Avaya Interaction Center

Security Guide

Release 7.3.x

July 2021

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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN Avaya HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/LicenseInfo under the link "Avaya Terms of Use for Hosted Services" or such successor site as designated by Avaya, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" or such successor site as designated by Avaya, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in Section M(i)1 or 2 as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time as indicated in the order, Documentation, or as authorized by Avaya in writing. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Heritage Nortel Software

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the

protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "**Unit**" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or onmultiple Servers provided that each of the Servers on which theSoftware is installed communicates with no more than oneInstance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

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

Copyright

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"**Third Party Components**" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS sourcecode (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD

PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BEAUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643- 2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com/ (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Introduction

Intended audience

This guide is intended for system administrators who are responsible for the security of the servers where IC 7.3 is installed. The measures described in this guide are not exhaustive. Administrators must manage their network of computers as a whole.

You must keep this guide secure. This guide describes the security features of Avaya IC 7.3 and is a potential security risk if distributed to a wide audience.

Scope of the guide

This guide describes the security-related features and services for IC. IC meets the enterprise needs for a multichannel Contact Center solution, while residing within the corporate intranet. The corporate firewall protects IC.

Related Avaya product security guides

This guide is a part of the set of security guides that describe the potential security risks to Avaya products and the features that Avaya products offer to mitigate these security risks.

This guide references other product documentation for the actual procedures for configuring and using security features.

Other product-specific security guides cover the following products:

- Operational Analyst
- Experience Portal

Additionally, the Avaya Cross-Product Security Guide describes the security risks and mitigating features integrated into all Avaya products. This guide provides information on security risks and identifies security features implemented within the products of Avaya.

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.

7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.

8. Click **Enter**.

Multilayer hardening strategy of Avaya

To prevent security violations and attacks, IC uses the following multilayer hardening strategy of Avaya:

- Default security
- Secure communications

The following sections provide a summary of hardening steps for Windows Server and Internet Explorer.

Default security

You must apply the security updates for the operating system (OS) when Windows, Solaris, or AIX (up to 7.3.2) platforms supported by IC 7.3 release the updates. If Avaya finds any problems with a particular OS upgrade or patch, Avaya issues a security advisory.

Avaya provides recommended ranges of access ports, services, and executables. These recommendations help to protect the system from virus attacks. For more information on Avaya Security Advisories, see Avaya Security Advisories.

It is advisable to enhance security by disabling non-secure service ports which are configured by default, for example, telnet and FTP.

Secure communications

Secure communications use numerous features and protocols to prevent access to and the transmissions from Avaya communications systems. Avaya uses media encryption to ensure privacy for the voice stream. Along with media encryption, integrated signaling security protects and authenticates messages to all connected media gateways and IP telephones and eliminates tampering with confidential call information. These features protect sensitive information such as caller and called party numbers, user authorization, barrier codes, sensitive credit card numbers, and other personal information that the caller uses while making calls to banks or automated retailers.

You can also encrypt critical adjunct connections, for example, the CTI link that can be separated in a dedicated security zone.

With Application Enablement Services (AES) 4.2 onwards, customers can secure the CTI link between the IC Telephony Server and AES machine.

Additionally, IC 7.3 provides secure communication between the following systems within IC or the adjunct of IC:

- IC Website framework

  See the **Configuring IC Websites over HTTPs** section in the *Interaction Center 7.3.x Installation and Configuration*.

- Collaborative form filling (requires signed jar files)

  See the **Tenant Websites** > **Collaborative Form-filling** section in the *Interaction Center 7.3.x Administration Guide.*

- Email Accounts for SSL

See the **Configuring the email accounts for SSL** section in the *Interaction Center 7.3.x Installation and Configuration*.

- License Server and WebLM (Managed by WebLM Team)

  See the **Installing and configuring the WebLM server** section in the *Avaya WebLM for Core Services 3.2 Developer Guide*.

For information about configuration, see the respective administration guides.

Software-only product

Avaya provides IC 7.3 as a software-only product. You must install IC on a customer-provided computer that runs an off-the-shelf operating system. To use IC, customers must ensure that the operating system and the other third-party software are secure.

Security updates

When security-related application updates are available, Avaya tests the updates, if applicable, and then makes the updates available to the customers. Avaya notifies customers about the availability of security updates through Security Advisories. Customers can subscribe to notifications about Security Advisories by email.

When software security updates are available, customers can install the updates or employ an installer from the services support. When Avaya installs the updates, the installer follows the best security practices for server access, file transfers, and data backups and restores.

IC security

Avaya designs and tests the products to ensure security. When Avaya sells IC release as a software package, the design and testing includes the security of the system and the components of the system.

The customer is responsible for the appropriate security configurations on the data network of the customer. The customer is also responsible for using and configuring the security features available on IC software. However, Avaya offers a service for assessing the network of the customer for performance and security issues. Avaya also offers configuration services for the product's digital certificates of Avaya.

Security benefits of digital signatures

Digital signatures provide the following for authentication and data integrity security:

- Maintaining secure authentication: The sender and recipient validate the public key of each other and hence, validate each other.
- Maintaining data integrity: The data exchanged between the sender and recipient is digitally signed. The recipient can validate the digital signature to know that the data is not modified.
- Verifying that a message comes from the actual sender by assuming that only the sender knows the private key that corresponds to the public key. Without knowing the private key, you cannot create a valid digital signature.
- Time stamping documents: A trusted party signs the document and the timestamp with the private key, thereby assuring that the document existed at the indicated time.

OpenSSL Poodle vulnerability fix

IC 7.3.3 onwards has OpenSSL upgraded to 0.9.8zc. It also has configuration provisions to not use SSLv3.

Refer to https://www.us-cert.gov/ncas/alerts/TA14-290A which lists the OpenSSL 0.9.8zc to prevent the Poodle (renegotiation) vulnerability.

IC 7.3.5 has the OpenSSL library upgraded further to 1.0.x.

OpenSSL particulars

IC 7.3.5 has the OpenSSL library version upgraded from 0.9.8 to 1.0.x.

IC components (TLS enabled servers) now accept TLSv1.2 during TLS handshake. However, if required TLS 1.1 and TLS 1.0 can be used.

TLS versions TLS 1.0 and TLS 1.1 can be enabled through configuration. For details, see *IC 7.3.5 Release Notes*.

Configuration parameter **allow_sslv3** (to allow SSLv3) is obsolete and must be removed when IC is upgraded to 7.3.5.

AIC components that needs auxiliary protection

The following is a list of Interaction Center components that require diligent protection through auxiliary means. It implies that the listed articles do not have world read/write access.

- ds.ffd
- vesp.imp
- pdm.xml
- If you use Full Text search, then note that the `<AVAYA_IC_HOME/etc/wru-sql/ec56` file has the DB password in clear text. This is a third party constraint.
- Ensure that the DB user being used for the IC DB access does not have DBA rights and has access only to IC related databases. This is to minimize the risk and ensure that no customer data can be accessed by rouge elements even if they have access to the DB.

Authenticating server administrator accounts

IC 7.3 supports standard Authentication and Authorization Services (AA Services) for authenticating administrator logins. IC does provide central authentication infrastructure external to IC using Active Directory (LDAP).

Through an authentication server, Avaya's support of AA Services facilitates the following:

- Enforcement of password aging, minimum length, and reuse requirements.
- Avaya product adherence to the enterprise corporate security standards regarding logins and passwords.

Intrusion detection

Host intrusion detection

An Intrusion Detection System (IDS) monitors operating systems and applications for some of the following common hacking techniques:

- Making unauthorized changes to system files.
- Altering configuration files.
- Replacing or infecting binaries.
- Downloading new executables.
- Creating unauthorized files and directories.

AIC does not provide this feature OOTB.

AIC is not tested or validated with any intrusion detection systems.

Configurable security

IC encryption

Overview

Digital encryption reduces the risk of intercepting phone conversations, voicemail, and signaling messages that support both. Digital phone calls consist of voice or bearer data and call signaling or control messages. Both bearer and signaling data can pass through many devices and networks, sometimes over a separate network or virtual path from each other. Without encrypting both data types, anyone with access can intercept the following:

- Secure CTI communication for voice.
- Email and chat communication.
- Translation or administration data in transit or saved on a storage device including IP addresses and routing information from which an attacker can analyze traffic patterns.
- Configuration data through TLS connections.
- Application-specific traffic.
- Data exchanged during management and administration sessions.

IC certificates use following Security aspects with encryption summary.

Encryption summary

The IC secure protocols are as follows:

Item	Application Name, Version, and Description *	Purpose of Encryption functionality in application, for example, secure internet communication between server and client	Encryption algorithms including key length, Hashes, and Messages Digests	Key Management algorithms and modulus sizes
1	Interaction Center 7.3 Contact Center software Poller and ICEmail servers.	Provides authentication for communication between IC components. For example, Poller and IMAP, and POP server. Also, between SMTP and ICEMail server.	3rd party Hunny Mail++ using OpenSSL (all supported by negotiation). It is recommended that the Exchange server restrict to usage of strong ciphers.	TLS negotiations
2	Interaction Center 7.3 Contact Center software License server.	Provides secure communication between the IC components (License server) and WebLM (Avaya License Management product) over HTTPS.	OpenSSL ciphers TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WIT	1024-bit RSA

Item	Application Name, Version, and Description *	Purpose of Encryption functionality in application, for example, secure internet communication between server and client	Encryption algorithms including key length, Hashes, and Messages Digests	Key Management algorithms and modulus sizes
			H_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128 _CBC_SHA,TLS_RSA_WIT H_AES_256_CBC_SHA,TL S_ECDH_ECDSA_WITH_A ES_128_CBC_SHA,TLS_E CDH_ECDSA_WITH_AES_ 256_CBC_SHA,TLS_ECD H_RSA_WITH_AES_128_ CBC_SHA,TLS_ECDH_RS A_WITH_AES_256_CBC_ SHA,TLS_ECDHE_ECDSA _WITH_AES_128_CBC_S HA,TLS_ECDHE_ECDSA_ WITH_AES_256_CBC_SH A,TLS_ECDHE_RSA_WIT H_AES_128_CBC_SHA,TL S_ECDHE_RSA_WITH_AE S_256_CBC_SHA,TLS_KR B5_WITH_3DES_EDE_CB C_SHA	
3	Interaction Center 7.3 Contact Center software VESP client and servers	VESP Toolkit provides secure communication with Directory server.	OpenSSL ALL:!aNULL:!eNULL:!ADH:! EXP:!MD5:!RC4:+HIGH:+M EDIUM:-LOW:-SSLv2:- SSLv3)	TLS negotiation
4	Interaction Center 7.3 Contact Center software Experience Portal and HTTPConnector.	Provides secure communication between the Voice Portal application and HTTPConnector.	Open SSL (ALL:!aNULL:!eNULL:!ADH: !EXP:!MD5:!RC4:+HIGH:+ MEDIUM:-LOW:-SSLv2:- SSLv3)	TLS negotiation

Digital certificates and server trust relationships

Chain of trust

Digital signatures certify that a public key belongs to its owner. To ensure authenticity, a trusted party signs the public key and the information about the key owner, creating a public-key certificate called a certificate.

A trusted party called Certification Authority (CA) issues digital certificates. A CA can be an external certification service provider or even government, or a CA can belong to the same organization as the entities it serves. CAs can also issue certificates to other sub-CAs that create a tree-like certification hierarchy called a Public Key Infrastructure (PKI).

Public Key Infrastructure

Public Key Infrastructure (PKI) combines software, encryption technologies, and services to help enterprises to secure their communications and transactions over data networks. A successful PKI provides management infrastructure for integrating public key technology, for example, digital certificates, public keys, and certificate authorities, across the infrastructure of the customer, including IP telephony. To conduct electronic business ensuring the following:

- The sending process or person is actually the originator.
- The receiving process or person is the intended recipient.
- The data integrity is not compromised.

Avaya uses standard X.509 PKI to manage certificates in an enterprise. In the enterprise, the hierarchy of certificates is always a top-down tree, with a root certificate at the top that represents the central CA. The certificate is integral to the trusted-party scheme and does not need third-party authentication.

PKI is limited to device-to-device authentication to automatically establish a TLS or similar connection to ensure confidentiality, integrity, and authenticity. The Voice over IP (VoIP) devices, which use Avaya software or need to establish a TLS connection with other devices that Avaya manufactures or distributes or the devices that you must use in coordination with Avaya products, use certificates issued by CAs or downloads from Signing Authorities (SA) under the Avaya Product PKI.

The following table uses Avaya public and private keys and their uses:

Entity	Key type	Uses
Subscriber	Private key	Digital signatures Encryption
Relying party	Public key	Authenticate TLS connections

Installing trusted certificates

IC relies on trusted certificates for secure interoperation. Customers can generate and install custom certificates for communication between the following servers:

- ICEmail and IMAP and POP server for authentication for communication between IC components. For more information, see the **Configuring Email Management, Configuring email accounts** and **Configuring the email accounts for SSL** topics in the *Avaya Interaction Center Release 7.3.x Installation and Configuration*.
- See *Interaction Center 7.3.x Administration Guide*, Chapter 6 Additional Configuration options; Configuring LDAP for secure communication between IC and LDAP authentication.
- See *Avaya Interaction Center Release 7.3.x Installation and Configuration* for securing communication for the following components.
  - Chapter 6: Configuring IC Websites over HTTPs
  - Chapter 10: Configuring Web Management; Configuring SSL security for Web servers (optional)
  - Chapter 15: Configuring and Deploying Avaya Agent Web Client; Advanced Configuration; Configuring SSL security for Avaya Agent Web Client (optional)
  - Chapter 16: Deploying Client SDK components; Starting and stopping the Client SDK server; Enabling the SDK server for SSL (optional)
  - Chapter 17: Deploying Web Services; Starting and stopping the Web Services server; Enabling the Web Services server on Windows

Administrative Accounts

Credentials complexity and expiration requirements

IC logins comply with:

- Password complexity policies
- Credentials expiration and lockout policies

Password complexity policies

The following table lists the password complexity rules that apply to passwords for local administrator and user accounts:

Password complexity rule	Parameters
Minimum length	This parameter is customer defined. Default value: 6
Forced Password Change	If set to Yes, this parameter forces agents to change their password when they log in after a Password change has been made in IC Manager. The exception to this is if PasswordReuseCycles is set to 0. The setting of 0 means there are no restrictions on password reuse. Default value: Yes
Maximum Login Attempts required	The maximum number of times the agent can attempt to log in with incorrect passwords before IC deactivates the account of the agent. To reactivate the account of the agent, the system administrator needs to clear the Disable Login check box on the Security tab of the Agent Manager screen. Default value: 3
Maximum Password Length	The maximum number of alphanumeric characters that you can use in a password. Default value: 40
Minimum Password Alphabets	The minimum number of alphabetic characters that you can use in a password. Default value: 1
Minimum Password Numerics	The minimum number of numeric characters that you can use in a password. Default value: 1
Number of Days	The NumOfDays and NumOfPasswordChanges properties work together. Agents cannot change their password more than the limit specified in NumOfDays. For example, with the default settings, agents can only change their password 3 times in a single day.
Number of Password Changes	The NumOfDays and NumOfPasswordChanges properties work together. Agents cannot change their password more times than specified in

Password complexity rule	Parameters
	NumOfPasswordChanges Default value: 3
Password Change	Determines whether agents can change their password at runtime. If you set this property to Yes, Avaya Agent users will have a Change Password option on the main agent interface. Default value: No
PasswordChangeDuration	The number of days before a password expires. If you want to specify that the password never expires, set this property to 0 (zero). Default value: 60
Password Reuse Cycles	The number of unique passwords that you must use before an agent can reuse a previous password. Default value: 5

Note: Attempts to create invalid passwords result in an instructive error message.

Password administration rules

Avaya Services does not access systems frequently but are often required to maintain maximum uptime, therefore, do not activate password aging for Avaya services accounts.

Applying profiles for role-based administration

Role Based Access Control (RBAC) helps businesses to assign server, gateway, and application access permissions based on the job function or role of a user. Avaya customers can create and modify profiles to help access Avaya server and gateway information according to job functions and business needs.

The following table lists the RBAC profile examples:

Profile name	Job function and access permissions
Administrator	Administrators have all system privileges. Administrators can create, update, delete, and monitor all the entities of the Avaya IC system including agents, workgroups, tenants, servers, and queues. Administrators can also perform agent, queue and workgroup assignments, administer scripts, assign supervisor accounts, assign roles to agents, and assign task load and task ceiling values to activities of an agent. Administrators can access the Business Advocate Administration tool and view all the Business Advocate administrative data.
Supervisor	If a supervisor is a member of a workgroup, that supervisor can modify the records of any agents belonging to that workgroup, but the supervisor cannot modify the agent records for anyone else. This authority is cumulative. Supervisors can change agent records for all agents, except agents with Clerk roles, in all the workgroups to which a supervisor belongs. A supervisor can: • Create, edit, and delete agent information. • Assign task load and task ceiling values to the activities of an agent. • Change agent property settings.

Profile name	Job function and access permissions
	• Assign roles to all agents of Supervisor level and below. • Monitor the agent activities on the system. • Generate reports. • Administer the content and resources of the system. Other supervisory duties include creating, updating, and deleting Web Self-Service documents and mail templates, administrating and approving Web self-service documents, and maintaining Auto Reply and other messages. If you want an agent to monitor the web chats for a workgroup, then the monitoring agent must be a supervisor. Supervisors can access the Business Advocate Administration tool, but they can only view site-specific agents and profile data.
Clerk	Clerks can create, delete, and update agent accounts and workgroups. Clerks can assign agents to workgroups, and import and export agent records to and from the system. In addition, clerks can assign roles to all agents of clerk level and lower. The difference between clerks and supervisors is that clerks can edit all workgroups and agents, while supervisors can only edit those workgroups to which the supervisors belong.
Operator	Operators are responsible for monitoring the status of the Avaya IC servers and can stop and start system servers to resolve problems. Operators also monitor alarms and server activities on the system.
Editor	Out-of-the-box, Editors facilitates content analysis administration.
Postmaster	Postmasters supervise email channel tasks for the agent and are authorized to administer email filters, mail accounts (POP3/SMTP accounts), and email queue changes.
Support	Support contacts assist customers who have problems with the products of the company. Support contacts do not have permission to log in to IC Manager.
Agent	Agents can receive tasks from any valid media channel, view personal statistics for the customer, and create and submit new web self-service documents. Agents do not have permission to log into IC Manager.

Configuring FIPS for Random Number Generation

Avaya CEC standards for Encryption states Random Number Generation as requirement.

On Windows, IC uses Microsoft Cryptographic Library and on Unices, it uses /dev/urand device to generate random number in case of authentication of client over SSL.

Windows PRNG is FIPS-140 compliant, as well as /dev/urandom.

The following are the steps to configure FIPS on Windows (https://support.microsoft.com/en-us/kb/2784079).

The first step in configuring a FIPS 140-2 compliant operating environment is to configure the computer that is running Windows Server 2008 R2 SP1 x64 by enabling the FIPS security setting. To enable the Windows Server FIPS security setting either in the Local Security Policy or as part of Group Policy, perform the following steps:

1. Using an account that has administrative credentials, log on to a computer that is running Windows Server 2008 R2 SP1 x64 on which any of the CRM Server roles are installed.
2. Click **Start**, click **Run**, type `gpedit.msc`, and then press **ENTER**.
3. In the Local Group Policy Editor, under the **Computer Configuration** node, double-click **Windows Settings**, and then double-click **Security Settings**.
4. Under the **Security Settings** node, double-click **Local Policies**, and then click **Security Options**.
5. In the details pane, double-click **System cryptography**: **Use FIPS-compliant algorithms for encryption, hashing, and signing**.
6. In the **System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing** dialog box, click **Enabled**, and then click **OK** to close the dialog box.
7. Close the Local Group Policy Editor.

   For more information, click the following article number to view the article in the Microsoft Knowledge Base:

   "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" security setting effects in Windows XP and in later versions of Windows

Server versions cloaking

To prevent version-specific attacks, server signatures, given in HTTP response headers by Apache and IIS servers, may be hidden.

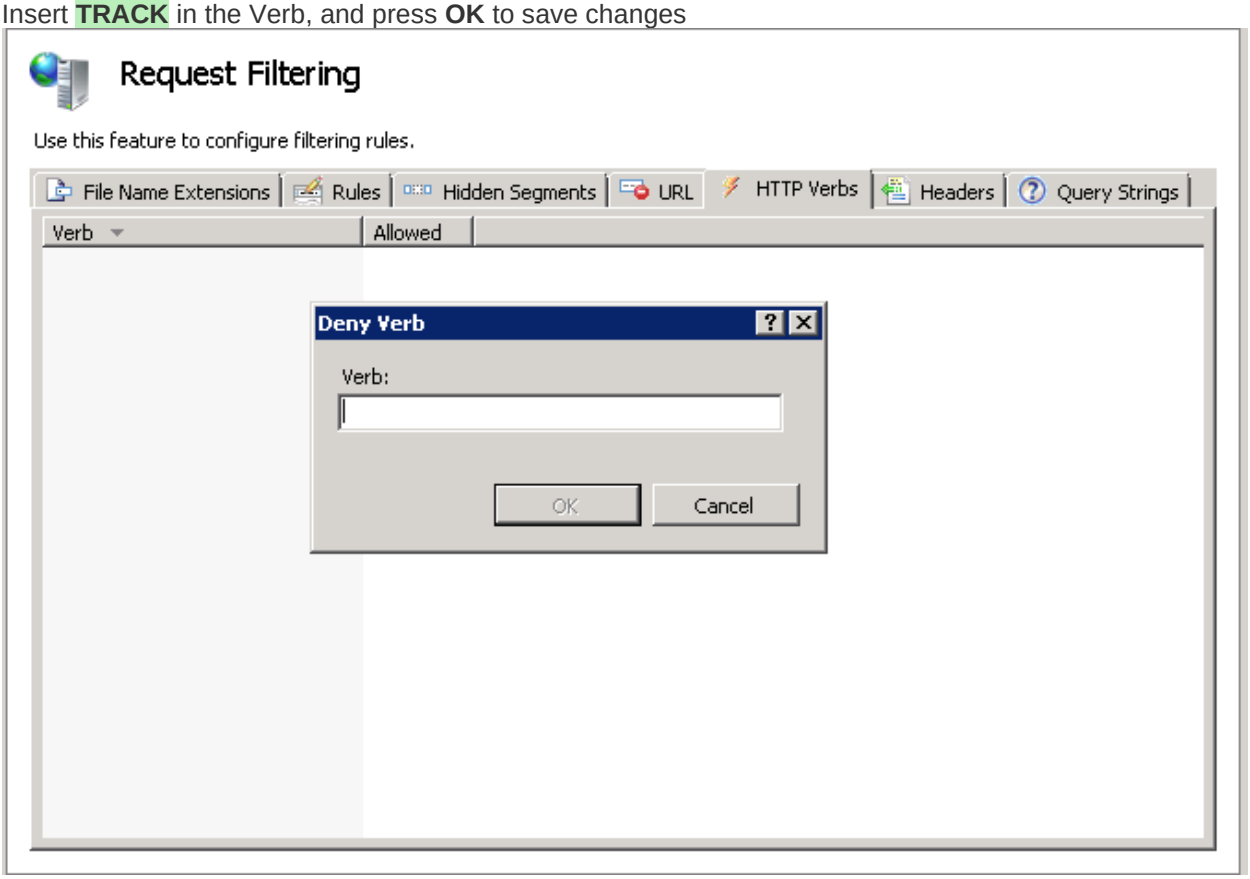
- To obtain that goal for Apache, mod_security module should be installed and configured with SecServerSignature directive. For additional information, visit ModSecurity/wiki/SecServerSignature.
- For IIS, this task is accomplished by installing the URL Rewriter module and modifying following headers in HTTP response: "X-Powered-By", "Server", "X-AspNet-Version". For more information visit microsoft.com/url-rewrite-module/modifying-http-response-headers.

Disabling Insecure HTTP Methods in IIS and Apache

To disable Insecure HTTP methods in IIS, follow these steps:

1. Double click on **Request Filtering.**
2. Change to the **HTTP Verbs** tab
3. From the **Actions** pane, select **Deny Verb.**

4. Insert **TRACK** in the Verb, and press **OK** to save changes



5. Repeat paragraph 6 with the remaining unsafe methods. (PUT, MOVE, DELETE, TRACE, OPTIONS)

Disabling Methods in Apache Insecure HTTP

1. To disable Insecure HTTP methods in Apace, follow these steps:
2. In ...Apache\conf\httpd.conf required to add the following:

```
<Location />
Order allow,deny
Allow from all
<LimitExcept POST GET>
Deny from all
</LimitExcept>
```

Network security integration

Securely integrating into a customer network

Firewall or topology configurations

See the Firewall guidelines for Avaya Agent Section under Network Topology and configuration guidelines in *Avaya Interaction Center Planning and Prerequisite Guide*.

See Appendix A for a list of accessible ports that IC Agents and Servers use.

Operational security

Intrusion Detection

None provided OOTB.

Secure Backup/Restore

None provided OOTB.

Remote Maintenance

AIC allows for remote maintenance, with the requirement for access into the customers network.

IC Manager allows for configuration and maintenance of IC servers which could have been deployed on disparate machines at different sites (in different geographical areas).

AIC does supports additional authentication environment for Windows deployment, through ASG (Avaya Security Gateway).

Avaya Security Gateway (ASG)

According to Avaya Common Engineering Criteria (CEC), strong authentication tools can be deployed in the environments where needs for large scale remote access to customer equipment exits. Such requirement can be satisfied by a multi-user, one-time token system (challenge-response) that is able to securely generate responses to satisfy challenges posed by remote systems.

ASG i.e. Access Security Gateway is identified as a solution to this. ASG is a secured and strong authentication mechanism that allows Avaya Service Engineers to login remotely to customer system using a Challenge-Response authentication mechanism. The following are key points in this Challenge/response Mechanism:

- There is no password
- A challenge is generated and it must be matched with a proper response
- A different challenge is generated upon each login attempt
- Access to generate proper response is restricted to Avaya Associates

When an Avaya service/support engineer tries to connect remotely to Avaya IC systems installed on Windows box, support personnel is presented the Avaya ASG Service login – init (member of Administrators group) or craft (member of Power Users group) – with a challenge and a customer specific Product ID. Once they have this information, they access ASG Web mobile (Must have Avaya global login access) and enter the customer specific Product ID, Service login name (init or craft), and the challenge. ASG mobile will generate the correct response. The service engineer then uses this response as the reply to the challenge in the login. This response is authenticated by the Avaya ASG Module installed on the IC Server system not by the Windows authentication. As a security precaution, the challenge changes (and hence response changes) every time a user attempts to login into the system, thus preventing replay attacks.

Avaya Security Advisories

Avaya Security Advisory overview

The Avaya Product Security Support Team (PSST) is responsible for the following:

- Managing Avaya product vulnerabilities and threats
- Maintaining information posted at http://support.avaya.com/security
- Performing security testing and auditing of Avaya's core products
- Resolving security-related field problems in support of Avaya Global Services
- Managing the securityalerts@avaya.com mailbox

As a result, the PSST actively monitors security issues related to the following topics:

- Avaya products
- Products that are incorporated into Avaya products
- General data networking and telecommunications, as identified by government agencies

When security vulnerability is identified, the PSST determines susceptibility of Avaya products to those vulnerabilities and assigns one of the four risk levels: High, Medium, Low, and None (see Interpreting an Avaya Security Advisory). Depending on the category of risk, the PSST creates an Avaya Security Advisory to notify customers of the vulnerability.

Depending on the vulnerability and its risk level, the advisory might include a recommended mitigation action, a recommendation regarding the use of a 3rd-party-provided patch, a planned Avaya software patch or upgrade, and additional guidance regarding the vulnerability.

Obtaining Avaya Security Advisories

Avaya Security Advisories are posted on the Security Support Web site at http://support.avaya.com/security. PSST also sends an email to customers who have signed up for receiving advisories. The advisories are distributed in a period as indicated in the following table:

Avaya's vulnerability classification	Target intervals between assessment and notification
High	Within 24 hours
Medium	Within 2 weeks
Low	Within 30 days
None	At Avaya's discretion

Customers can sign up to receive advisories by email on the Avaya Security Support Web site by following these steps:

1. Browse to http://support.avaya.com.
2. If you already have an account for email notifications, select **My E-notifications** on the lower right menu.

   If you do not have an account, click **New User Registration** and follow the instructions. To register, you need an Avaya SSO login and a Sold To number.
3. Log in using your existing credentials.

4. Once you have logged in, click **My Account**.
5. Click **Enroll for Avaya Applications**.
6. Click **Next**.
7. Click **Add More**.
8. Select **Customer Self Service — support.avaya.com** and click **Add Selected Items**.
9. Click **Submit** and when processing is complete, click **Close**.
10. Use the **Quick Links** drop down menu in the upper right-hand corner to select **Customer Self Service — support.avaya.com**.
11. Select **My E-notifications** on the lower right-hand menu.
12. At the Online Service Manager Web page, select **Add New E-Notifications** and click **Submit**.
13. Select **Security Advisories**, and click **Continue**.
14. Select **Add**, and then click **Submit**.

    The system displays a confirmation page.

    You are now ready to receive email E-Notifications whenever an Avaya Security Advisory is updated or published.

Interpreting an Avaya Security Advisory

The exact definitions that the Avaya Product Security Support Team (PSST) follows in classifying vulnerabilities relative to their potential threat to Avaya products is in Avaya's Security Vulnerability Classification document (http://support.avaya.com/elmodocs2/security/security_vulnerability_classification.pdf)

The following table summarizes the three main categories of Avaya's security vulnerability classification:

Vulnerability classification	Criteria for classification
High	The product is vulnerable to: • Attacks from a remote unauthenticated user who can easily access administrative control of a system or critical application without interaction with a user of the product beyond standard operating procedures. • Attacks from remote unauthenticated user who can easily cause the system or a critical application to shutdown, reboot, or become unusable without requiring interaction with a product user. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-002.htm.
Medium	The product does not meet criteria for high vulnerability, but is vulnerable to: • Attack from a user who can access a user account, and access does not directly require the privileges of a high-level administrative account. The system and critical application shutting down, rebooting, or becoming unusable are the effects of this attack. An existing administrative or local account is used for this attack. • Attack from a user who can access a local user account from which higher-level privileges are available. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-262.htm.

Vulnerability classification	Criteria for classification
Low	The product does not meet criteria for medium or high vulnerability, but is vulnerable to: • Compromise of the confidentiality, integrity, or availability of resources, although any compromise is difficult or unlikely without non-standard direct user interaction. • Non-critical applications shutting down, rebooting, or becoming unusable. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2007-015.htm.
None	A related third-party product has vulnerability but the affected software packages, modules, or configurations are not used on an Avaya product and there is therefore not vulnerable. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-261.htm.

Organizing an advisory

Overview

For an operating system or third-party software, a link is also provided for quick access to a Web site for more information. The information provides:

- A description of the risks.
- Instructions on how to correct the problem, which might include:
  a. Installing an update
  b. Revising administration of the product
  c. Describing what additional security fixes, if any, are included in the update.

Avaya Software-Only Products

A listing of the specific Avaya products that are used, but are not bundled with the operating system software that might be vulnerable.

Information includes:

- The product version affected.
- Possible actions to take to reduce or eliminate the risk.

Avaya System Products

A listing of specific Avaya products those are vulnerable or bundled with the operating system software that might be vulnerable.

Information includes:

- The level of risk.
- The product version affected.
- Possible actions to take to reduce or eliminate the risk.

Recommended Actions

The following information lists the vulnerability and descriptions to remove the vulnerability. The steps might include installing a security update, administering a security feature, or performing a software upgrade. For an operating system and third-party software, the recommended actions are identified in detail through the Web site links in the security advisory.

Software and Firmware updates

Delivering security updates

Avaya makes security updates available through the Avaya Security Web site at http://support.avaya.com/security. In addition, Avaya incorporates security updates, if applicable, in subsequent software release packages.

Based on the classification of vulnerability and the availability of a vendor-supplied update, Avaya makes a best effort attempt to provide remediation actions based on the following target intervals:

Vulnerability	Target remediation intervals
High	If Avaya needs to develop a software update, the Avaya Security Advisory provides a timeline for availability of the update. Avaya incorporates the fix into a separate service pack or update The maximum delivery time is 30 days. If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Medium	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update The maximum delivery time is one year. If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Low	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update. The maximum delivery time is one year. If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
None	No remediation actions are required.

Avaya product development staff incorporates a third-party update into its software in one of the following ways:

- Avaya bundles the specific update or the new release of the affected software with the Avaya IC software such that the security-related updates are automatically incorporated into the Avaya product operation.
- Avaya modifies the Avaya IC software so that the specific update or the new release of the affected software is appropriately incorporated into the Avaya IC operation.
- Avaya modifies the specific update or the new release of the affected software so that the security-related updates are automatically incorporated into the Avaya IC operation.

When Avaya incorporates one or more security fixes into its software, the fixes might be delivered in one of the following three forms:

- A security update: includes operating system and/or third-party software security fixes.
- An Avaya software update: includes software security fixes to the Avaya application software.
- An Avaya full release of software: includes all software for the Avaya product, including software security fixes to the Avaya application software and security fixes for the operating system and third-party fixes.

Validating a security update

When Avaya determines that a third-party security update applies to one or more of its products, Avaya product development tests the update on the affected current products to ensure there are no adverse effects to the published functionality of the products. In addition, when third-party updates are included in new software releases, the products are thoroughly tested.

Avaya-generated security updates are tested on all affected products prior to release. Avaya security updates are tested before incorporation into subsequent releases. Testing meets requirements of internal Avaya testing standards, including testing for the following:

- Denial of Service
- Encryption standards
- Certificate management
- Audits and logging
- Access control

Regulatory issues

Considerations for customers who must comply with the Sarbanes-Oxley Act

Note: The Sarbanes-Oxley Act law applies to U.S. customers only. Customers must rely on appropriate legal counsel and external auditors for interpretation of the act's requirements. Suggestions in this guide must not be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Sarbanes-Oxley Act of 2002 is a federal law enacted in response to a number of accounting scandals involving major U.S. corporations. A key requirement of the act is that public companies evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting. One major area of internal control consists of information technology controls. As a result, the Sarbanes-Oxley Act holds chief information officers responsible for the security, accuracy and the reliability of the systems that manage and report the financial data.

When a company uses data collected or transmitted by Avaya IC as part of its overall cost or revenue reporting and financial management, the company can use its security-related features to secure the data. Using these features can further demonstrate the company's good faith data management and reporting.

Avaya IC security features also help prevent unauthorized access to the customer's network.

Considerations for customers who must comply with the Graham-Leach-Bliley Act

Note: The Graham-Leach-Bliley Act applies to U.S. customers only. Customers must rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this guide must not be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Graham-Leach-Bliley Act (GLB) requires financial institutions to disclose privacy policies regarding customer data. This disclosure must describe the ways the institution may use and disclose private information.

Wherever indicated in their policy, financial institutions must protect the privacy of their customers, including the nonpublic, personal information of the customers. To ensure this protection, the Graham-Leach-Bliley Act mandates that all institutions establish appropriate administrative, technical, and physical safeguards.

Avaya IC data to which the Graham-Leach-Bliley Act might apply includes customer names, telephone numbers, called, and calling number data, and abbreviated dial lists.

Considerations for customers who must comply with Health Insurance Portability and Accountability Act

Note: The HIPAA applies to U.S. customers only. Customers must rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this guide must not be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires health care providers to disclose to health care recipients the ways in which the institution may use and disclose private information. HIPAA also requires health care providers to protect the privacy of certain individually identifiable health data for health care recipients.

Avaya IC data to which HIPAA might apply includes customer names and telephone numbers, and called and calling number data.

Considerations for customers who must comply with Communication Assistance for Law Enforcement Act

Note: The CALEA law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this guide must not be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

In response to concerns that emerging technologies such as digital and wireless communications are increasing the difficulty for law enforcement agencies to execute authorized surveillance, Congress enacted the Communication Assistance for Law Enforcement Act (CALEA) in 1994. CALEA preserves the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that the systems support the necessary surveillance capabilities of law enforcement agencies.

In an order effective September 23, 2005, the FCC concluded that CALEA applies to facilities-based broadband Internet access providers and interconnected VoIP service providers. To the extent that CALEA applies to Avaya offerings, such offerings have achieved compliance with the applicable CALEA requirements. In the event that an Avaya customer is subject to CALEA requirements, there are various third-party products, including Session Border Controller products that claim to provide or facilitate CALEA compliance. Examples of these products are:

- NexTone
- AcmePacket
- Sipera

Considerations for customers who must comply with Federal Information Security Management Act

Note: The Federal Information Security Management Act law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this guide must not be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Federal Information Security Management Act of 2002 provides for development and maintenance of minimum controls required to protect Federal information and information systems. Telecommunications systems and commercially-developed information security systems are included in the systems referenced under this act.

As a result, in most cases, government agencies can use Avaya's security-related features to secure telecommunications data. Avaya IC security features can also help prevent unauthorized access to the customer's network.

Features related to system security and documented in more detail in other sections of this guide are:

Considerations for customers who want to comply with ISO 17799

ISO 17799 of the International Standards Organization, "Information technology - Security techniques - Code of practice for information security management," is an internationally-accepted standard of good practice for information security. ISO 17799 suggests a well-structured set of controls to address information security risks, covering confidentiality, integrity and availability aspects. None of the suggested controls is mandatory; however, an organization wishing to be in compliance should show a security strategy that explains the decision not to implement key controls.

Considerations for non-US customers who must comply with regulations

Any specific country might have unique regulations that raise compliance issues for Avaya products. For example, countries such as Switzerland and Liechtenstein have Banking Secrecy laws that require a financial organization to inform a customer when the customer's identity has been revealed or that information that might reveal the customer's identity has been released. Such revelations can have negative affect on a bank's business. Therefore, a bank's communications services must be secure to prevent unauthorized access to data such as names, telephone numbers, account codes, and so on. To meet such requirements, Avaya IC, through its authentication processes, access control, and encryption methods, can protect call detail records, as well as the calls to customers. In this way, Avaya can help a customer comply with banking secrecy laws and protect the integrity of its business. Avaya also offers these security features to protect administered data that might reveal a customer's identity, for example, if a customer's IP address or phone number is contained within the firewall rules established for the product.

Basel II

Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework is a comprehensive set of banking standards compiled by the Basel Committee on Banking Supervision. The national banking overseers in many European countries seek to implement country-specific laws and procedures to meet the Basel II standards. To measure risk levels for a banking standards, Basel II mandates tracking of loss event data, which includes financial systems hacking, theft of data, and impersonation. To this end, Avaya systems offer a number of security features, such as those described in the previous paragraph, to minimize loss event data, and therefore, risk level measurements.

For any country in which Avaya IC is sold, there might be a need to inform customers about Avaya IC support for governmental regulations. In this case, the sales engineer or account executive should engage an Avaya legal officer, security specialist, or a compliance specialist to determine the specific ways in which Avaya IC might help the customer comply with regulations.

Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC) and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures the following:

The security properties of the product are evaluated by competent and independent licensed laboratories to determine their assurance.

Supporting documents that are used within the Common Criteria certification process define how the criteria and evaluation methods are applied when certifying specific technologies.

The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation.

All the signatories of the CCRA recognize these certificates.

The CC web portal, http://www.commoncriteriaportal.org/index.html, reports the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news, and events.

Security Enhancements

This section enlists security enhancements to various components of AIC as part of release 7.3.2.

General Security fixes

1. SSLv2 is a weak protocol and hacks exist to break it easily. The Directory server side code has been updated to not allow accepting SSLv2 connections.
2. Updated the allowed cipher list to use strong ciphers only (encrypted connections).
3. A bug in the WebChannel connector server allowed a malicious user to access files outside of the IC installation folder. This has been fixed.

Security related changes in Website:

Session Hijacking/spoofing prevention

Webservers are stateless servers. The way they understand and distinguish requests from multiple clients is through use of sessions. If an attacker gains access to the session information of a user, they can easily spoof client and perform unauthorized operations on the website.

A malicious user can send a link to an unsuspecting victim with the session id embedded as a link in an email. When the user clicks on the link and authenticates, the attacker has access to the session to which the user has logged in. The attacker can then hijack the user session to perform unauthorized operations.

In order to prevent this kind of an attack, the session id is changed every time the user does a login to the website. This prevents the attacker from hijacking the session as they are unaware of the actual session id of the authenticated session.

Secure and HTTPOnly Cookie

Attackers can use XSS to inject JavaScript code into a user's response stream to steal data from cookies. They can also cause cookie data to be sent to other malicious sites.

Cookies served by the website application are now served as HTTPOnly, which means that JavaScript code cannot access the cookies, which leads to the data stored in the cookie being protected from such attacks. As an additional measure, when the website is configured for HTTPS, the cookies are also served as secure, which means that they will not be submitted to the server for HTTP requests. This causes the data stored in the cookie to be more secure.

Minor Security Enhancements

1. HTTP response splitting attack prevention
2. The session cookie has now been renamed as AIC_SESSIONID instead of the default JSESSIONID
3. The session Id is no longer visible in the URL
4. The website will now never return a 404 error code in the response. This prevents bots from capturing this data for attacks.

Admin Website

SQL Injection

A filter to avoid SQL Injection related attacks has been provided for use with the Admin website. By default this filter is disabled, and can be enabled for those who wish to use this filter to avoid SQL injection related vulnerabilities.

Refer to *Appendix B* for further information as to how to enable and configure these filters.

The filter can be customized by modifying the “SQL attack pattern keywords”. A default set of keywords have already been provided to mitigate the most common SQL Injection attacks.

Logout functionality

“Logout” functionality has been added to the Admin website. The user now has an option to logout and login as a different user without closing the browser. This also adds security to the Admin website as the session cookies are deleted when the user logs out.

The “Logout” functionality is provided on the navigation bar as well as the selection bar.

Redirection Validation

All redirection parameters are now validated to allow redirection only to allowed URLs. This feature blocks a user from unknowingly navigating to malicious sites which may steal user data, or render arbitrary HTML or JavaScript content in the user’s browser.

Password Encryption

Passwords are now submitted encrypted to the server. This is true even when using HTTP. This feature prevents any attackers sniffing for traffic on the network to capture the plain text password. This prevents any unauthorized users from gaining access to the Administrative interface. It is also recommended to have HTTPS enabled for the websites.

Public Website

Reflected XSS

A security filter has been provided to prevent cross site scripting attacks which may inject arbitrary JavaScript content into a user’s browsing session. The injected content may exploit or harm a user’s browser and may also steal data from the session.

Configuration with security aspects

Configuration that are related to security aspects for Website and CSPortal are documented in Installation and Configuration document.

Topics like “limiting large requests”, “timeout to prevent DoS”, and “maximum connections/requests/threads” are covered in this guide under sections:

- Chapter 9: Configuring Web Management.
- Chapter 10: Deploying CSPortal WebAPI.

Security related changes in AAWC

ActiveX related changes

When an agent logged in to IC using AAWC logs out, the browser presents the login page again to the agent. This functionality is provided through and ActiveX control installed in the agent's browser. Vulnerability present in one of the methods used in this ActiveX control could lead an attacker to bypass the browser's "Same Origin Policy" and perform a "remote code execution".

Changes have been made in the ActiveX control to prevent exploiting the vulnerability. This changes the browser behavior when an agent logs out. The agent is no longer presented with a login page during the logout process. In case the agent needs to re-login, they need to explicitly invoke the browser again.

Reflected XSS

A security filter has been provided on the AAWC server side to prevent malicious users from performing reflected cross site scripting attacks.

Password Encryption

Passwords are now submitted encrypted to the server. This is true even when using HTTP. This feature prevents any attackers sniffing for traffic on the network to capture the plain text password. This prevents any unauthorized users from gaining access to the agent interface. It is also recommended to have HTTPS enabled for AAWC servers.

Error Handling

Whenever an error occurs in the application, the agent is redirected to an error page. The default implementation is to show a stack trace along with server details to the user. This is a big issue wherein a malicious user can understand the details of the system, and by gaining knowledge of the associated vulnerabilities, can compromise the security of the system

This behavior has now been changed to not to reveal any details regarding the system, thereby increasing the security.

Security related changes in SDK

Login Changed to POST

Login to SDK based custom client now submits the credentials to the server as a POST request as opposed to a GET request earlier. The credentials are also submitted as the body of the request and are no longer available on URL. This prevents the credentials from being cached at proxy servers which could be open to hacking. This also prevents malicious users sniffing traffic on the network from gaining access to the credentials.

Password Encryption

Passwords are now submitted encrypted to the server. This is true even when using HTTP. This feature prevents any attackers sniffing for traffic on the network to capture the plain text password. This prevents any unauthorized users from gaining access to the agent interface. It is also recommended to have HTTPS enabled for SDK servers.

Java Security

Introduction

Java 7u51 and higher versions have new security requirements for Rich Internet Applications (Applet & Web Start) to enhance authentication and authorization of the RIAs. If the RIA does not adhere to these requirements, it will be blocked.

The requirements are as follows:

- It is required to sign all RIAs (Applets and Web Start applications).
- It is required to set the "Permissions" attribute within the Manifest.

Refer *here* for more details on new security requirements.

Note:
This only applies to RIAs and not to Java on server or desktop applications that run outside of a browser. The application will be affected if it uses Java started through a web browser. It will not be affected if it runs anywhere outside of a web browser.

Modifications

To fulfill the security requirements, the following changes are done to the jar files:

1. Manifest attributes:
   The following manifest attributes are added in the manifest file of each jar:
   a. Application-Library-Allowable-Codebase: *
   b. Permissions: all-permissions
   c. Caller-Allowable-Codebase: *
   d. Codebase: *
2. Signer info: The jar has been signed using an Avaya certificate issued by Symantec.

Modification details

Impacted Components:

- Core Servers
- Web-Client
- Design & Admin (for jar version consistency)
- AARC (for jar version consistency)

Additional details about the modified components and Jars can be found in the following table:

Component	Jars	Deployment location
WebClient	s_avaya-ic-webclient.jar	<AVAYA_IC_HOME>/web/WebContent/lib
	s_common-base.jar	<AVAYA_IC_HOME>/web/WebContent/lib
	s_avaya-common.jar	<AVAYA_IC_HOME>/web/WebContent/lib
	s_avayaiccommon.jar	<AVAYA_IC_HOME>/web/WebContent/lib
	s_client-base.jar	<AVAYA_IC_HOME>/web/WebContent/lib

Component	Jars	Deployment location
	s_ssce.jar	<AVAYA_IC_HOME>/web/WebContent/lib
	cobrowse.jar	<AVAYA_IC_HOME>/web/WebContent/lib
	webphone.jar	<AVAYA_IC_HOME>/web/WebContent/lib
Core Servers	cobrowse.jar	<AVAYA_IC_HOME>/comp/icm/vdir
	cobrowse.jar	<AVAYA_IC_HOME>/Java/jar
	webphone.jar	<AVAYA_IC_HOME>/comp/icm/vdir
	webphone.jar	<AVAYA_IC_HOME>/Java/jar
	s_rlmanager-applet.jar	<AVAYA_IC_HOME>/email/jsp/lib
Design & Admin*	cobrowse.jar	<AVAYA_IC_HOME>/Java/jar
	webphone.jar	<AVAYA_IC_HOME>/Java/jar
AARC*	cobrowse.jar	<AVAYA_IC_HOME>/Webagent/jars
	webphone.jar	<AVAYA_IC_HOME>/Webagent/jars

*For consistency purpose.

Updating Jars (Optional)

The OOB Jars have default entries for Manifest attributes. However, if there is a need to make the application more secure, the manifest entries can be updated.

System Administrators can overwrite the application's signature and add the appropriate Manifest entries. While it does not involve code changes, modifying a JAR file breaks the digital signature and requires the jar to be signed again. If modifications are made to a signed document, the changes invalidate the document originally signed, so one needs to white-out the original signature and apply its own.

Tutorials on Modifying a Manifest file can be referred for updating the manifest. The sub-set of steps needed for updating to the latest requirements is:

1. Extract the `MANIFEST.MF` file by using following command:

   ```
   jar -xf <JAR_FILE> META-INF/MANIFEST.MF
   ```

2. Open the `META-INF/MANIFEST.MF` file in a text editor and update the values of following attributes based on your requirement:

   a. Codebase

      The `Codebase` attribute is used to restrict the code base of the JAR file to specific domains. Use this attribute to prevent someone from re-deploying your application on another website for malicious purposes.

      The default value for this attribute is set to "*", because enough information regarding this optional attribute is not known in advance (where will the application be deployed). Provide the actual hosting location and domain in order to restrict the application from being deployed at other locations. For example, Codebase: https://www.example.com.

   b. Caller-Allowable-Codebase

      The `Caller-Allowable-Codebase` attribute is used to identify the domains from which JavaScript code can make calls to the RIA without security prompts. Set this attribute to the domain that hosts

the JavaScript code. If a call is made from JavaScript code that is not located in a domain specified by the `Caller-Allowable-Codebase` attribute, the call is blocked.

The default value for this attribute is set to "*".Provide the actual hosting location and domain in order to restrict the application from being deployed at other locations.

c. Application-Library-Allowable-Codebase:

The `Application-Library-Allowable-Codebase` attribute identifies the locations where your signed RIA is expected to be found.

The default value for this attribute is set to "*".Provide the actual hosting location and domain in order to restrict the application from being deployed at other locations.

3. Place your `MANIFEST.MF` file back into the JAR file:

```
jar -ufm <JAR_FILE_NAME> META-INF\MANIFEST.MF
```

4. Sign the JAR file using your own certificate.

a. Optional: If you want to verify that these modifications invalidated the previous signature:

```
jarsigner -verify <JAR_FILE_NAME>
```

b. Apply your own signature to the file:

```
jarsigner -storetype  <STORE_TYPE> -tsa  <TSA_URL> <JAR_FILE_NAME>
<CERTIFICATE_ALIAS>
```

Example:

```
jarsigner -storetype pkcs12 -tsa https://timestamp.geotrust.com/tsa -
signedjar cobrowse.jar cert_alias
```

Refer *here* for more details on Jar Signing.

Tomcat Hardening

Tomcat ships with a number of web applications that are enabled by default and are not required by IC. It is highly recommended that all such non-IC applications must be removed.

Follow the steps given below to remove the OOB tomcat applications:

1. Take a backup of the `<AVAYA_IC73_HOME>\tomcat` directory at any other location, for example, `C:\tomcat_backup`.
2. Navigate to *`<AVAYA_IC73_HOME>\tomcat\webapps`* directory and delete following directories:
   - `docs`
   - `examples`
   - `host-manager`
   - `manager`
   - `ROOT`
3. The `<AVAYA_IC73_HOME>\tomcat\work` directory contains the application deployed on the server. Remove all the non-IC application deployments from the “work” directory.

Banner cloaking

To prevent version-specific attacks and banner collection, the Tomcat version may be hidden from the default error pages.
To do this, create directory `CATALINA_BASE\lib\org\apache\catalina\util` and put the `ServerInfo.properties file` in it with following content

```
server.info = AVAYA IC
server.number = 0.0.0.0
server.built =
```

"AVAYA IC" may be replaced with any desired server name to be displayed on default error pages.

Windows Server Hardening

The following lists the result of the hardening exercise for the Windows server which has IC deployed.

A summary is provided, while the detailed information is available in a different document.

91.8%

Adjusted Score: 91.8%
Original Score: 91.8%
Compliance Status: GREEN

Score

Pass:	235	Not Applicable:	0
Fail:	21	Not Checked:	0
Error:	0	Not Selected:	0
Unknown:	0	Total:	256

BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

System Information

Target:	DBICSRVWIN55
Operating System:	Windows Server 2008 R2 Standard
OS Service Pack:	Service Pack 1
Domain:	WORKGROUP
Processor:	Intel(R) Xeon(R) CPU E5405 @ 2.00GHz
Processor Architecture:	Intel64 Family 6 Model 23 Stepping 6
Processor Speed:	1995 mhz
Physical Memory:	6144 mb
Manufacturer:	VMware, Inc.
Model:	VMware Virtual Platform
Serial Number:	VMware-56 4d 2b 87 2c 3d 00 ba-12 95 49 a0 2a c9 9b 5b
BIOS Version:	6.00
Interfaces:	[00000007] Intel(R) PRO/1000 MT Network Connection • 148.147.167.8,fe80::5166:7511:e303:1586 • 00:0C:29:C9:9B:5B

Stream Information

Stream:	U_Windows_2008_R2_MS_V1R14_STIG_Benchmark
Profile:	MAC-1_Classified
Status:	accepted (2014-07-09)
Title:	Windows Server 2008 R2 Member Server Security Technical Implementation Guide
Description:	The Windows Server 2008 R2 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements were developed from DoD consensus, as well as the Windows Server 2008 R2 Security Guide and security templates published by Microsoft Corporation. Comments or proposed revisions to this guide should be sent via e-mail to the following address: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.
Notice:	Developed_by_DISA_for_the_DoD
Target Platforms:	cpe:/o:microsoft:windows_server_2008:r2
Reference:	DISA, Field Security Operations - STIG.DOD.MIL
Stream Version:	1
OVAL Version:	5.10.1
Start Time:	2014-10-31T22:28:22
End Time:	2014-10-31T22:29:38
Scanner:	cpe:/a:spawar:scc:3.1.2
Identity:	Administrator
Identity Privileged:	true
Identity Authenticated:	true
Release Info	Release: 12 Benchmark Date: 25 Jul 2014

Results

- **Unsupported Service Packs**
  Systems must be at supported service pack (SP) or release levels. - Pass
- **Display Shutdown Button**
  The shutdown option will not be available from the logon dialog box. - (CCE-10419-0) - Pass
- **NTFS Requirement**
  Local volumes will be formatted using NTFS. - Pass
- **Legal Notice Display**
  The required legal notice will be configured to display before console logon. - (CCE-10673-2) - Pass
- **Caching of logon credentials**
  Caching of logon credentials will be limited. - (CCE-10926-4) - Pass
- **Anonymous shares are not restricted**
  Anonymous enumeration of shares will be restricted. - (CCE-10557-7) - Pass
- **Bad Logon Attempts**

The number of allowed bad-logon attempts will meet minimum requirements. - (CCE-11046-0) - Fail

- **Bad Logon Counter Reset**
  The time before the bad-logon counter is reset will meet minimum requirements. - (CCE-11059-3) - Fail
- **Lockout Duration**
  The lockout duration will meet minimum requirements. - (CCE-10399-4) - Fail
- **User Right - Act as part of OS**
  Unauthorized accounts will not be granted the "Act as part of the operating system" user right. - (CCE-10232-7) - Pass
- **Maximum Password Age**
  The maximum password age will meet DoD requirements. - (CCE-10562-7) - Pass
- **Minimum Password Age**
  The minimum password age will meet requirements. - (CCE-10760-7) - Fail
- **Password Uniqueness**
  The password uniqueness will meet minimum requirements. - (CCE-10809-2) - Fail
- **Disable Guest Account**
  The built-in guest account will be disabled. - (CCE-9989-5) - Pass
- **Rename Built-in Guest Account**
  The built-in guest account will be renamed. - (CCE-10747-4) - Fail
- **Rename Built-in Administrator Account**
  The built-in administrator account will be renamed. - (CCE-10976-9) - Fail
- **Forcibly Disconnect when Logon Hours Expire**
  Users will be forcibly disconnected when their logon hours expire. - (CCE-10983-5) - Pass
- **Unencrypted Password is Sent to SMB Server.**
  Unencrypted passwords will not be sent to third-party SMB Server. - (CCE-10838-1) - Pass
- **Disable Automatic Logon**
  Automatic logons must be disabled. - (CCE-10745-8) - Pass
- **Microsoft Strong Password Filtering**
  The built-in Microsoft password complexity filter will be enabled. - (CCE-10901-7) - Pass
- **Secure Print Driver Installation**
  The print driver installation privilege will be restricted to administrators. - (CCE-9999-4) - Pass
- **LanMan Authentication Level**
  The LanMan authentication level will be set to Send NTLMv2 response only\refuse LM & NTLM. - (CCE-10984-3) - Pass
- **Ctrl+Alt+Del Security Attention Sequence**
  The Ctrl+Alt+Del security attention sequence for logons will be enabled. - (CCE-10810-0) - Pass
- **Deny Access from the Network**
  The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-10733-4) - Fail
- **Smart Card Removal Option**
  The Smart Card removal option will be configured to Force Logoff or Lock Workstation. - (CCE-10573-4) - Fail
- **Recovery Console - SET Command**
  The Recovery Console SET command will be disabled. - (CCE-10643-5) - Pass
- **Recovery Console - Automatic Logon**

The Recovery Console option will be set to prevent automatic logon to the system. - (CCE-10370-5) - Pass

- **SMB Server Packet Signing (if client agrees)**
  The Windows SMB server will perform SMB packet signing when possible. - (CCE-10978-5) - Pass
- **Encryption of Secure Channel Traffic**
  Outgoing secure channel traffic will be encrypted when possible. - (CCE-10875-3) - Pass
- **Signing of Secure Channel Traffic**
  Outgoing secure channel traffic will be signed when possible. - (CCE-10871-2) - Pass
- **Computer Account Password Reset**
  The computer account password will not be prevented from being reset. - (CCE-10775-5) - Pass
- **SMB Client Packet Signing (if server agrees)**
  The Windows SMB client will be enabled to perform SMB packet signing when possible. - (CCE-10974-4) - Pass
- **Format and Eject Removable Media**
  Ejection of removable NTFS media is not restricted to Administrators. - (CCE-10637-7) - Pass
- **Password Expiration Warning**
  Users will be warned in advance that their passwords will expire. - (CCE-10930-6) - Fail
- **Global System Objects Permission Strength**
  The default permissions of Global system objects will be increased. - (CCE-11010-6) - Pass
- **Idle Time Before Suspending a Session.**
  The amount of idle time required before suspending a session will be properly set. - (CCE-10362-2) - Pass
- **Reversible Password Encryption**
  Reversible password encryption will be disabled. - (CCE-10905-8) - Pass
- **Disable Media Autoplay**
  Autoplay will be disabled for all drives. - (CCE-11126-0) - Pass
- **Anonymous Access to Named Pipes**
  Named pipes that can be accessed anonymously will be configured to contain no values. - (CCE-10944-7) - Pass
- **Remotely Accessible Registry Paths**
  Unauthorized remotely accessible registry paths will not be configured. - (CCE-10949-6) - Pass
- **Anonymous Access to Network Shares**
  Network shares that can be accessed anonymously will not be allowed. - (CCE-10821-7) - Pass
- **Remote Assistance - Solicit Remote Assistance**
  Solicited Remote Assistance will not be allowed. - (CCE-11723-4) - Pass
- **Limit Blank Passwords**
  The use of local accounts with blank passwords will be restricted to console logons only. - (CCE-9992-9) - Pass
- **Undock Without Logging On**
  A system must be logged on to before removing from a docking station. - (CCE-10883-7) - Pass
- **Maximum Machine Account Password Age**
  The maximum age for machine account passwords will be set to requirements. - (CCE-10903-3) - Pass
- **Strong Session Key**
  The system will be configured to require a strong session key. - (CCE-10541-1) - Pass

- **Storage of Passwords and Credentials**

  The system will be configured to prevent the storage of passwords and credentials - (CCE-10292-1) - Pass
- **Everyone Anonymous rights**

  The system will be configured to prevent anonymous users from having the same rights as the Everyone group. - (CCE-10297-0) - Pass
- **Sharing and Security Model for Local Accounts**

  The system will be configured to use the Classic security model. - (CCE-10825-8) - Pass
- **LAN Manager Hash stored**

  The system will be configured to prevent the storage of the LAN Manager hash of passwords. - (CCE-10830-8) - Pass
- **Force Logoff When Logon Hours Expire**

  The system will be configured to force users to log off when their allowed logon hours expire. - (CCE-10588-2) - Pass
- **LDAP Client Signing**

  The system will be configured to the required LDAP client signing level. - (CCE-10614-6) - Pass
- **Session Security for NTLM SSP Based Clients**

  The system will be configured to meet the minimum session security requirement for NTLM SSP based clients. - (CCE-10035-4) - Pass
- **FIPS Compliant Algorithms**

  The system will be configured to use FIPS-compliant algorithms for encryption, hashing, and signing. - (CCE-10789-6) - Pass
- **Case Insensitivity for Non-Windows**

  The system will be configured to allow case insensitivity for non-Windows subsystems. - (CCE-10986-8) - Pass
- **TS/RDS - Session Limit**

  Remote Desktop Services will limit users to one remote session. - (CCE-12016-2) - Pass
- **TS/RDS - Password Prompting**

  Remote Desktop Services will always prompt a client for passwords upon connection. - (CCE-11299-5) - Pass
- **TS/RDS - Set Encryption Level**

  Remote Desktop Services will be configured with the client connection encryption set to the required level. - (CCE-11677-2) - Pass
- **TS/RDS - Do Not Use Temp Folders**

  Remote Desktop Services will be configured to use session-specific temporary folders. - (CCE-10669-0) - Pass
- **TS/RDS - Delete Temp Folders**

  Remote Desktop Services will delete temporary folders when a session is terminated. - (CCE-12046-9) - Pass
- **TS/RDS - Time Limit for Disc. Session**

  Remote Desktop Services will be configured to set a time limit for disconnected sessions. - (CCE-11117-9) - Pass
- **TS/RDS - Time Limit for Idle Session**

  Remote Desktop Services will be configured to disconnect an idle session after the specified time period. - (CCE-11506-3) - Pass
- **Group Policy - Do Not Turn off Background Refresh**

The system will be configured to enable the background refresh of Group Policy. - (CCE-14437-8) - Pass

- **Remote Assistance - Offer Remote Assistance**

  The system will be configured to prevent unsolicited remote assistance offers. - (CCE-11625-1) - Pass
- **Error Reporting - Report Errors**

  The system will be configured to prevent automatic forwarding of error information. - (CCE-11750-7) - Pass
- **Safe DLL Search Mode**

  The system will be configured to use Safe DLL Search Mode. - (CCE-10772-2) - Pass
- **Media Player - Disable Automatic Updates**

  Media Player must be configured to prevent automatic checking for updates. - (CCE-11298-7) - Pass
- **Session Security for NTLM SSP based Servers**

  The system will be configured to meet the minimum session security requirement for NTLM SSP based servers. - (CCE-10040-4) - Pass
- **Audit Log Warning Level**

  The system will generate an audit event when the audit log reaches a percent full threshold. - (CCE-11011-4) - Pass
- **Disable IP Source Routing**

  The system will be configured to prevent IP source routing. - (CCE-10732-6) - Pass
- **Disable ICMP Redirect**

  The system will be configured to prevent ICMP redirects from overriding OSPF generated routes. - (CCE-10518-9) - Pass
- **Disable Router Discovery**

  The system will be configured to disable the Internet Router Discover Protocol (IRDP). - (CCE-10768-0) - Pass
- **TCP Connection Keep-Alive Time**

  The system will be configured to limit how often keep-alive packets are sent. - (CCE-10381-2) - Pass
- **Name-Release Attacks**

  The system will be configured to ignore NetBIOS name release requests except from WINS servers. - (CCE-10653-4) - Pass
- **TCP Data Retransmissions**

  The system will limit how many times unacknowledged TCP data is retransmitted. - (CCE-10941-3) - Pass
- **Screen Saver Grace Period**

  The system will be configured to have password protection take effect within a limited time frame when the screen saver becomes active. - (CCE-10019-8) - Pass
- **Remotely Accessible Registry Paths and Sub-Paths**

  Unauthorized remotely accessible registry paths and sub-paths will not be configured. - (CCE-10935-5) - Pass
- **Strong Key Protection**

  Users will be required to enter a password to access private keys. - (CCE-11035-3) - Pass
- **Optional Subsystems**

  Optional Subsystems will not be permitted to operate on the system. - (CCE-10913-2) - Pass
- **Software Restriction Policies**

  Software certificate restriction policies will be enforced. - (CCE-10900-9) - Pass
- **TS/RDS - Secure RPC Connection.**

The Remote Desktop Session Host will require secure RPC communications. - (CCE-11368-8) - Pass

- **Group Policy - Registry Policy Processing**
  Group Policy objects will be reprocessed even if they have not changed. - (CCE-12754-8) - Pass
- **Encrypting and Signing of Secure Channel Traffic**
  Outgoing secure channel traffic will be encrypted or signed. - (CCE-10871-2) - Pass
- **SMB Client Packet Signing (Always)**
  The Windows SMB client will be enabled to always perform SMB packet signing. - (CCE-10970-2) - Pass
- **SMB Server Packet Signing (Always)**
  The Windows SMB server will be enabled to always perform SMB packet signing. - (CCE-10992-6) - Pass
- **Anonymous Access to Named Pipes and Shares**
  Anonymous access to Named Pipes and Shares will be restricted. - (CCE-10940-5) - Pass
- **Minimum Password Length**
  For systems utilizing a logon ID as the individual identifier, passwords will, at a minimum, be 14 characters. - (CCE-10372-1) - Fail
- **Display of Last User Name**
  The system will be configured to prevent the display of the last user name on the logon screen. - (CCE-10788-8) - Pass
- **Audit Access of Global System Objects**
  Auditing Access of Global System Objects must be turned off. - (CCE-10487-7) - Pass
- **Audit Backup and Restore Privileges**
  Audit of Backup and Restore Privileges will be turned off. - (CCE-10619-5) - Pass
- **Audit Policy Subcategory Setting**
  Audit policy using subcategories will be enabled. - (CCE-10112-1) - Pass
- **IPSec Exemptions**
  IPSec Exemptions will be limited. - (CCE-10018-0) - Pass
- **UAC - Admin Approval Mode**
  User Account Control approval mode for the built-in Administrator will be enabled. - (CCE-11028-8) - Pass
- **UAC - Admin Elevation Prompt**
  User Account Control will, at minimum, prompt administrators for consent. - (CCE-11023-9) - Pass
- **UAC - User Elevation Prompt**
  User Account Control will automatically deny standard user requests for elevation. - (CCE-10807-6) - Pass
- **UAC - Application Installations**
  User Account Control will be configured to detect application installations and prompt for elevation. - (CCE-10794-6) - Pass
- **UAC - UIAccess Application Elevation**
  User Account Control will only elevate UIAccess applications that are installed in secure locations - (CCE-10570-0) - Pass
- **UAC - All Admin Approval Mode**
  User Account Control will run all administrators in Admin Approval Mode, enabling UAC. - (CCE-10684-9) - Pass
- **UAC - Secure Desktop Mode**

User Account Control will switch to the secure desktop when prompting for elevation. - (CCE-10109-7) - Pass

- **UAC - Non UAC Compliant Application Virtualization**

  User Account Control will virtualize file and registry write failures to per-user locations. - (CCE-10865-4) - Pass
- **Enumerate Administrator Accounts on Elevation**

  The system will require username and password to elevate a running application. - (CCE-11450-4) - Pass
- **TS/RDS - Prevent Password Saving**

  Passwords will not be saved in the Remote Desktop Client. - (CCE-11905-7) - Pass
- **TS/RDS - Drive Redirection**

  Local drives will be prevented from sharing with Remote Desktop Session Hosts (Remote Desktop Services Role). - (CCE-11709-3) - Pass
- **RPC - Unauthenticated RPC Clients**

  Unauthenticated RPC clients will be restricted from connecting to the RPC server. - (CCE-10881-1) - Pass
- **RPC - Endpoint Mapper Authentication**

  Client computers will be required to authenticate for RPC communication. - (CCE-10715-1) - Pass
- **Internet Download / Online Ordering**

  Web publishing and online ordering wizards will be prevented from downloading a list of providers. - (CCE-11136-9) - Pass
- **Printing Over HTTP**

  Printing over HTTP will be prevented. - (CCE-11360-5) - Pass
- **HTTP Printer Drivers**

  Downloading print driver packages over HTTP will be prevented. - (CCE-11563-4) - Pass
- **Windows Update Device Drive Searching**

  Windows will be prevented from using Windows Update to search for drivers. - (CCE-10357-2) - Pass
- **IPv6 Transition**

  IPv6 will be disabled until a deliberate transition strategy has been implemented. - Fail
- **Windows Peer to Peer Networking**

  Windows Peer-to-Peer networking services will be turned off. - (CCE-11604-6) - Pass
- **Prohibit Network Bridge**

  Network Bridges will be prohibited in Windows. - (CCE-12074-1) - Pass
- **Root Certificates Update**

  Root Certificates will not be updated automatically from the Microsoft site. - (CCE-11264-9) - Pass
- **Event Viewer Events.asp Links**

  Event Viewer Events.asp links will be turned off. - (CCE-10693-0) - Pass
- **Internet File Association Service**

  The Internet File Association service will be turned off. - (CCE-10697-1) - Pass
- **Order Prints Online**

  The Order Prints Online wizard will be turned off. - (CCE-11243-3) - Pass
- **Classic Logon**

  The classic logon screen will be required for user logons. - (CCE-11256-5) - Pass
- **RSS Attachment Downloads**

  Attachments will be prevented from being downloaded from RSS feeds. - Pass

- **Windows Explorer – Shell Protocol Protected Mode**
  Windows Explorer shell protocol will run in protected mode. - (CCE-11530-3) - Pass
- **Windows Installer – IE Security Prompt**
  Users will be notified if a web-based program attempts to install software. - (CCE-10343-2) - Pass
- **Windows Installer – User Control**
  Users will be prevented from changing installation options. - (CCE-10906-6) - Pass
- **Windows Installer – Vendor Signed Updates**
  Non-administrators will be prevented from applying vendor signed updates. - (CCE-11468-6) - Pass
- **Media Player – First Use Dialog Boxes**
  Users will not be presented with Privacy and Installation options on first use of Windows Media Player. - (CCE-11596-4) - Pass
- **Network – Mapper I/O Driver**
  The Mapper I/O network protocol driver will be disabled. - (CCE-10484-4) - Pass
- **Network – Responder Driver**
  The Responder network protocol driver will be disabled. - (CCE-11304-3) - Pass
- **Network – WCN Wireless Configuration**
  The configuration of wireless devices using Windows Connect Now will be disabled. - (CCE-11242-5) - Pass
- **Network – Windows Connect Now Wizards**
  The Windows Connect Now wizards will be disabled. - (CCE-11155-9) - Pass
- **Device Install – PnP Interface Remote Access**
  Remote access to the Plug and Play interface will be disabled for device installation. - (CCE-11248-2) - Pass
- **Device Install – Drivers System Restore Point**
  A system restore point will be created when a new device driver is installed. - (CCE-10546-0) - Pass
- **Device Install – Generic Driver Error Report**
  An Error Report will not be sent when a generic device driver is installed. - (CCE-12274-7) - Pass
- **Driver Install – Device Driver Search Prompt**
  Users will not be prompted to search Windows Update for device drivers. - (CCE-11319-1) - Pass
- **Handwriting Recognition Error Reporting**
  Errors in handwriting recognition on Tablet PCs will not be reported to Microsoft. - (CCE-11030-4) - Pass
- **Power Mgmt – Password Wake on Battery**
  Users will be prompted for a password on resume from sleep (on battery). (Applicable to Server 2008 R2 if the system is configured to sleep.) - (CCE-12088-1) - Pass
- **Power Mgmt – Password Wake When Plugged In**
  The user will be prompted for a password on resume from sleep (Plugged In). (Applicable on Server 2008 R2 if the system is configured to sleep.) - (CCE-11651-7) - Pass
- **Remote Assistance – Session Logging**
  Remote Assistance log files will be generated. - (CCE-11263-1) - Pass
- **Game Explorer Information Downloads**
  Game explorer information will not be downloaded from Windows Metadata Services. - (CCE-11739-0) - Pass
- **Defender – SpyNet Reporting**
  Windows Defender SpyNet membership will be disabled. - (CCE-11638-4) - Pass

- **Error Reporting – Logging**
  Error Reporting events will be logged in the system event log. - (CCE-11621-0) - Pass
- **Error Reporting – Windows Error Reporting**
  Windows Error Reporting to Microsoft will be disabled. - (CCE-11708-5) - Pass
- **Error Reporting – Additional Data**
  Additional data requests in response to Error Reporting will be declined. - (CCE-11584-0) - Pass
- **Windows Explorer – Heap Termination**
  Windows Explorer heap termination on corruption will be disabled. - (CCE-10981-9) - Pass
- **Logon – Report Logon Server**
  Users will be notified if the logon server was inaccessible and cached credentials were used. - (CCE-12260-6) - Pass
- **Media DRM – Internet Access**
  Windows Media Digital Rights Management will be prevented from accessing the Internet. - (CCE-11052-8) - Pass
- **Software Certificate Installation Files**
  Software certificate installation files will be removed from a system. - Fail
- **UAC - UIAccess Secure Desktop**
  UIAccess applications will not be allowed to prompt for elevation without using the secure desktop. - (CCE-10534-6) - Pass
- **TS/RDS – COM Port Redirection**
  The system will be configured to prevent users from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role) - (CCE-10600-5) - Pass
- **TS/RDS – LPT Port Redirection**
  The system will be configured to prevent users from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role) - (CCE-11623-6) - Pass
- **TS/RDS - PNP Device Redirection**
  The system will be configured to prevent users from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role) - (CCE-11128-6) - Pass
- **TS/RDS – Smart Card Device Redirection**
  The system will be configured to ensure smart card devices can be redirected to the Remote Desktop Session. (Remote Desktop Services Role) - (CCE-11517-0) - Pass
- **TS/RDS – Printer Redirection**
  The system will be configured to allow only the default client printer to be redirected in the Remote Desktop session. (Remote Desktop Services Role) - (CCE-10977-7) - Pass
- **TS/RDS – Remove Disconnect Option**
  The system will be configured to remove the Disconnect option from the Shut Down Windows dialog box on the Remote Desktop Client. (Remote Desktop Services Role) - (CCE-11997-4) - Pass
- **UAC - Application Elevations**
  Windows will elevate all applications in User Account Control, not just signed ones. - (CCE-10922-3) - Pass
- **Windows Customer Experience Improvement Program**
  The Windows Customer Experience Improvement Program will be disabled. - (CCE-11354-8) - Pass
- **User Right - Debug Programs**
  Unauthorized accounts must not have the Debug programs user right. - (CCE-10915-7) - Pass
- **SPN Target Name Validation Level**

The service principal name (SPN) target name validation level will be turned off. - (CCE-10617-9) - Pass

- **Computer Identity Authentication for NTLM**

  Services using Local System that use negotiate when reverting to NTLM authentication will use the computer identity vs. authenticating anonymously. - (CCE-10817-5) - Pass
- **NTLM NULL Session Fallback**

  NTLM will be prevented from falling back to a Null session. - (CCE-10812-6) - Pass
- **PKU2U Online Identities Authentication**

  PKU2U authentication using online identities will be prevented. - (CCE-10839-9) - Pass
- **Kerberos Encryption Types**

  Kerberos encryption types will be configured to prevent the use of DES encryption suites. - (CCE-10843-1) - Pass
- **IPv6 Source Routing**

  IPv6 source routing will be configured to highest protection. - (CCE-10888-6) - Pass
- **IPv6 TCP Data Retransmissions**

  IPv6 TCP data retransmissions will be configured to prevent resources from becoming exhausted. - (CCE-10804-3) - Pass
- **Elevate when setting a network's location**

  Domain users will be required to elevate when setting a network's location. - (CCE-11610-3) - Pass
- **Direct Access – Route Through Internal Network**

  All Direct Access traffic will be routed through the internal network. - (CCE-11300-1) - Pass
- **Windows Update Point and Print Driver Search**

  Windows Update will be prevented from searching for point and print drivers. - (CCE-11976-8) - Pass
- **Prevent device metadata retrieval from Internet**

  Device metadata retrieval from the Internet will be prevented. - (CCE-11589-9) - Pass
- **Prevent Windows Update for device driver search**

  Device driver searches using Windows Update will be prevented. - (CCE-11787-9) - Pass
- **MSDT Interactive Communication**

  Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft will be prevented. - (CCE-10855-5) - Pass
- **Windows Online Troubleshooting Service**

  Access to Windows Online Troubleshooting Service (WOTS) will be prevented. - (CCE-11161-7) - Pass
- **Disable PerfTrack**

  Responsiveness events will be prevented from being aggregated and sent to Microsoft. - (CCE-11889-3) - Pass
- **Application Compatibility Program Inventory**

  The Application Compatibility Program Inventory will be prevented from collecting data and sending the information to Microsoft. - (CCE-11043-7) - Pass
- **Autoplay for non-volume devices**

  Autoplay will be turned off for non-volume devices. - (CCE-11375-3) - Pass
- **Turn Off Game Updates**

  Downloading of game update information will be turned off. - (CCE-11807-5) - Pass
- **Prevent Joining Homegroup**

  The system will be prevented from joining a homegroup. - (CCE-10691-4) - Pass

- **Windows Anytime Upgrade**
  Windows Anytime Upgrade will be disabled. - (CCE-10544-5) - Pass
- **Explorer Data Execution Prevention**
  Explorer Data Execution Prevention will be enabled. - (CCE-12161-6) - Pass
- **Default Autorun Behavior**
  The default autorun behavior will be configured to prevent autorun commands. - (CCE-11431-4) - Pass
- **Restrict Anonymous SAM Enumeration**
  Anonymous enumeration of SAM accounts will not be allowed. - (CCE-10027-1) - Pass
- **Legal Banner Dialog Box Title**
  The Windows dialog box title for the legal banner will be configured. - (CCE-10010-7) - Fail
- **Access this computer from the network**
  Unauthorized accounts will not have the "Access this computer from the network" user right. - (CCE-10086-7) - Pass
- **Adjust memory quotas for a process**
  Unauthorized accounts will not have the "Adjust memory quotas for a process" user right. - (CCE-10849-8) - Pass
- **Allow log on locally**
  Unauthorized accounts will not have the "Allow log on locally" user right. - (CCE-10853-0) - Pass
- **Allow log on through Remote Desktop Services**
  Unauthorized accounts will not have the "Allow log on through Remote Desktop Services" user right. - (CCE-10858-9) - Pass
- **Back up files and directories**
  Unauthorized accounts will not have the "Back up files and directories" user right. - (CCE-10880-3) - Pass
- **Bypass traverse checking**
  Unauthorized accounts will not have the "Bypass traverse checking" user right. - (CCE-10369-7) - Pass
- **Change the system time**
  Unauthorized accounts will not have the "Change the system time" user right. - (CCE-10122-0) - Pass
- **Change the time zone**
  Unauthorized accounts will not have the "Change the time zone" user right. - (CCE-10897-7) - Pass
- **Create a pagefile**
  Unauthorized accounts will not have the "Create a pagefile" user right. - (CCE-9937-4) - Pass
- **Create a token object**
  Unauthorized accounts will not have the "Create a token object" user right. - (CCE-10770-6) - Pass
- **Create global objects**
  Unauthorized accounts will not have the "Create global objects" user right. - (CCE-10792-0) - Pass
- **Create permanent shared objects**
  Unauthorized accounts will not have the "Create permanent shared objects" user right. - (CCE-10796-1) - Pass
- **Create symbolic links**
  Unauthorized accounts will not have the "Create symbolic links" user right. - (CCE-10911-6) - Pass
- **Deny log on as a batch job**

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems. - (CCE-10596-5) - Fail

- **Deny log on as a service**

  The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. - (CCE-10226-9) - Fail

- **Deny log on locally**

  The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems. - (CCE-10750-8) - Fail

- **Deny log on through Remote Desktop \ Terminal Services**

  The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-10878-7) - Fail

- **Enable accounts to be trusted for delegation**

  Unauthorized accounts will not have the "Enable computer and user accounts to be trusted for delegation" user right. - (CCE-10618-7) - Pass

- **Force shutdown from a remote system**

  Unauthorized accounts will not have the "Force shutdown from a remote system" user right. - (CCE-10785-4) - Pass

- **Generate security audits**

  Unauthorized accounts will not have the "Generate security audits" user right. - (CCE-10274-9) - Pass

- **Impersonate a client after authentication**

  Unauthorized accounts will not have the "Impersonate a client after authentication" user right. - (CCE-9946-5) - Pass

- **Increase a process working set**

  Unauthorized accounts will not have the "Increase a process working set" user right. - (CCE-10548-6) - Fail

- **Increase scheduling priority**

  Unauthorized accounts will not have the "Increase scheduling priority" user right. - (CCE-9961-4) - Pass

- **Load and unload device drivers**

  Unauthorized accounts will not have the "Load and unload device drivers" user right. - (CCE-10202-0) - Pass

- **Lock pages in memory**

  Unauthorized accounts will not have the "Lock pages in memory" user right. - (CCE-10955-3) - Pass

- **Log on as a batch job**

  Unauthorized accounts will not have the "Log on as a batch job" user right. - (CCE-10549-4) - Pass

- **Modify an object label**

  Unauthorized accounts will not have the "Modify an object label" user right. - (CCE-10567-6) - Pass

- **Modify firmware environment values**

  Unauthorized accounts will not have the "Modify firmware environment values" user right. - (CCE-10659-1) - Pass

- **Perform volume maintenance tasks**

  Unauthorized accounts will not have the "Perform volume maintenance tasks" user right. - (CCE-9984-6) - Pass

- **Profile single process**

Unauthorized accounts will not have the "Profile single process" user right. - (CCE-10458-8) - Pass

- **Profile system performance**

  Unauthorized accounts will not have the "Profile system performance" user right. - (CCE-10193-1) - Pass
- **Remove computer from docking station**

  Unauthorized accounts will not have the "Remove computer from docking station" user right. - (CCE-10969-4) - Pass
- **Replace a process level token**

  Unauthorized accounts will not have the "Replace a process level token" user right. - (CCE-10599-9) - Pass
- **Restore files and directories**

  Unauthorized accounts will not have the "Restore files and directories" user right. - (CCE-10805-0) - Pass
- **Shut down the system**

  Unauthorized accounts will not have the "Shut down the system" user right. - (CCE-10439-8) - Pass
- **Take ownership of files or other objects**

  Unauthorized accounts will not have the "Take ownership of files or other objects" user right. - (CCE-10954-6) - Pass
- **Audit - Credential Validation - Success**

  The system will be configured to audit "Account Logon -> Credential Validation" successes. - Pass
- **Audit - Credential Validation - Failure**

  The system will be configured to audit "Account Logon -> Credential Validation" failures. - Pass
- **Audit - Computer Account Management - Success**

  The system will be configured to audit "Account Management -> Computer Account Management" successes. - Pass
- **Audit - Computer Account Management - Failure**

  The system will be configured to audit "Account Management -> Computer Account Management" failures. - Pass
- **Audit - Other Account Management Events - Success**

  The system will be configured to audit "Account Management -> Other Account Management Events" successes. - Pass
- **Audit - Other Account Management Events - Failure**

  The system will be configured to audit "Account Management -> Other Account Management Events" failures. - Pass
- **Audit - Security Group Management - Success**

  The system will be configured to audit "Account Management -> Security Group Management" successes. - Pass
- **Audit - Security Group Management - Failure**

  The system will be configured to audit "Account Management -> Security Group Management" failures. - Pass
- **Audit - User Account Management - Success**

  The system will be configured to audit "Account Management -> User Account Management" successes. - Pass
- **Audit - User Account Management - Failure**

  The system will be configured to audit "Account Management -> User Account Management" failures. - Pass
- **Audit - Process Creation - Success**

The system will be configured to audit "Detailed Tracking -> Process Creation" successes. - Pass

- **Audit - Logoff - Success**
  The system will be configured to audit "Logon/Logoff -> Logoff" successes. - Pass
- **Audit - Logon - Success**
  The system will be configured to audit "Logon/Logoff -> Logon" successes. - Pass
- **Audit - Logon - Failure**
  The system will be configured to audit "Logon/Logoff -> Logon" failures. - Pass
- **Audit - Special Logon - Success**
  The system will be configured to audit "Logon/Logoff -> Special Logon" successes. - Pass
- **Audit - File System - Failure**
  The system will be configured to audit "Object Access -> File System" failures. - Pass
- **Audit - Registry - Failure**
  The system will be configured to audit "Object Access -> Registry" failures. - Pass
- **Audit - Audit Policy Change - Success**
  The system will be configured to audit "Policy Change -> Audit Policy Change" successes. - Pass
- **Audit - Audit Policy Change - Failure**
  The system will be configured to audit "Policy Change -> Audit Policy Change" failures. - Pass
- **Audit - Authentication Policy Change - Success**
  The system will be configured to audit "Policy Change -> Authentication Policy Change" successes. - Pass
- **Audit - Sensitive Privilege Use - Success**
  The system will be configured to audit "Privilege Use -> Sensitive Privilege Use" successes. - Pass
- **Audit - Sensitive Privilege Use - Failure**
  The system will be configured to audit "Privilege Use -> Sensitive Privilege Use" failures. - Pass
- **Audit - IPSec Driver - Success**
  The system will be configured to audit "System -> IPSec Driver" successes. - Pass
- **Audit - IPSec Driver - Failure**
  The system will be configured to audit "System -> IPSec Driver" failures. - Pass
- **Audit - Security State Change - Success**
  The system will be configured to audit "System -> Security State Change" successes. - Pass
- **Audit - Security State Change - Failure**
  The system will be configured to audit "System -> Security State Change" failures. - Pass
- **Audit - Security System Extension - Success**
  The system will be configured to audit "System -> Security System Extension" successes. - Pass
- **Audit - Security System Extension - Failure**
  The system will be configured to audit "System -> Security System Extension" failures. - Pass
- **Audit - System Integrity - Success**
  The system will be configured to audit "System -> System Integrity" successes. - Pass
- **Audit - System Integrity - Failure**
  The system will be configured to audit "System -> System Integrity" failures. - Pass
- **6to4 State**
  The 6to4 IPv6 transition technology will be disabled. - (CCE-11356-3) - Pass
- **IP-HTTPS State**
  The IP-HTTPS IPv6 transition technology will be disabled. - (CCE-10832-4) - Pass

- **ISATAP State**
  The ISATAP IPv6 transition technology will be disabled. - (CCE-11141-9) - Pass
- **Teredo State**
  The Teredo IPv6 transition technology will be disabled. - (CCE-11865-3) - Pass
- **Maximum Log Size - Application**
  The Application event log will be configured to a minimum size requirement. - (CCE-11143-5) - Pass
- **Maximum Log Size - Security**
  The Security event log will be configured to a minimum size requirement. - (CCE-11033-8) - Pass
- **Maximum Log Size - Setup**
  The Setup event log will be configured to a minimum size requirement. - (CCE-11717-6) - Pass
- **Maximum Log Size - System**
  The System event log will be configured to a minimum size requirement. - (CCE-11174-0) - Pass
- **Device Install Software Request Error Report**
  Windows will be prevented from sending an error report when a device driver requests additional software during installation. - (CCE-11336-5) - Pass
- **Always Install with Elevated Privileges Disabled**
  The Windows Installer Always install with elevated privileges must be disabled. - (CCE-12401-6) - Pass
- **Local admin accounts filtered token policy enabled on domain systems.**
  Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems. - Fail
- **WINGE-000200**
  A group named DenyNetworkAccess must be defined on domain systems to include all local administrator accounts. - Fail

Internet Explorer Hardening

The following lists the Internet Explorer 9 hardening results.

Score

94.49%

Adjusted Score: 94.49%
Original Score: 94.49%
Compliance Status: GREEN

Pass:	120	Not Applicable:	0
Fail:	7	Not Checked:	0
Error:	0	Not Selected:	0
Unknown:	0	Total:	127

BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

System Information

Target:	DBICSRVWIN55
Operating System:	Windows Server 2008 R2 Standard
OS Service Pack:	Service Pack 1
Domain:	WORKGROUP
Processor:	Intel(R) Xeon(R) CPU E5405 @ 2.00GHz
Processor Architecture:	Intel64 Family 6 Model 23 Stepping 6
Processor Speed:	1995 mhz
Physical Memory:	6144 mb
Manufacturer:	VMware, Inc.
Model:	VMware Virtual Platform
Serial Number:	VMware-56 4d 2b 87 2c 3d 00 ba-12 95 49 a0 2a c9 9b 5b
BIOS Version:	6.00
Interfaces:	[00000007] Intel(R) PRO/1000 MT Network Connection • 148.147.167.8,fe80::5166:7511:e303:1586 • 00:0C:29:C9:9B:5B

Stream Information

Stream:	U_Microsoft_IE9_V1R5_STIG_Benchmark
Profile:	MAC-1_Classified
Status:	accepted (2014-01-08)
Title:	Internet Explorer 9 Security Technical Implementation Guide
Description:	The Internet Explorer 9 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. Comments or proposed revisions to this guide should be sent via e-mail to the following address: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.
Notice:	

Target Platforms:	cpe:/a:microsoft:ie:9
Reference:	DISA, Field Security Operations - STIG.DOD.MIL
Stream Version:	1
OVAL Version:	5.10.1
Start Time:	2015-03-25T01:20:56
End Time:	2015-03-25T01:21:05
Scanner:	cpe:/a:spawar:scc:3.1.2
Identity:	Administrator
Identity Privileged:	true
Identity Authenticated:	true
Release Info	Release: 7 Benchmark Date: 24 Jan 2014

Results

- **DTBI320 - Security zone machine settings**
- **DTBI319 - Changing of policies**
- **DTBI318 - Addition and deletion of sites**
- **DTBI367 - Proxy settings**
- **DTBI022 - Download signed ActiveX - Internet**
- **DTBI023 - Download unsigned ActiveX - Internet**
- **DTBI024 - Initialize and script ActiveX - Internet**
- **DTBI030-Font download control - Internet Zone**
- **DTBI031 - Java Permission - Internet**
- **DTBI032 - Data sources across domains - Internet**
- **DTBI036-Drag and drop or copy and paste-Internet**
- **DTBI038 - Programs and files in IFRAME - Internet**
- **DTBI039 - Navigating across domains - Internet**
- **DTBI042-Userdata persistence - Internet Zone**
- **DTBI044 - Paste operations via script - Internet**
- **DTBI046-User Authentication-Logon - Internet Zone**
- **DTBI061 - Java Permission - Intranet Zone**
- **DTBI091- Java Permission - Trusted**
- **DTBI112-Download signed ActiveX - Restricted Sites**
- **DTBI113 - Download unsigned ActiveX - Restricted**
- **DTBI114 - Initialize and script ActiveX-Restricted**
- **DTBI115 - ActiveX control and plugins - Restricted**
- **DTBI116 - ActiveX control marked safe - Restricted**
- **DTBI119-File download control - Restricted Sites**
- **DTBI120-Font download control - Restricted Sites**
- **DTBI122-Access data sources - Restricted Sites**
- **DTBI123 - META REFRESH - Restricted Sites**
- **DTBI126-Drag and drop or copy and paste-Restricted**

- **DTBI127-Installation of desktop items - Restricted**
- **DTBI128 - Programs and files in IFRAME-Restricted**
- **DTBI129 - Navigating across domains - Restricted**
- **DTBI132-Userdata persistence - Restricted Sites**
- **DTBI133-Active scripting - Restricted Sites**
- **DTBI134 - Paste operations via script - Restricted**
- **DTBI136-User Authentication - Logon - Restricted**
- **DTBI121 - Java Permission - Restricted**
- **DTBI697 - IE - Users enable or disable add-ons**
- **DTBI305-Automatic configuration is not disabled**
- **DTBI315 - Customer Experience Improvement Pgm**
- **DTBI325 - Security settings check feature**
- **DTBI340 - Active content from CD's**
- **DTBI350 - Software with invalid signatures**
- **DTBI355 - Third-party browser extensions**
- **DTBI365 - Check for server certificate revocation**
- **DTBI370 - Signature checking - downloaded programs**
- **DTBI375 - Network paths (UNC's) - Intranet**
- **DTBI385 - Script initiated windows - Internet**
- **DTBI390 - Script initiated windows - Restricted**
- **DTBI395 - Scriptlets - Internet**
- **DTBI415 - Prompt for file downloads - Internet**
- **DTBI425 - Java permission - Local Machine**
- **DTBI430 - Java permission - Locked Down Machine**
- **DTBI435 - Java permission - Locked Down Intranet**
- **DTBI440 - Java permission - Locked Down Trusted**
- **DTBI445 - Java permission - Locked Down Internet**
- **DTBI450 - Java permission - Locked Down Restricted**
- **DTBI455 - Loose XAML files - Internet**
  Loose XAML files must be disallowed (Internet zone). - Fail
- **DTBI460 - Loose XAML files - Restricted**
  Loose XAML files must be disallowed (Restricted Sites zone). - Fail
- **DTBI465 - MIME sniffing - Internet**
- **DTBI470 - MIME sniffing - Restricted**
- **DTBI475 - First-Run Opt-In - Internet**
  First-Run Opt-In ability must be disallowed (Internet zone). - Fail
- **DTBI480 - First-Run Opt-In - Restricted**
- **DTBI485 - Protected Mode - Internet**
- **DTBI490 - Protected Mode - Restricted**
- **DTBI495 - Pop-up Blocker - Internet**
- **DTBI500 - Pop-up Blocker - Restricted**
- **DTBI515 - Less privileged web content - Internet**

Web sites in less privileged web content zones must be disallowed to navigate into the Internet zone. - Fail

- **DTBI520 - Less privileged web content - Restricted**
- **DTBI575 - Binary and script behaviors - Restricted**
- **DTBI580 - Prompt for file downloads - Restricted**
- **DTBI590 - MIME handling - Reserved**
- **DTBI595 - MIME sniffing - Reserved**
- **DTBI600 - MK Protocol - Explorer**
- **DTBI605 - MK Protocol - IExplore**
- **DTBI610 - Zone elevation - Reserved**
- **DTBI630 - File download processes - Reserved**
- **DTBI635 - File download processes - Explorer**
- **DTBI640 - File download processes - IExplore**
- **DTBI645 - Restricting Pop Up Windows - Reserved**
- **DTBI650 - .NET w/Authenticode unsigned-Restricted**
- **DTBI655 - .NET w/Authenticode signed - Restricted**
- **DTBI670 - Scripting of Java applets - Restricted**
- **DTBI675 - Displaying URL's for update checking**
- **DTBI680 - Update check interval**
- **DTBI592 - MIME handling - Explorer**
- **DTBI594 - MIME handling - IExplore**
- **DTBI599 - MK Protocol - Reserved**
- **DTBI612 - Zone Elevation - Explorer**
- **DTBI614 - Zone elevation - IExplore**
- **DTBI647 - Internet Explorer Processes for restrict**
- **DTBI649 - Restricting Pop Up windows - IExplore**
- **DTBI715 - Crash Detection**
- **DTBI596 - MIME sniffing - Explorer**
- **DTBI597 - MIME sniffing - IExplore**
- **Prevent performance of First Run Customize setting**
- **DTBI300 - Configuring History lists**
- **DTBI740 - Managing SmartScreen Filter**

  Managing SmartScreen Filter use must be enforced. - Fail
- **DTBI750 - Microsoft web site list updates**
- **DTBI760 - Browsing History on exit**
- **DTBI770 - Web site visit history**
- **DTBI780 - InPrivate Browsing**
- **DTBI800 - Browser scripting control - Internet**
- **DTBI810 - Local directory paths - Internet**
- **DTBI820 - Programs and unsafe files – Internet**

  Launching programs and unsafe files property must be set to prompt (Internet zone). - Fail
- **DTBI830 - ActiveX controls no prompt - Internet**
- **DTBI840 - Cross-Site Scripting Filter - Internet**

- **DTBI850 - Browser scripting control - Restricted**
- **DTBI860 - Local directory paths - Restricted**
- **DTBI870 - Programs and unsafe files - Restricted**
  Launching programs and unsafe files property must be set to prompt (Restricted Site zone). - Fail
- **DTBI880 - ActiveX controls no prompt - Restricted**
- **DTBI890 - Cross-Site Scripting Filter - Restricted**
- **DTBI900 - Restrict ActiveX Install - Reserved**
- **DTBI910 - Status bar updates via script - Internet**
- **DTBI920 - .NET w/Authenticode unsigned - Internet**
- **DTBI930 - .NET w/Authenticode signed - Internet**
- **DTBI940 - Scriptlets - Restricted**
- **DTBI950 - Status bar update by script - Restricted**
- **DTBI1010 - Restrict ActiveX Install - Explorer**
- **DTBI1020 - Restrict ActiveX Install - IExplore**
- **DTBI745 - Add-On Performance Notifications**
- **DTBI755 - Browser Geolocation Functionality**
- **DTBI765 - Suggested Sites Functionality**
- **DTBI775 - Internet Explorer Update Checking**
- **DTBI805 - Opt-In Prompts for ActiveX**
- **DTBI815 - Notification Bar Process - Reserved**
- **DTBI825 - Notification Bar Processes - Explorer**
- **DTBI835 - Notification Bar Processes - IExplore**

Appendix A: Network services on IC servers

The following is a list of ports used by Avaya IC:

- **Source Initiator:** The device or application initiating a data flow.
- **Source Ports:** This is the default port(s) used by the source device or application. Valid values include: 0 – 65535.
- **Destination Receiver:** The device or application receiving a data flow from a source.
- **Destination Ports:** This is the default port(s) used at the device or application responding to an initiator. Valid values include: 0 – 65535.
- **Network / Application Protocol:** Labels of the network and application protocols used.
- **Destination Configurable:** “Yes” means the destination port is configurable. “No” means the destination port is not configurable. Valid values include: Yes or No.
- **Range** If populated, this field lists the range of ports that can be used by the destination. The range may or may not be configurable. Valid values include: 0 – 65535.
- **Source Configurable:** “Yes” means the source port is configurable. “No” means the source port is not configurable. Valid values include: Yes or No
- **Range:** If populated, this field lists the range of ports that can be used by the source. The range may or may not be configurable. Valid values include: 0 – 65535.
- **Default Port State:** A port is open, closed, or filtered.

  Open ports will respond to queries.

  Closed ports may or may not respond to queries and are only listed when they can be optionally enabled.

  Filtered ports can be open or closed. Filtered UDP ports will not respond to queries. Filtered TCP will respond to queries, but will not allow connectivity.
- **Traffic Purpose:** Describes the purpose of the data flow.
- **Comments:** Important comments.

	Source		Destination		Network/ Application Protocol	Destination Configurable? Range	Source Configurable? Range	Default Port state (Destination)	Traffic Purpose (Comments)
	Initiator	Port(s)	Receiver	Ports					
1.	Client Desktop (Qui)/JAB [1]	Ephemeral	ORB	9001	TCP	Yes 1024 - 65535	No	Open	Send server management requests.
2.	Client Softphone (VTel)	Ephemeral	ORB	9001	TCP	Yes 1024 - 65535	No	Open	Send server management requests.
3.	Client Desktop (Qui) /JAB	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login and configuration related data
4.	Client Softphone (VTel)	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login and configuration related data
5.	Client Desktop (Qui) /JAB	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
6.	Client Desktop (Qui)	Ephemeral	Http Connector	9170	TCP	Yes 1024 - 65535	No	Open	HTTP data
7.	Client Desktop (Qui) /JAB	Ephemeral	Blender	90xx	TCP	Yes 1024 - 65535	No	Open	Controls agent state and load
8.	Client Softphone (VTel) /JAB	Ephemeral	Telephony server	90xx	TCP	Yes 1024 - 65535	No	Open	Telephony state changes
9.	Client Softphone (VTel) /JAB	Ephemeral	EDU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Contact related data
10.	Client Desktop (Qui) /JAB	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Agent related statistical data
11.	Client Softphone (VTel)	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Agent related statistical data
12.	Client Desktop (Qui) /JAB	Ephemeral	Paging Server	90xx	TCP	Yes 1024 - 65535	No	Open	Events related to Paging server

[1] JAB: Java Application Bridge is the common server interface for SDK and AAWC.

	Source		Destination		Network/ Application Protocol	Destination Configurable ? Range	Source Configurable ? Range	Default Port state (Destination)	Traffic Purpose (Comments)
	Initiator	Port(s)	Receiver	Ports					
13.	Client Desktop (Qui) /JAB	Ephemeral	Paging Server	4200	TCP	Yes 1024 - 65535	No	Open	Communication path to email/chat related servers
14.	Client Desktop (Qui) /JAB	Ephemeral	WACD	90xx	TCP	Yes 1024 - 65535	No	Open	VESP connection for server down notification.
15.	Client Desktop (Qui) /JAB	Ephemeral	Email Server	19113	TCP	Yes 1024 - 65535	No	Open	Receiving email related data
16.	Attribute Server	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Read/Write/Update ADU data
17.	ICM Service	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Read/Write/Update ADU data
18.	Tomcat (Website)	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Read/Write/Update ADU data
19.	Workflow Server	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Read/Write/Update ADU data
20.	Alarm Server	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login/ get configuration related data
21.	Data Server	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login/ get configuration related data
22.	Email Server	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login/ get configuration related data
23.	IC Manager	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login/ get configuration related data
24.	WACD Server	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login/ get configuration related data
25.	Workflow Server	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login/ get configuration related data

	Source		Destination		Network/ Application Protocol	Destination Configurable ? Range	Source Configurable ? Range	Default Port state (Destination)	Traffic Purpose (Comments)
	Initiator	Port(s)	Receiver	Ports					
26.	ICM Service	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login/ get configuration related data
27.	Tomcat (Website/CSPortal)	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login/ get configuration related data
28.	Alarm Server	Ephemeral	Alarm Server	9003	TCP	Yes 1024 - 65535	No	Open	Alarm propagation across sites
29.	IC Manager	Ephemeral	Alarm Server	9003	TCP	Yes 1024 - 65535	No	Open	Send/Receive Alarms
30.	ICM Service	Ephemeral	Alarm Server	9003	TCP	Yes 1024 - 65535	No	Open	Send/Receive Alarms
31.	Tomcat (Website)	Ephemeral	Alarm Server	9003	TCP	Yes 1024 - 65535	No	Open	Send/Receive Alarms
32.	WACD Server	Ephemeral	License Server	9004	TCP	Yes 1024 - 65535	No	Open	Acquire/renew Agent/Feature License
33.	Telephony Server	Ephemeral	License Server	9004	TCP	Yes 1024 - 65535	No	Open	Acquire/renew Agent/Feature License
34.	Email Server	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
35.	WACD Server	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
36.	Report Server	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
37.	Comhub Server	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
38.	Workflow Server	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
39.	DUStore Server	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations

	Source		Destination		Network/ Application Protocol	Destination Configurable? Range	Source Configurable? Range	Default Port state (Destination)	Traffic Purpose (Comments)
	Initiator	Port(s)	Receiver	Ports					
40.	ICM Service	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
41.	Tomcat (Website)	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
42.	HTTP Connector	Ephemeral	Data Server	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
43.	Workflow Server	Ephemeral	Email Server	90xx	TCP	Yes 1024 - 65535	No	Open	Receive events about email contacts coming in
44.	EDU Server	Ephemeral	EDU Server	90xx	TCP	Yes 1024 - 65535	No	Open	EDU servers talk to each other and act as proxy for EDU requests
45.	EDU Server	Ephemeral	DUStore Server	90xx	TCP	Yes 1024 - 65535	No	Open	Idle EDUs are stored and retrieved to the DB using DUStore server
46.	Blender Server	Ephemeral	Workflow Server	90xx	TCP	Yes 1024 - 65535	No	Open	Blender server requests Workflow server to run agent blending flows
47.	Telephony Server	Ephemeral	EDU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Read/Write/Update EDUs related to voice contacts
48.	IC Manager	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Agent related events
49.	Blender Server	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Blender server monitors/sets agent state using ADUs
50.	Workflow Server	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Blender flows read ADU data to run routing algorithms

	Source		Destination		Network/ Application Protocol	Destination Configurable ? Range	Source Configurable ? Range	Default Port state (Destination)	Traffic Purpose (Comments)
	Initiator	Port(s)	Receiver	Ports					
51.	Telephony Server	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Read/Write/Update ADUs for agents which are handling voice contacts
52.	EDU Server	Ephemeral	Report Server	90xx	TCP	Yes 1024 - 65535	No	Open	Sends events on the EDUs which are completed
53.	Attribute Server	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Agent related events
54.	ICM Service	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Agent related events
55.	Tomcat (Website)	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Agent related events
56.	WACD Server	Ephemeral	ADU Server	90xx	TCP	Yes 1024 - 65535	No	Open	Read/Write/Update ADUs for agents which are handling email/chat contacts
57.	Email Server	Ephemeral	WACD Server	90xx	TCP	Yes 1024 - 65535	No	Open	Receive events about incoming contacts and inform WACD about the state of an email contact
58.	Workflow Server	Ephemeral	WACD Server	90xx	TCP	Yes 1024 - 65535	No	Open	Receives events about flows to be run for incoming chat/email tasks and outgoing emails
59.	Attribute Server	Ephemeral	WACD Server	90xx	TCP	Yes 1024 - 65535	No	Open	Passes data back and forth between website and WACD
60.	Attribute Server	Ephemeral	ICM Service	9503	TCP	Yes 1024 - 65535	No	Open	Chat data between ICM Server and ICM Bridge (Attribute server).

	Source		Destination		Network/ Application Protocol	Destination Configurable? Range	Source Configurable? Range	Default Port state (Destination)	Traffic Purpose (Comments)
	Initiator	Port(s)	Receiver	Ports					
61.	Tomcat (Website/CSPortal)	Ephemeral	ICM Service	9505	TCP	Yes 1024 - 65535	No	Open	Chat data between Website and ICM Server
62.	ICM /Tomcat (Website/ CSPortal)	Ephemeral	Attribute Server	2300	TCP	Yes 1024 - 65535	No	Open	Attribute server updates (pushes) the administration data changes.
63.	IIS (DataWake Plug-in)	Ephemeral	Attribute Server	2300	TCP	Yes 1024 - 65535	No	Open	DataWake information.
64.	Tomcat (RL Manager)	Ephemeral	Email Server	19114	TCP	Yes 1024 - 65535	No	Open	Data about response templates for email contacts
65.	Paging Server	Ephemeral	ComHub Server	4001	TCP	Yes 1024 - 65535	No	Open	Comhub server acts as a Hub between various servers, including Paging Server
66.	WACD Server	Ephemeral	ComHub Server	4001	TCP	Yes 1024 - 65535	No	Open	Comhub server acts as a Hub between various servers, including WACD Server
67.	Tomcat (Admin Website)	Ephemeral	WACD Server	4010	TCP	Yes 1024 - 65535	No	Open	Data related to various email/chat contacts, their status, and agent status
68.	SDK Client	Ephemeral	Tomcat (SDK Server)	9700	TCP	Yes 1024 - 65535	No	Open	Http listener primarily used for initiating connections.
69.	AAWC (Browser Client)	Ephemeral	Tomcat (AAWC Server)	9080	TCP	Yes 1024 - 65535	No	Open	Http listener primarily used for initiating connections

	Source		Destination		Network/ Application Protocol	Destination Configurable ? Range	Source Configurable ? Range	Default Port state (Destination)	Traffic Purpose (Comments)
	Initiator	**Port(s)**	**Receiver**	**Ports**					
70.	SDK Client/AAW C (Browser Client)	Ephem eral	Tomcat (SDK Server)	2 ports in the range 8000 to 9000	TCP		No	Open	All agent/server communication for all data related to all contacts
71.	HTTPConn ector	Ephem eral	Workflow Server	90xx	TCP	Yes 1024 - 65535	No	Open	Process Http request of VP-IC integration to IC system to execute the call flow.
72.	HTTPVox	Ephem eral	EDU	90xx	TCP	Yes 1024 - 65535	No	Open	Sets the EDUID with ADUID
73.	Telephony Server	Ephem eral	HTTPVo x	90xx	TCP	Yes 1024 - 65535	No	Open	To monitor the extension of new call
74.	HTTPVox	Ephem eral	ADU	90xx	TCP	Yes 1024 - 65535	No	Open	Monitors the Extension and sets ADUID with extension
75.	Workflow Server	Ephem eral	HTTPvox	90xx	TCP	Yes 1024 - 65535	No	Open	To get extension and eduid
76.	Vox	Ephem eral	EDU	90xx	TCP	Yes 1024 - 65535	No	Open	To create EDUID for new call(when TS is absent and VRU is networked)
77.	Telephony Server	Ephem eral	Vox	90xx	TCP	Yes 1024 - 65535	No	Open	To monitor the extension of new call
78.	VRU	Ephem eral	Vox	Reco mmen ded 3000	TCP	Yes 1024 - 65535	Yes	Open	To initiate connection with VRU
79.	Vox	Default port is ZERO	VRU	Config ured on VRU	TCP	Yes 1024 - 65535	Yes	Open	To initiate connection with Vox

	Source		Destination		Network/ Application Protocol	Destination Configurable ? Range	Source Configurable ? Range	Default Port state (Destination)	Traffic Purpose (Comments)
	Initiator	Port(s)	Receiver	Ports					
80.	Client Desktop (QUI) /JAB	Ephemeral	ICM Services	9501	TCP	Yes 1024 - 65535	No	Open	Communication with a Chat contact.
81.	WSCallback	Ephemeral	DataServer	90xx	TCP	Yes 1024 - 65535	No	Open	Database operations
82.	WSCallback	Ephemeral	Directory Server	9002	TCP	Yes 1024 - 65535	No	Open	Login/ get configuration related data
83.	WSCallback	Ephemeral	ICM Service	9502	TCP	Yes 1024 - 65535	No	Open	For scheduled calls.
84.	Tomcat Redirector (Webserver)	Ephemeral	RLManager (Tomcat)	9643	TCP	Yes	No	Open	Template administration.
85.	Tomcat Redirector (Webserver)	Ephemeral	Website (Tomcat)	9642	TCP	Yes	No	Open	Web services.
86.	Tomcat Redirector (Webserver)	Ephemeral	CSPortal (Tomcat)	9699	TCP	Yes	No	Open	CSPortal webservices.
87.	WebAdmin plugin (Webserver)	Ephemeral	WACD	4010	TCP	Yes	No	Open	WACD administration.
88.	VESP client	Ephemeral	Directory server	14433	TCP	Yes	No	Open	VESP Client secure logins.
89.	OA	Ephemeral	Event Collector	90xx	TCP	Yes	No	Open	OA events specific.
90.	OA	Ephemeral	Event Collector Bridge	90xx	TCP	Yes	No	Open	OA events specific.

Notes

- The ephemeral ports are used on the client side.
- 90xx port numbers can be changed and the default port numbers are allocated sequentially depending on the order in which the servers are created.
- Generally, a VESP client (e.g. custom client) can send a VESP request to any of the VESP servers listening port.

Disabling directory browse in IIS

1. Open Internet **Information Services (IIS) Manager**.
2. In the Connections pane, expand the server name, and then go to the site, application, or directory where you want to enable directory browsing.
3. In the **Home** pane, double-click Directory Browsing.
4. In the **Actions** pane, click **Disable**.
5. In the **Directory Browsing** pane, select the options that correspond to the information you want to display for each item in the directory, and then click Apply.

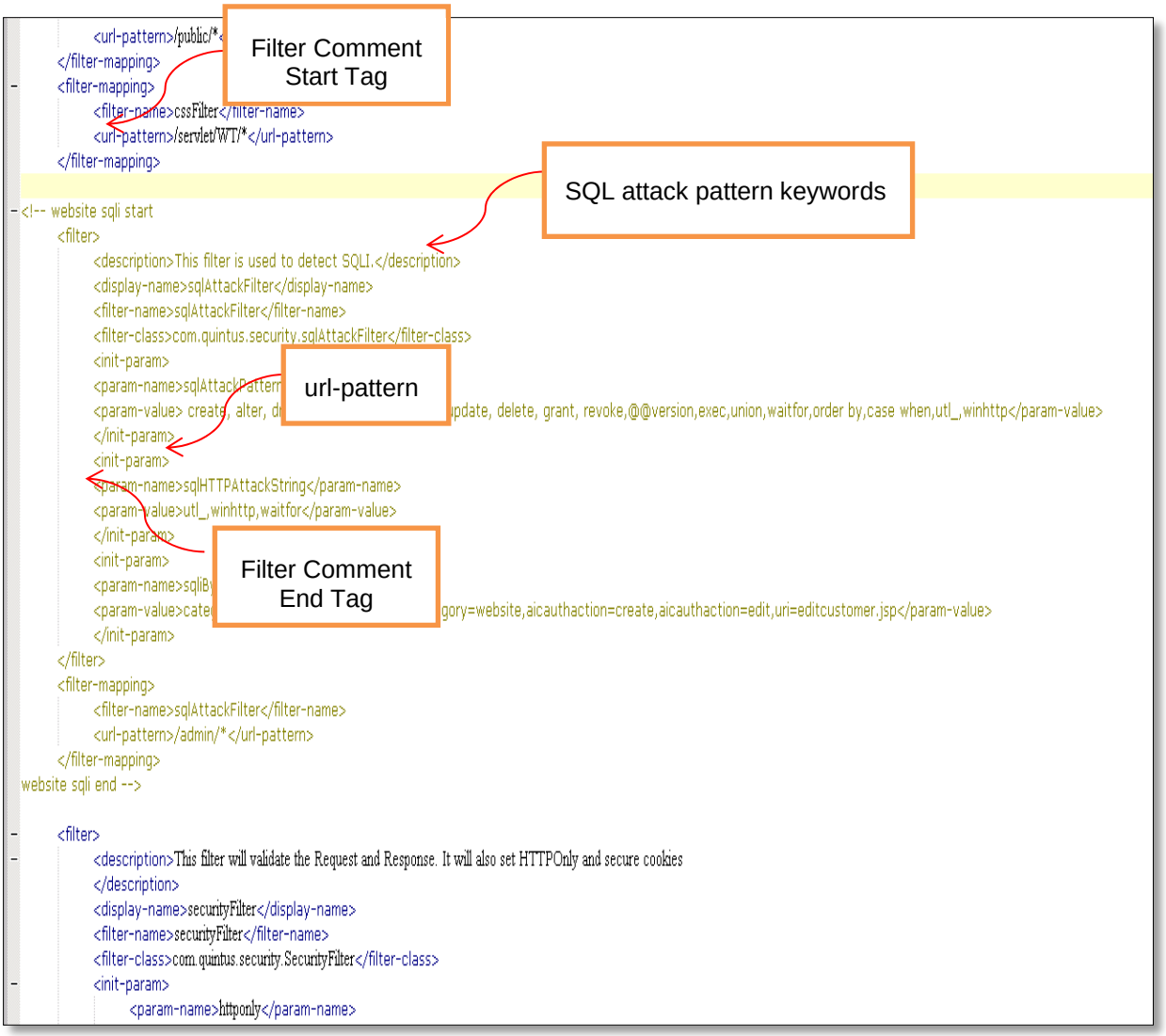
For more information:
https://docs.microsoft.com/en-us/iis/configuration/system.webserver/directorybrowse

Appendix B: Configuration for preventing SQL injection attacks

Enabling the filter

1. From the `<AVAYA_IC73_HOME>/comp/website/WEB-INF/` directory, open the `web.xml` file in a text editor.

   You see the following code:



2. Remove the filter comment start tag and the filter comment end tag to enable the filter for the admin site.

   Although SQL injection related vulnerabilities have not been discovered in the public website, there is no harm in enabling this for the public website as well. To enable the filter for the entire website, change the “url-pattern” value to “/*” in the filter mapping.

Extending/customizing the filter

The filter can be customized by modifying the “SQL attack pattern keywords”. A default set of keywords have already been provided to mitigate the most common SQL Injection attacks.

Reference documents

- Avaya Interaction Center Release 7.3.x Telephony Connectors Programmer
- Avaya Interaction Center Release 7.3.x Installation and Configuration
- Avaya Interaction Center Release 7.3.x Administration Help
- Avaya WebLM Release 6.3.4 for Core Services Developer Guide
- Avaya Interaction Center Release 7.3.x Release Notes

Security documents on the Avaya support site

For more information about security documents that complement the Avaya IC security guide, see the Avaya Security Vulnerability Classification document at: https://downloads.avaya.com/css/P8/documents/100066674.