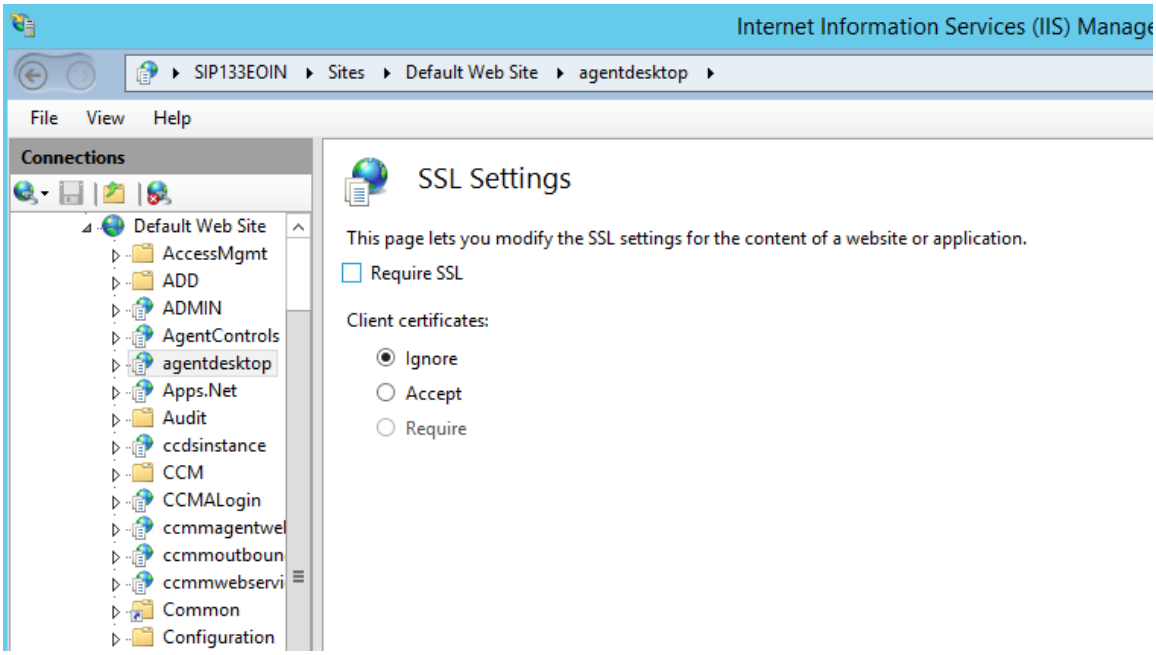
The next change is it sets the SSL settings for the Default Web Site


Internet Information Services (IIS) Manager
SIP133EOIN ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Default Web Site
AccessMgmt
ADD
ADMIN
AgentControls
agentdesktop
Apps.Net
Audit
ccdsinstance
CCM
CCMALogin
Common
Configuration
CRQM
csp
Dashboard
documentation
Multimedia
OCMT
Outbound
Default Web Site Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Profile
.NET Roles
.NET Trust Levels
.NET Users
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
IIS
ASP
Authentic...
Authorizat... Rules
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Redirect
HTTP Respon...
IP Address and Doma...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Management
Configurat... Editor
IIS Manager Permissions
Features View
Content View
Ready

It sets the Require SSL check box to check and Client certificates to Ignore



The last change is that this flag is turned off for the following folders to enable ClickOnce feature to be able to connect over HTTP while leaving the entire site as HTTPS and secure.



This is done for the following folders;

Agentdesktop

Dashboard

Admin

OCMT

TomCat / Jetty / CXF web servers

For these web servers the changes are not as extensive, when On is selected the encrypted password are sent to these servers and it changes configuration files to use HTTPS the next time they are restarted.

Security Manager Password change

This process, writing to the Tomcat, Jetty and CXF servers is activated when the password is changed on the Security Manager and prompts you as such.

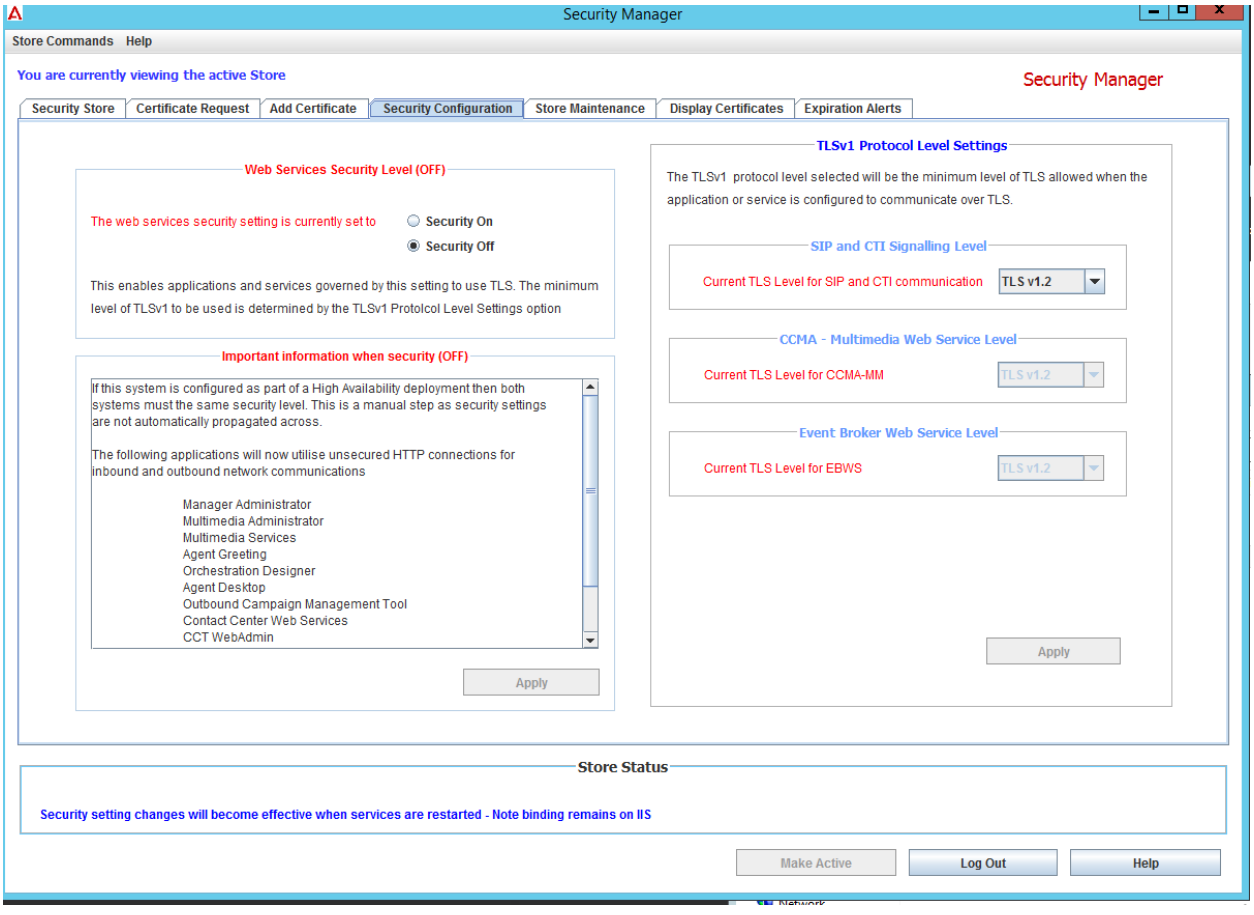
TURNING SECURITY LEVEL TO OFF

As with turning the security level to On, turning off also activates an automated sequence of events which will remove the security configuration on IIS, Tomcat, Jetty and CXF and the defined applications that use them.

Internet Information Services

In this case of IIS having been On already, which it will have been due to the new CC 7.0 Ignition wizard sequence which sets security level to On, the off operation or action on Security Manager will remove ONLY the Require SSL check box on the Default Web Site level.

This removes propagates to all of the folders under this site and therefore re-enables HTTP use on IIS.



It leaves the binding that was put in for the security On action and the server certificate that is associated with the binding as the information message shows above.

Why leave the server certificate and binding on IIS

The new browser based agent application introduced in release 7.0 requires that it establishes a connection over HTTPS. So the binding has to be left in place for this application.

This essentially allows HTTPS and HTTP at the same time on IIS.

TomCat / Jetty / CXF web servers

For these web servers the changes are not as extensive, when Off is selected the encrypted password are sent to these servers and it changes configuration files to use HTTP the next time they are restarted.

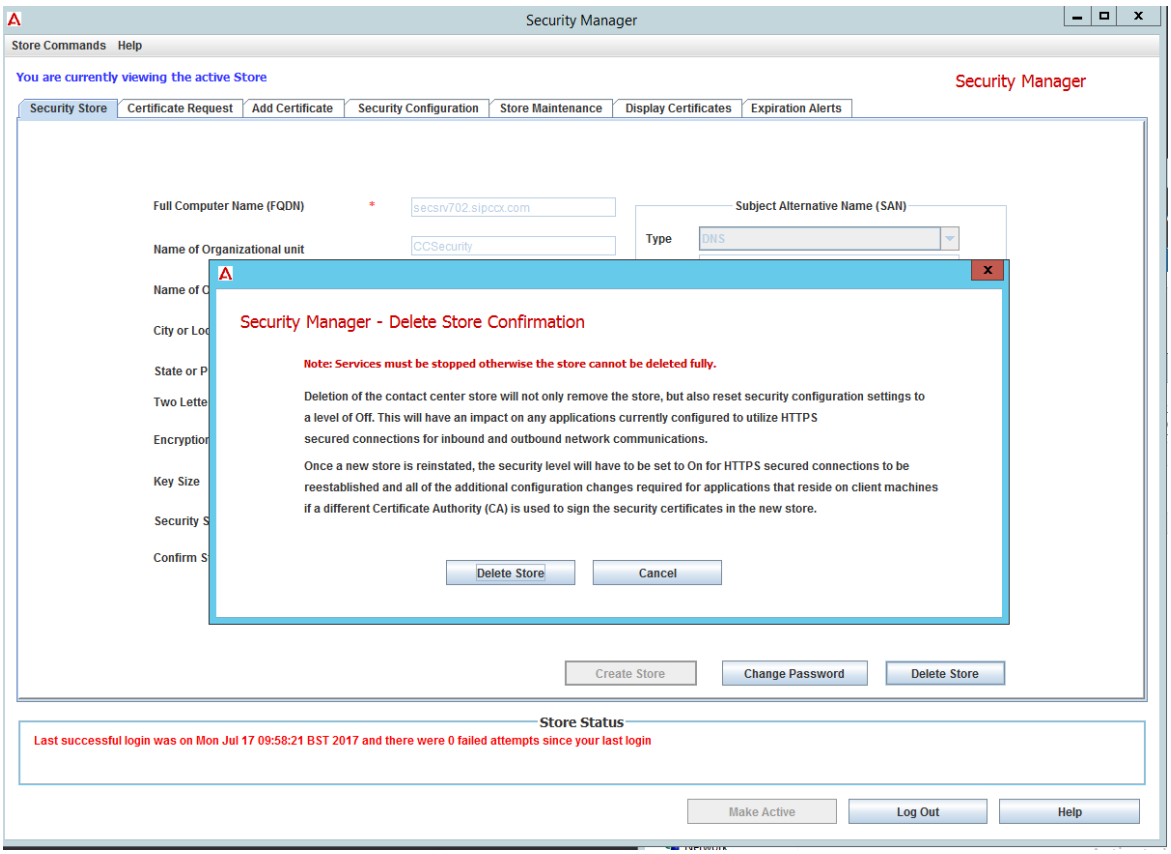
Appendix C - Replacing the OTB Store

As with the OTB section, the user can delete the OTB store and recreate the store and sign their own security certificates, in-house with their own CA or get some commercial company to sign it for them.

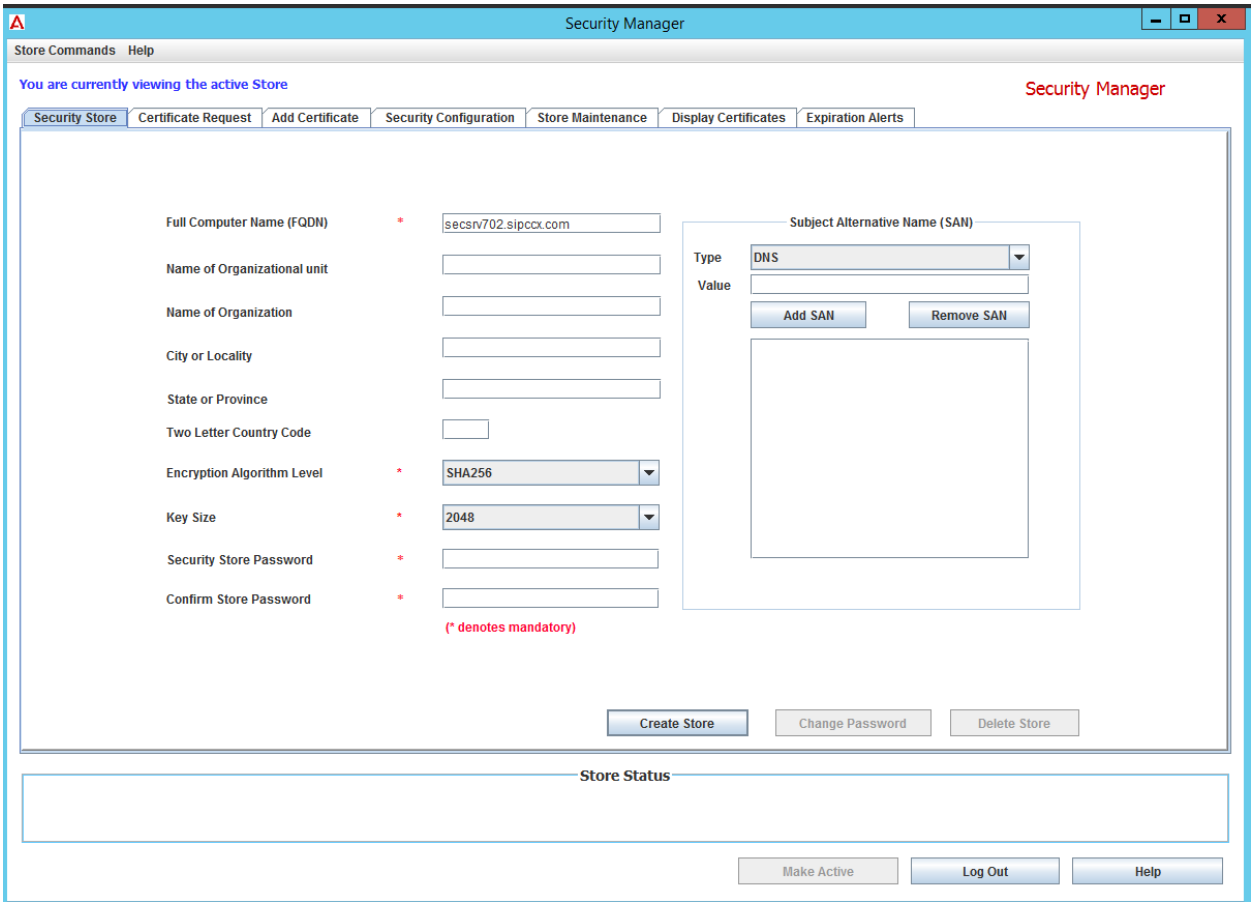
Security Manager has the capability to allow the user to generate the appropriate files to set-up their own custom certificate store.

How to

1. Stop services on the server
    a. Minimum services that need to be stopped is CCMS_OAM_CMF_Service which will bring down the CCMS_SIP_Service.
2. Launch Security Manager
3. On the main tab select the Delete Store button
4. A confirmation dialog will be presented and with the relevant information on the consequences of deleting the store

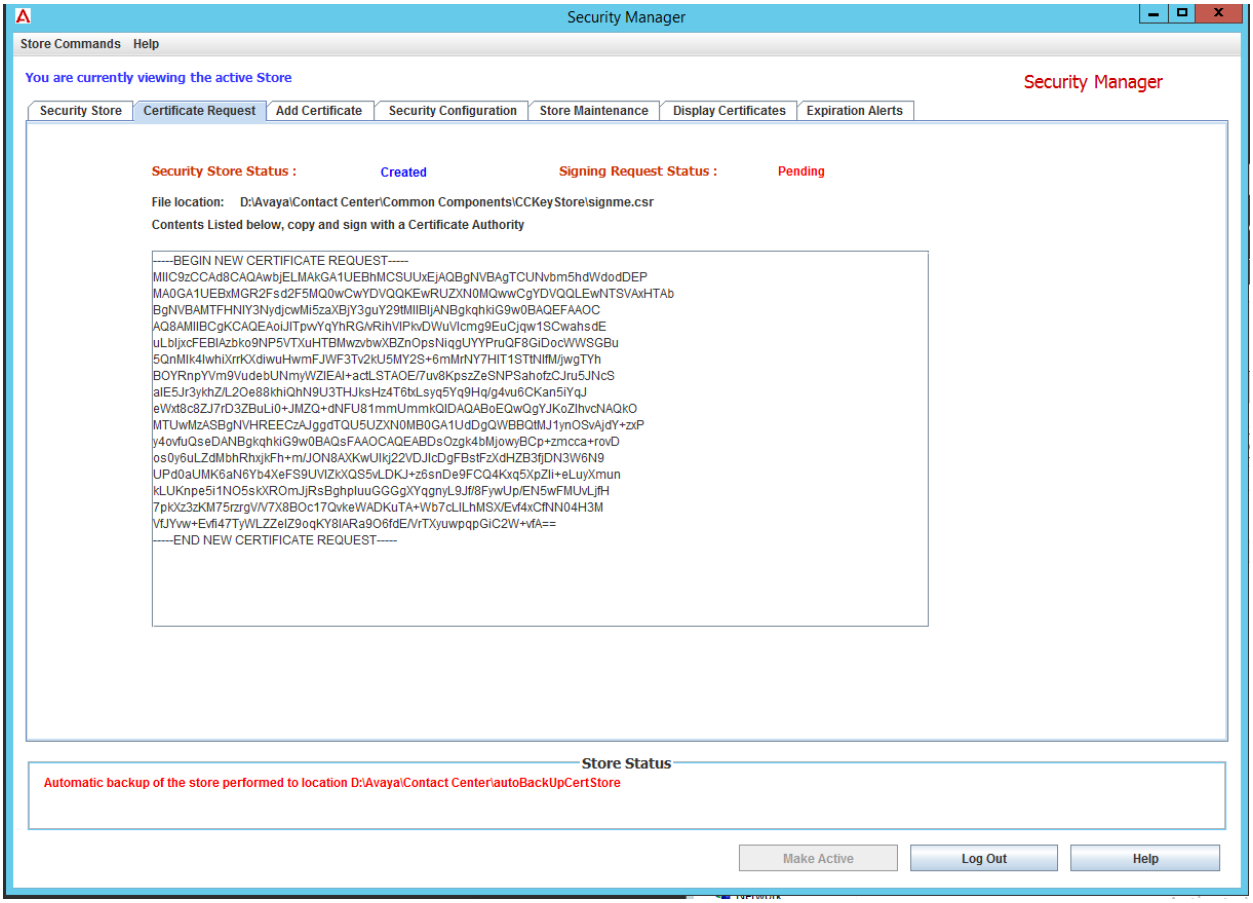


5. Select the Delete Store button. This will take a few seconds and will display the following information



6. As you will notice the Full Computer Name (FQDN) is prepopulated with the underlying name of the server.
    a. If this is changed from what it is then you will get the certificate name mismatch warning you see when using the OTB security certificates.
7. Fill in the information on the screen and press Create Store to create the store.

8. What should be presented to the user is the Certificate Signing Request (CSR) tab. This is the basis of the signed certificate and needs to be signed by a certificate authority (CA).



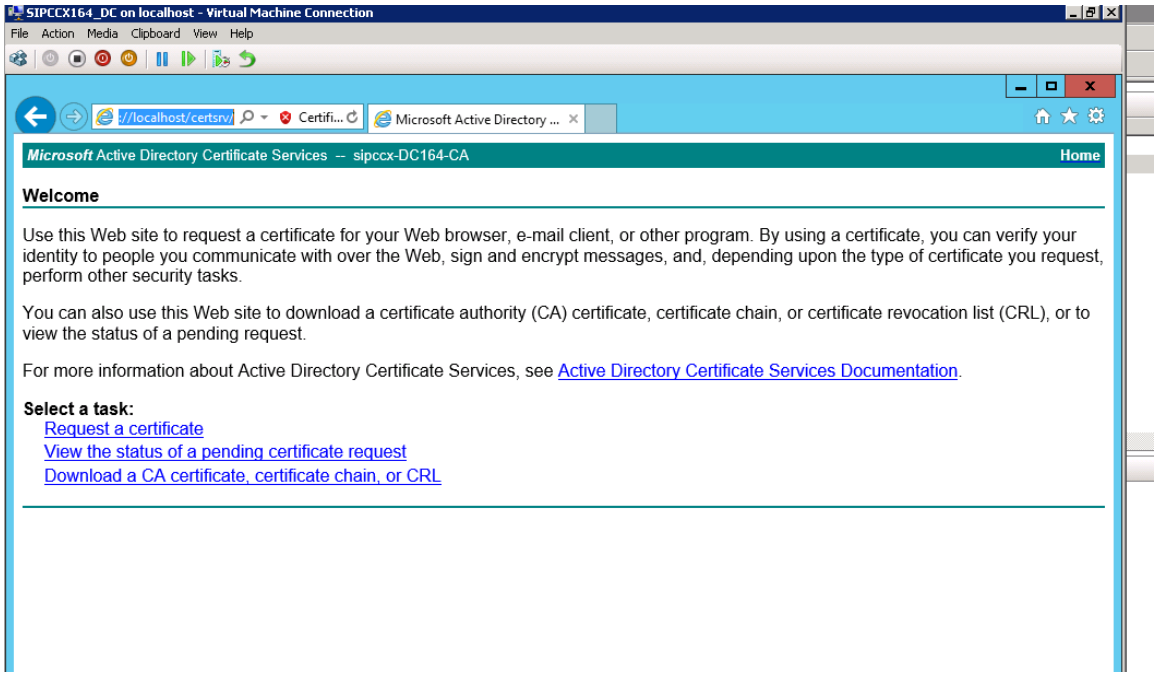
9. Copy this text or go to the location indicated on the screen and bring it to a certificate authority to be signed.

SIGNING A CERTIFICATE SIGNING REQUEST (CSR)

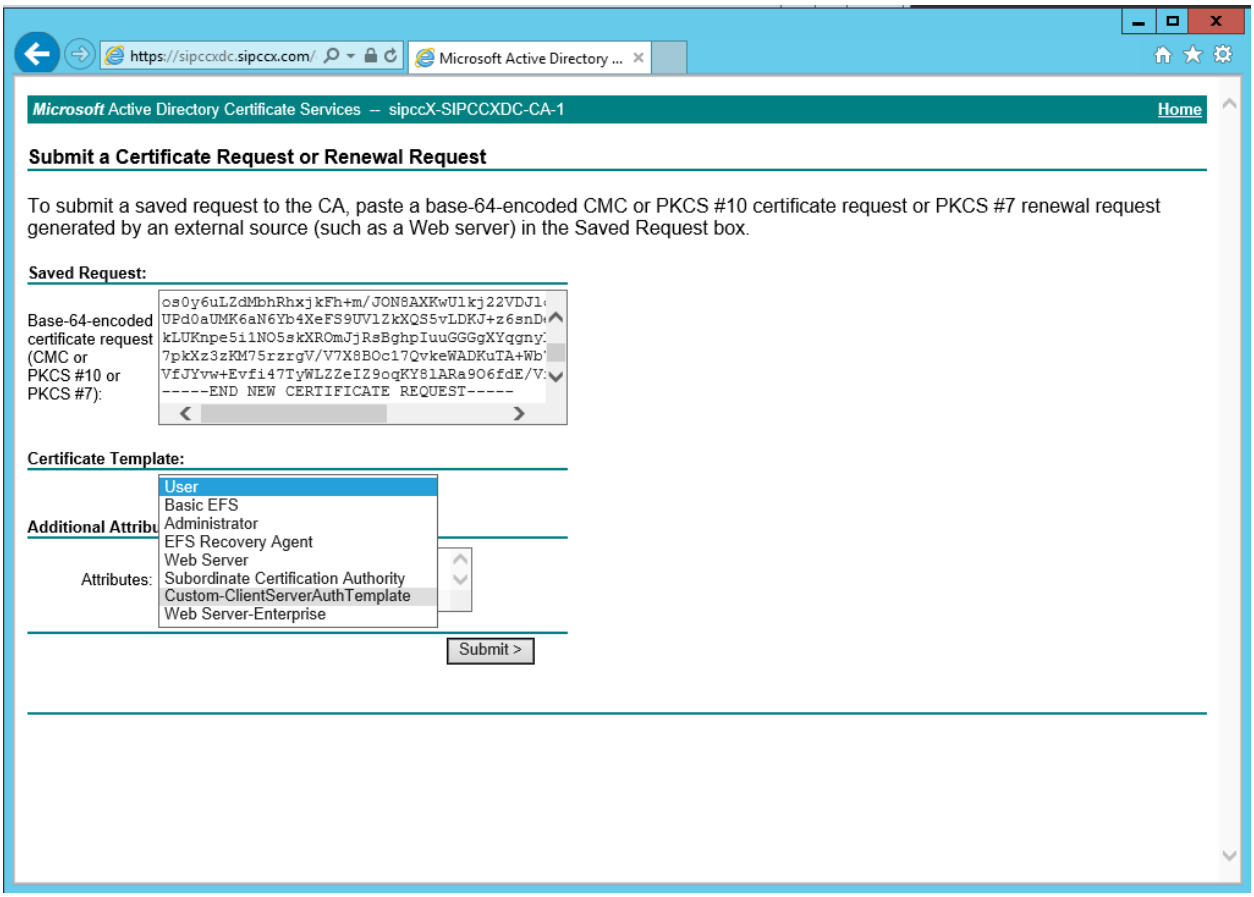
A Certificate Authority or CA can be created by adding a Role to an existing domain controller or server. The example we listed here is a Window 2012 domain controller

See example setup article https://technet.microsoft.com/en-us/library/cc731183.aspx

1. Go to the Certificate Authority and log into the machine or access it via a web page if it has it installed.
2. Copy the CSR file or contents of the file onto the CA server in a location of your choosing.
3. In this example I am using the Web interface, it can also be done via the Certificate Authority client on the server.
4. Launch Internet Explorer and add the following address
    a. https://localhost/certsrv/ [note localhost only if on server]

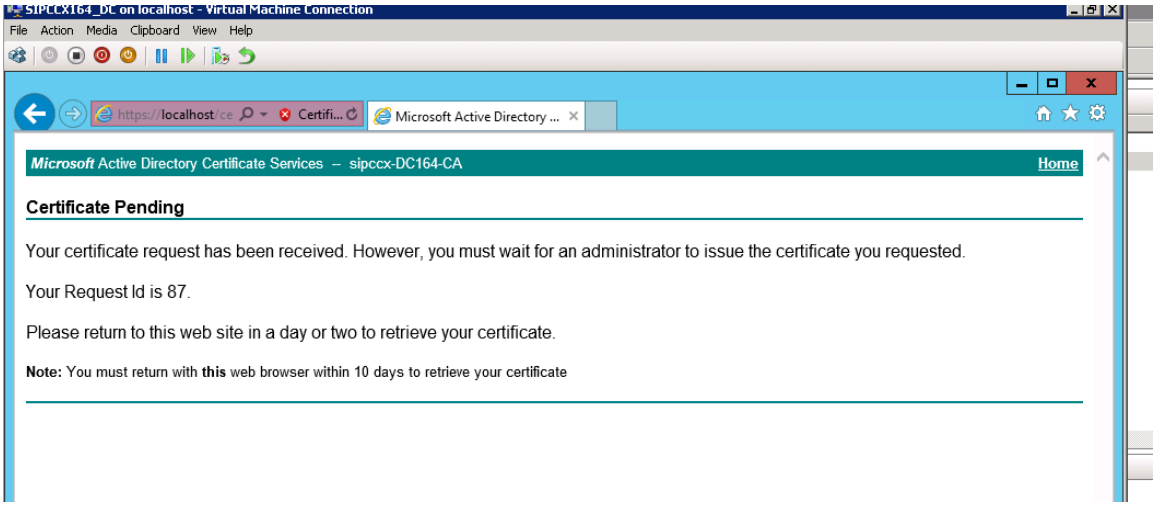


5. Select Request a certificate
6. Select advanced certificate request
7. Select Submit a certificate request by using a base-64-encoded or PKCS#19 file, or submit a renewal request by using a base-64-encoded PKCS #7 file
8. Copy in the CSR file contents into the window presented to you.
9. Ensure the template used to sign the CSR has Client and Server Authentication.

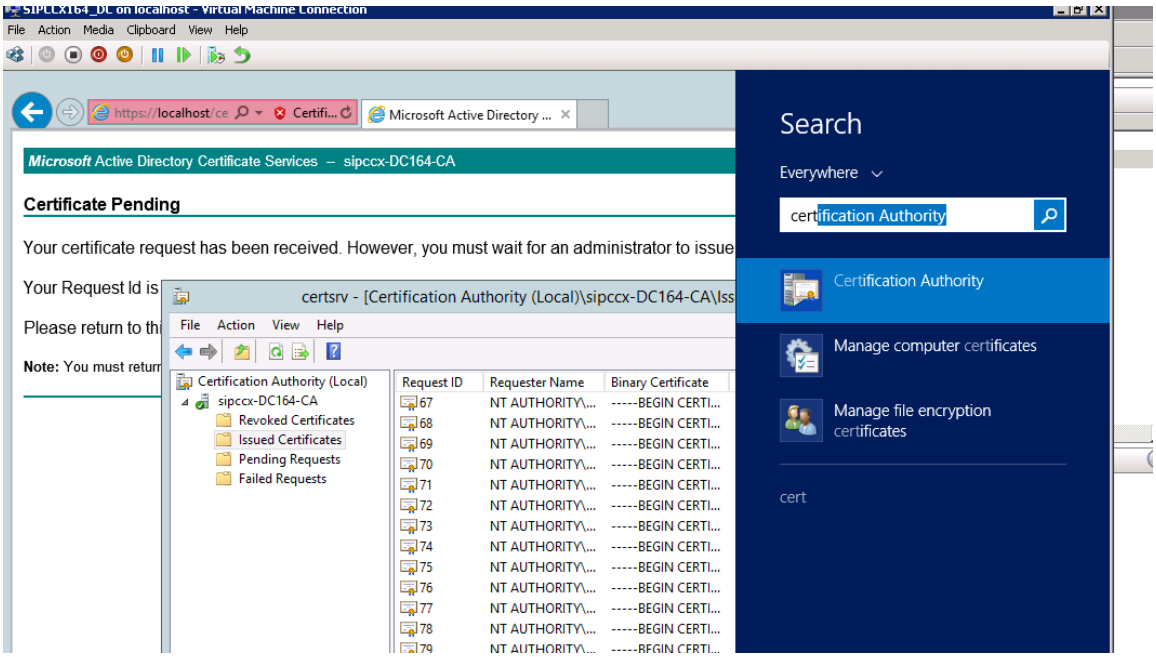


10. Hit Submit

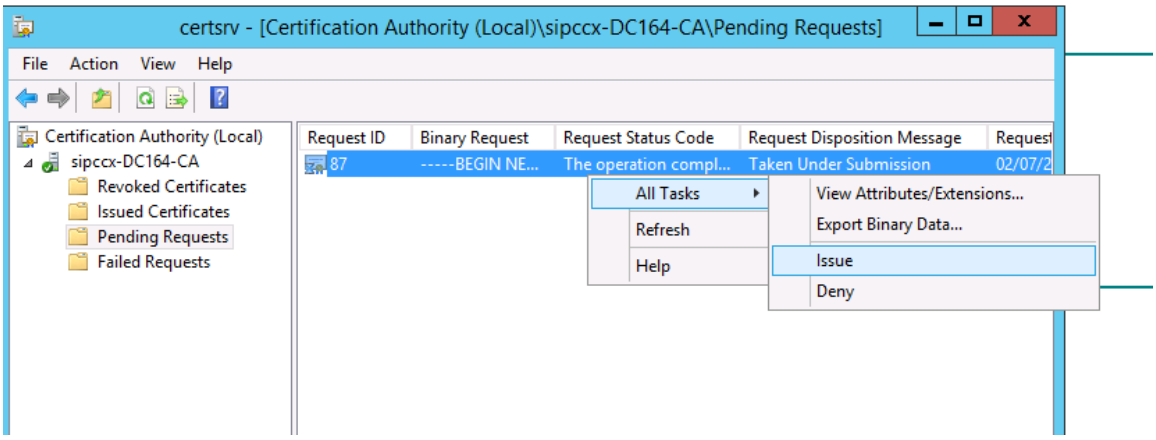
11. To get the certificate you must do the launch Certificate Authority Management Console



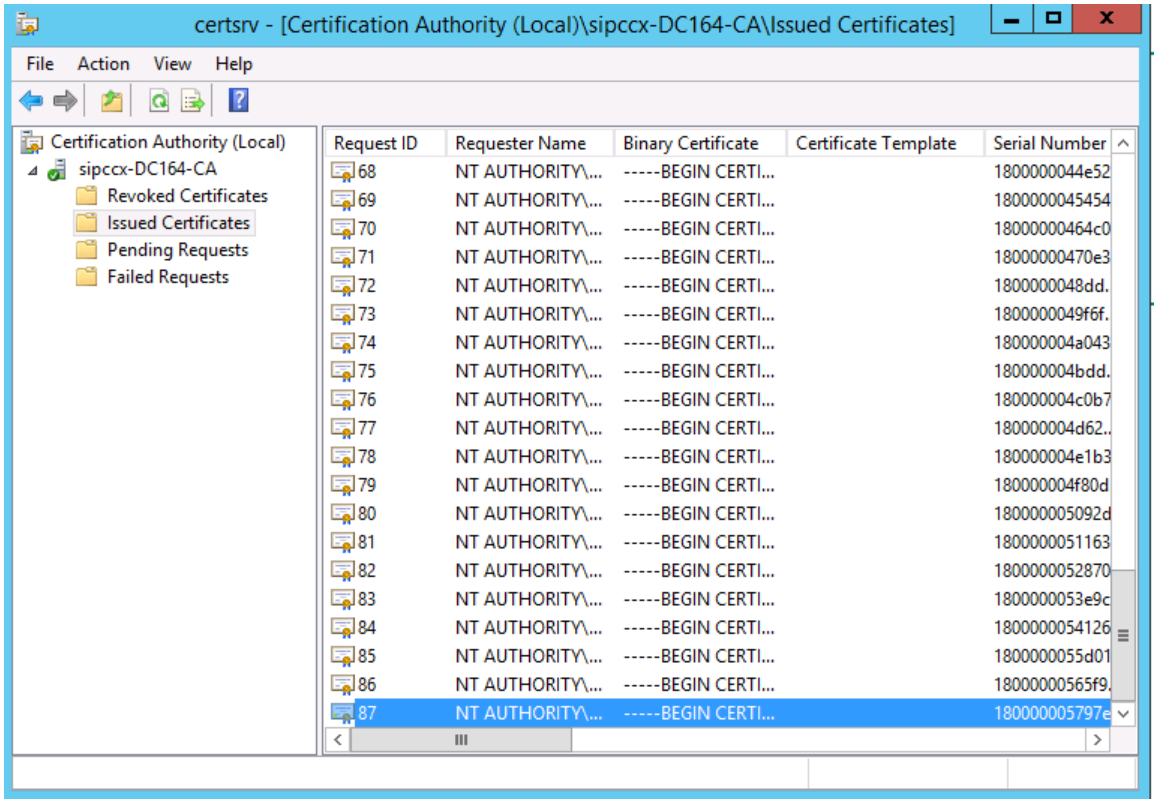
12. In Windows 2012 server you can right select the windows icon bottom left and select Search option and then type in cert and it should bring up the application you require



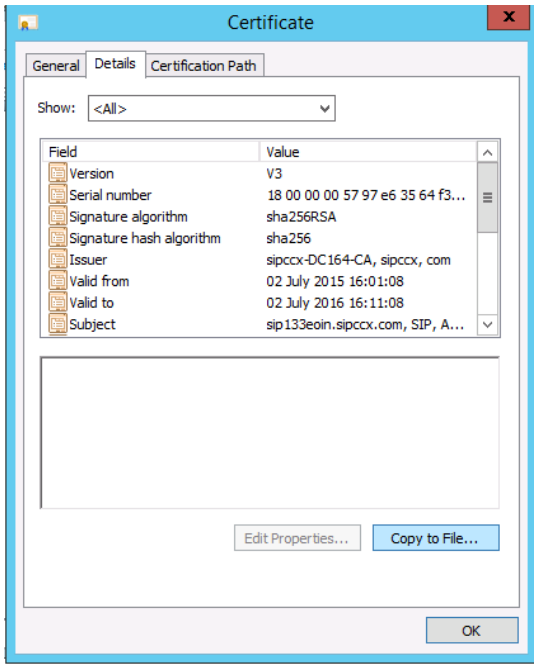
13. Once launched perform the following steps
    a. Select Pending Request
    b. Select the number of the pending request the previous screen informed you about
    c. Right select and select All tasks and Issue



d. Now go to Issued Certificates and go to the bottom of the list or search for your number.



e. Double click the certificate entry
f. Go to details tab
g. Select Copy to File… option

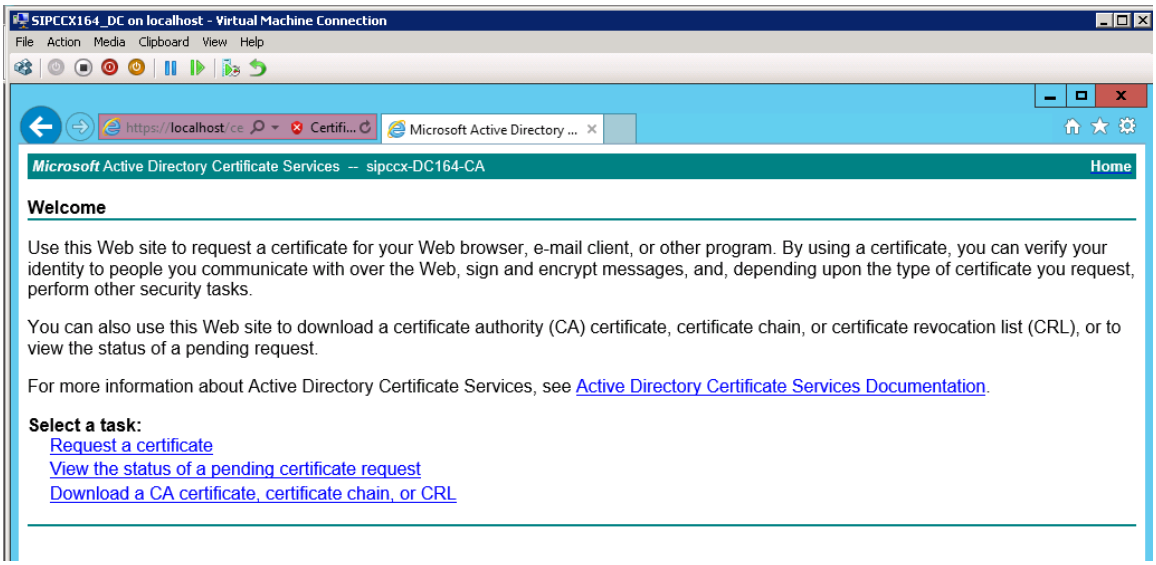


h. Hit Next
i. Leave default setting and hit Next
j. Select location where you want the file to be saved
k. Hit Next
l. Hit Finish
m. Select Ok on the dialog
n. Hit Ok
o. Go to the location and confirm the file is there and rename it to something appropriate. (Do not change the file type)

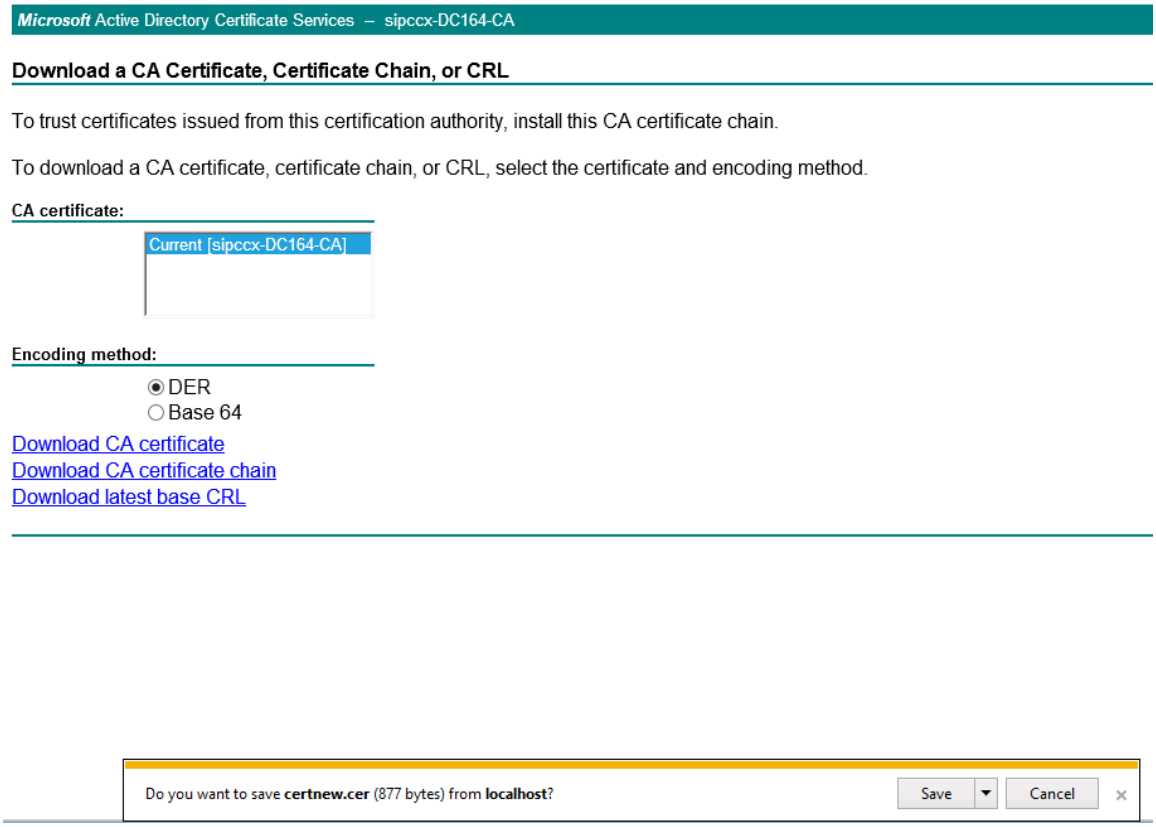
GETTING THE ROOT CERTIFICATE AUTHORITY CERTIFICATE

To partner the new signed certificate you have to retrieve the CA root certificate as well. Follow these steps:

1. Open the web page for the certificate authority if closed
2. Look to the right and select the Home link.
3. Select the Download a CA certificate, certificate chain, or CRL link



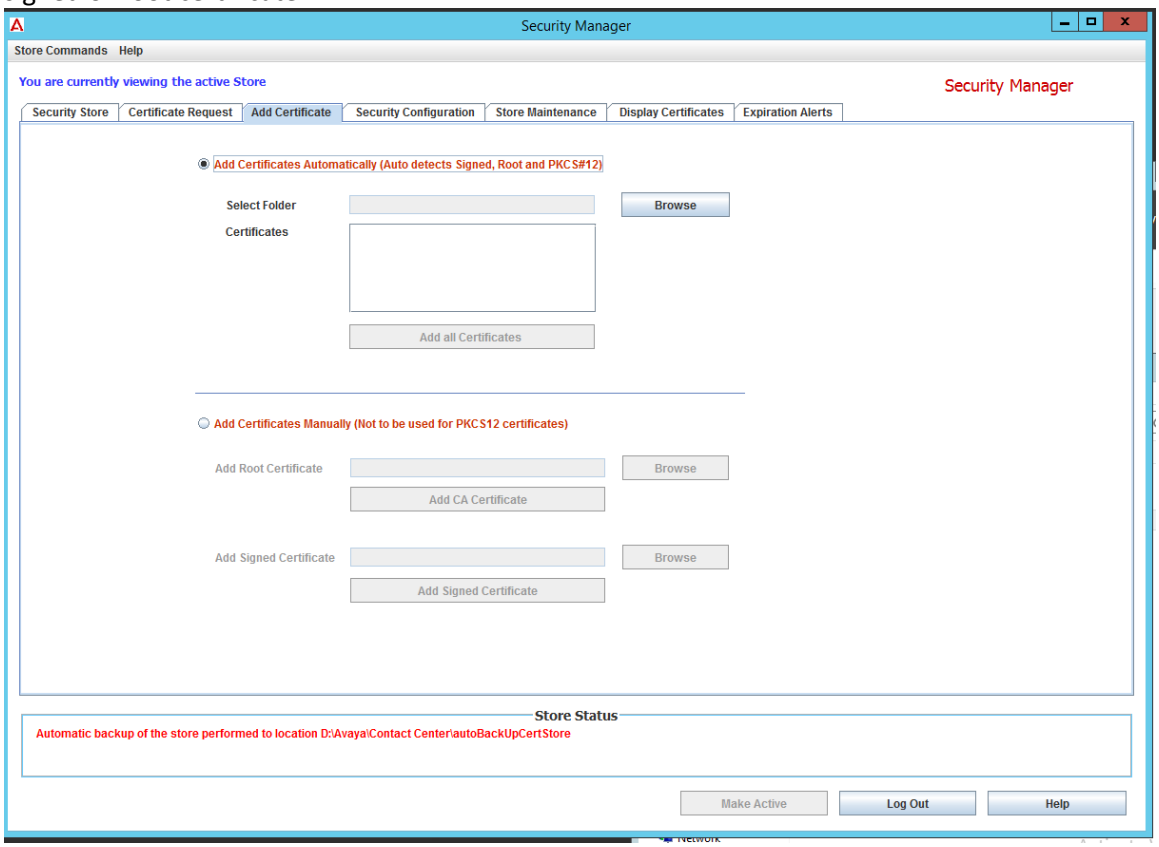
4. Select the Download CA certificate link and save the file (see bottom of screen)



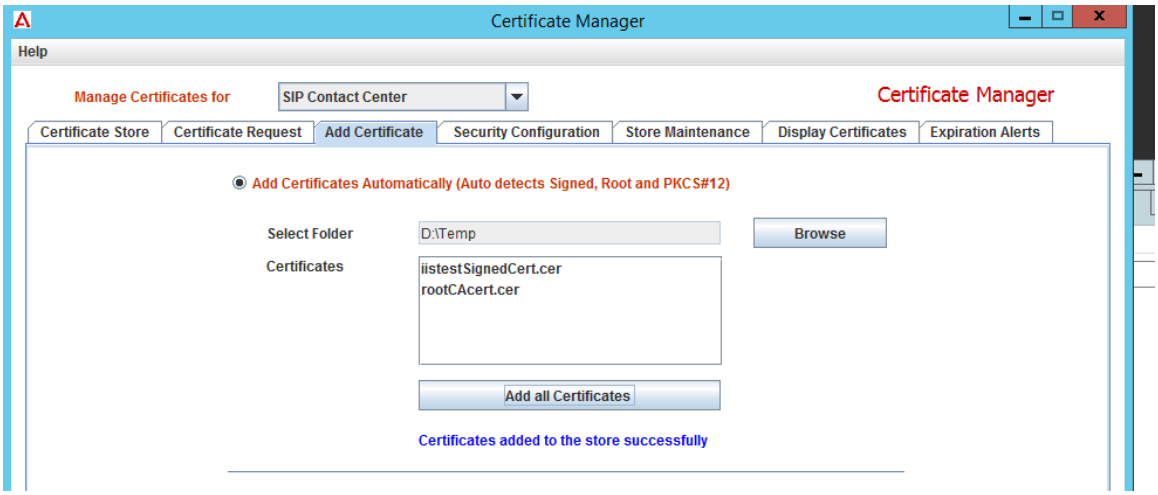
APPLYING THE CERTIFICATES TO SECURITY MANAGER

Now to place the certificates into the Contact Center certificate store

1. Launch Security Manager
2. Go to the Add Certificate tab
3. You have two options
    a. Select the folder where the certificates are and let the application decide which the signed cert is and which is the root certificate. (first option on the screen and enabled.
    b. Select the Add certificates manually option and then use the specific options to add signed or root certificate.



4. So add the two certificates you created using either method. Remember select only the folder for the Automatic detection option and not the file.



5. Confirm the files are in by selecting the Display Certificates tab and review.

RESTART SERVICES AND SET SECURITY LEVEL

Once the new store is in place, restart services and then reapply the required security levels as deletion of the store will remove all security settings in readiness for the new store and certificates.