



Survey Assist Installation Guide

Release 4.2.0.4
September 2020

© 2016-2020 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original Published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked 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> 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.

HostedService

THE FOLLOWING APPLIES IF YOU PURCHASE A 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/](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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER,

THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION,

AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Support Tools:

“AVAYA SUPPORT TOOLS” MEAN THOSE SUPPORT TOOLS PROVIDED TO PARTNERS OR CUSTOMERS IN CONNECTION WITH MAINTENANCE SUPPORT OF AVAYA EQUIPMENT (E.G., SAL, SLA MON, AVAYA DIAGNOSTIC SERVER, ETC.) AVAYA SUPPORT TOOLS ARE INTENDED TO BE USED FOR LAWFUL DIAGNOSTIC AND NETWORK INTEGRITY PURPOSES ONLY. The customer is responsible for understanding and complying with applicable legal requirements with regard to its network. The Tools may contain diagnostic capabilities that allow Avaya, authorized Avaya partners, and authorized customer administrators to capture packets, run diagnostics, capture key strokes and information from endpoints including contact lists, and remotely control and monitor end-user devices. The customer is responsible for enabling these diagnostic capabilities, for ensuring users are aware of activities or potential activities and for compliance with any legal requirements with respect to use of the Tools and diagnostic capabilities on its network, including, without limitation, compliance with laws regarding notifications regarding capture of personal data and call recording.

Licenses

THE SOFTWARE LICENSE TERMS OR SUPPORT TOOLS LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo)

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 and Support Tools, 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. 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. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. 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.

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 currently available for license from Avaya 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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.

Support Tools: Avaya Support Tools are provided as an entitlement of Avaya Support Coverage (e.g., maintenance) and the entitlements are established by Avaya. The scope of the license for each Tool is described in its License terms and/or the applicable service description document.

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.

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 Documentation or on Avaya’s website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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](http://www.mpegla.com).

Note to Service Provider

The Product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

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. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

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, 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.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

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.

Table of Contents

Chapter 1: Introduction.....	9
Scope	9
System Requirements.....	9
Definitions, acronyms, and abbreviations	9
Chapter 2: Before you begin	10
Key for SSL.....	10
Keystore requirements.....	10
Chapter 3: Installing Survey Assist Software on Single Box Deployments.....	11
Pre-Installation Steps	11
Creating Experience Portal Web Services User for POM Integration	11
Create System Manager Administrator User.....	12
Create System Manager User for AACC CCT Connector	13
Installation Steps.....	13
Unpacking the Distribution Bundle.....	13
Editing the Configuration File.....	14
Installation	18
Post-Installation Steps	19
Adding a certificate to the System Manager	19
Add Survey Assist as System Manager Element	21
Importing Survey Assist certificates into the Experience Portal.....	24
Configuring WebLM URL in Orchestration Designer Runtime.....	25
Configuring the WebLM URL Address.....	26
Restarting the OD Services	26
Upgrade Single Box Deployments	27
Upgrade from Previous Versions	27
Upgrade from 4.1 Versions	27
How to upgrade.....	29
Unpacking the Distribution Bundle.....	29
Generate Certificate Keystore.....	29
Upgrade	29
Chapter 4: Installing Survey Assist Software on Cluster Deployments	30
Pre-Installation Steps	30
Configuring NTP on cluster.....	30
Creating Experience Portal Web Services User for POM Integration	32
Create System Manager Administrator User	33
Create System Manager User for AACC CCT Connector	33
Installation Steps.....	34
Unpacking the Distribution Bundle.....	34

Editing the Configuration File	35
Installation	40
Post-Installation Steps	42
Adding a certificate to the System Manager	42
Add Survey Assist as System Manager Element	44
Importing Survey Assist certificates into the Experience Portal.....	47
Configuring WebLM URL in Orchestration Designer Runtime.....	49
Configuring the WebLM URL Address.....	49
Upgrade Cluster Deployments	50
Upgrade from Previous Versions	50
Upgrade from 4.1 Versions	50
Upgrade Steps	50
Unpacking the Distribution Bundle.....	50
Upgrade	51
Sample logs	51
Chapter 5: Installing Breeze Snap-in	54
Snap-in Installation.....	54
Loading the snap-in.....	54
Installing the snap-in	54
Snap-in Configuration	55
Snap-in attributes	55
Sequencing the DNIS for Survey Redirection.....	56
Service Profile in Avaya Breeze for Survey Redirection Snap-in	56
Implicit User Profile in Avaya Breeze for Survey Redirection Snap-in	57
Create Application in Session Manager for Survey Redirection Snap-in	57
Create Application Sequence in Session Manager for Survey Redirection Snap-in	57
Create Implicit User dial pattern in Session Manager for the Inbound DNIS.....	58
Chapter 6: Installing AACC CCT Connector Service.....	60
CCT Connector Service Installation.....	60
Installing the service.....	60
Configuring the service	60
Chapter 7: Regenerating and reimporting certificates.....	64
Chapter 8: Update Credentials	65
System Manager Credentials.....	65
POM Credentials.....	65
Chapter 9: Troubleshooting	66
Log files	66
Collecting Log files	66
Log files description	66

Survey services	67
List of services	67
Service commands.....	68
Common issues	69
Chapter 10: Security	70
Firewall Logs	70
Enabling Firewall Denied Logs	70
Displaying Firewall Denied Logs	70
Encryption Algorithms	71
Encryption Algorithms used for credentials.....	71
User Profiles.....	71
Avaya User Profiles matching.....	71
ROOT privileges.....	72
Components running with root user	72
Auditing file changes	72
Using the auditd service to log file changes	72
Appendix I.....	77
Related resources	77
Appendix II.....	78
System Manager Trust Management.....	78
Create an “End Entity Profile” for the Survey server.....	78
Create an “End Entity” for the Survey server	80
Create the keystore.....	83
Change keystore alias.....	84
Change keyStore password.....	84
Appendix III.....	86
OS network configuration.....	86
Running the Linux network configuration script	86

Chapter 1: Introduction

Survey Assist Solution enables the creation of surveys associated with other Avaya Products such as AES or POM. This solution provides users with a flexible and reliable way to create customized surveys for maximizing their business results. The primary purpose of this guide is to enable users to install the Survey package.

Scope

This document describes the stages to install or upgrade Survey Assist on Single Box and Cluster Deployments.

System Requirements

See *Survey Assist Hardware and Software Specification Guide*.

Definitions, acronyms, and abbreviations

AES: Avaya Enablement Services

CM: Communication Manager

CTI: Computer Telephony Integration

DNIS: Dialed Number Identification Service

DTMF: Dual Tone Multi Frequency (Touchtone)

IVR: Interactive Voice Response - The technology that simulates the behavior of a live agent.

POM: Proactive Outreach Manager

TTS: Text to Speech - a method of generating synthesized speech from text when pre-recorded system or custom phrases are not available

VDN: Vector Directory Number - an entry extension that provides access to the programming feature on the PBX

VP/AAEP: Voice Portal / Avaya Aura Experience Portal – a portal that enables callers to interact with VXML voice applications residing on a web application server

WEBLM: Web License Manager

Chapter 2: Before you begin

Go through the *Hardware and Software specification guide*. All pre-requisites must be met prior to installation.

Key for SSL

Starting from Survey Assist 4.2.0, a keystore with a private and public key must be provided as a pre-requisite.

For that purpose, there are two options:

- Providing the keystore.
- Using SMGR to generate the keystore. (See Appendix "System Manager Trust Management")

Keystore requirements

Procedure

1. The keystore file must be in **PKCS12** format.
2. Inside the keystore, a private key must be accompanied by the corresponding public key certificate.
3. The minimum key size of the Signature Algorithm is 2048 bits.
4. The entry alias for the certificate must be "**survey-https**".
5. The distinguished name of the owner of the certificate is "CN=SERVER_FQDN" (e.g survey1.avaya.com), which should be the same as the DNS server name used on the installation.
6. A self-signed certificate is not accepted.
7. The minimum validity period for the certificate must be greater than 30 days.
8. The Subject Alternative Name Field must contain the IP and DNS of the server (**for cluster installation it must contain the IP and DNS of each node**) (e.g SAN=dns:survey1.avaya.com,dns:survey2.avaya.com,dns:survey3.avaya.com,ip:10.1.1.1,ip:10.1.1.2,ip:10.1.1.3)

Chapter 3: Installing Survey Assist Software on Single Box Deployments

Pre-Installation Steps

First go through the *Hardware and Software specification guide*. All pre-requisites must be met prior to installation.

Creating Experience Portal Web Services User for POM Integration

About this task

This user is only required if Survey Assist is integrated with Proactive Outreach Manager (POM). If not, skip this step.

Before you begin

Create a new user on Experience Portal with web services role so Survey Assist can use POM Web Services.

Procedure

1. Log in to the Experience Portal Web Interface with an administrator user.
2. Go to User Management > Users and click **Add** button.
3. For the respective fields, do the following:
 - In the field **Name**, type in `surveypom`.
 - In **Enable**, select Yes.
 - In **Roles**, select **Web Services, POM Campaign Manager and POM Administration** roles.
 - In the field **password**, type in a password.
 - In the field **Verify Password**, repeat the password.
 - Uncheck **Enforce Password Longevity**.
4. Click **Save**.
5. Save the username and password for later usage.

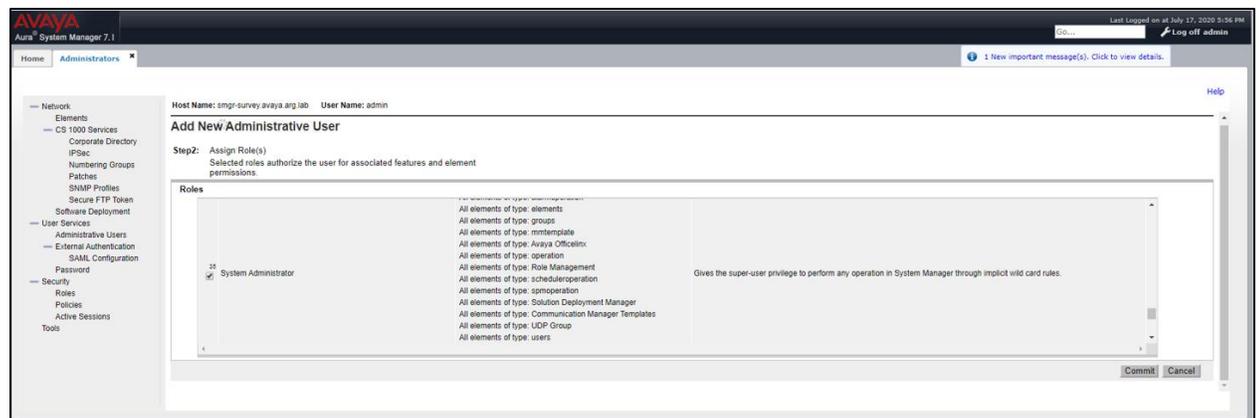
Create System Manager Administrator User

About this task

It is required to create a new System Manager user so Survey Assist can use System Manager Web Services for authentication purposes. This user is only used by the Web Services, to create the necessary users for Survey Assist refer to **Administration and Configuration guide: Create Survey System Administration users** and **Create Survey Users**.

Procedure

1. Log in to System Manager Web Interface with an Administrator user.
2. Go to **Users > Administrators** and click the **Add** button.
3. In the respective fields, type in the following:
 - In the field **User ID**, type in **surveyservices**.
 - In the field **Authentication**, type in **select Local**.
 - In the field **Full Name**, type in **surveyservices**.
 - In the field **Password**, type in a password.
 - In the field **Confirm password** repeat the password.
4. Click on **Commit and Continue**.
5. In **Assign Role(s)**, select the role **System Administrator** and click **Commit**.



6. Log out from the System Manager.
7. Go to the System Manager login. The password set during user creation for the user **surveyservices** must be changed before logging, click on the **Change Password** link, then update your password.
8. Type in a new password and click **Change**.
9. Test the new password by logging in to System Manager again.
10. Save the username and password for later usage.

Note: after the installation completes refer to the **Administration and Configuration Guide** to create the **Survey User** and the **Survey Administration User**, in chapter 2: **Configuring SMGR**.

Create System Manager User for AACC CCT Connector

About this task

This user is only required if Survey Assist is integrated with AACC using the AACC CCT Connector. If not, skip this step.

Procedure

1. Log in to System Manager Web Interface with an Administrator user.
2. Go to Home > **Users** Management > **Manager Users** and click the **New** button.
3. In the respective fields, type in the following:
 - In the field **Last Name**, type in surveycctservice (or the name of your choice).
 - In the field **First Name**, type in surveycctservice (or the name of your choice).
 - In the field **Login Name**, type in surveycctservice@<domain> (e.g. surveycctservice@avaya.com).
 - In the field **Temporary password**, type in a password.
 - In the field **Re-enter password** repeat the password.
4. Click on **Commit and Continue**.
5. In **Assign Role(s)**, select the role **Survey User** and click **Commit**.
6. Log out from System Manager.
7. Log in using the new user surveycctservice@<domain>. System Manager notifies you to change the password.
8. Type in a new password and click **Change**.
9. Test the new password by logging in to System Manager again.
10. Save the username and password for later usage.

Installation Steps

Unpacking the Distribution Bundle

Procedure

- Decompress the file at `/tmp/survey-installer/`. This directory is `<INSTALL_DIR>`

```
mkdir /tmp/survey-installer/

tar -vxf omsurvey-bundle-singlebox-4.1.1.tar.gz -C /tmp/survey-installer/
```

Editing the Configuration File

Before you begin

Before running the main installation script, edit the configuration file with the following information:

- Note:**
 - This step is not required when performing an upgrade.
 - This file is removed after successful installation.

Procedure

- Go to `INSTALL_DIR/userentry`.
- Edit the file `configuration.properties` with the following information:

Parameters	Explanation	Sample	Required
KEYSTORE_PATH	Path to the keystore file provided by the customer or generated for the installation	/home/myserver.p12	yes
KEYSTORE_PASS	Password defined for the keystore file being used	k3y\$t0r3_pa\$\$w0rd	yes
SMGR_FQDN	System Manager Fully Qualified Domain Name	smgr.avaya.com	yes
SMGR_USER	System Manager administrator user	surveyservices	yes
SMGR_PASS	System Manager administrator user's password	admin-smgr-pass	yes
WEBLM_FQDN	Web License Manager Fully Qualified Domain Name	weblm.avaya.com	yes
WEBLM_PORT	Web License Manager Port	443 or 52233	yes

Parameters	Explanation	Sample	Required
AES_ENABLED	Flag to indicate if AES will be used	true or false	
AES_FQDN	Application Enablement Services ; Fully Qualified Domain Name	aes.avaya.com or aes1.avaya.com;aes2.avaya.com	
POM_ENABLED	Flag to indicate if POM will be used	true or false	yes
POM_FQDN	Proactive Outreach Manager Fully Qualified Domain Name	pom.avaya.com	
POM_USER	Proactive Outreach Manager Web Service username	surveypom	
POM_PASSWORD	Proactive Outreach Manager Web Service username password	pom-ws-pass	
OCEANA_ENABLED	Flag to indicate if Oceana will be used	true or false	yes
OCEANA_HOST	The Oceana Core Data Services (OCDS) Fully Qualified Domain Name	oceana.cds.avaya.com	
OCEANA_PORT	The Oceana Core Data Services (OCDS) Port number	443	
OCEANA_PROTOCOL	The Oceana Core Data Services (OCDS) Protocol	https OR http	
OCEANA_USER	The Oceana Core Data Services (OCDS) Username	oceana-username	
OCEANA_PASS	The Oceana Core Data Services (OCDS) Password	oceana-password	

SAMPLE FILE

```

#
*****
*****

#       Survey Assist SSL Certificates and Configuration
#
#       -----
-----

#       IMPORTANT: THIS FILE WILL BE AUTOMATICALLY REMOVED AFTER A
SUCCESSFULL INSTALLATION
#       -----
-----

#
#
*****
*****

# -----
# Certificates Information (Required)
# -----
# The keystore path.
KEYSTORE_PATH=/path/to/keystore.p12
# The keystore password.
KEYSTORE_PASS=your_pass
# -----
# System Manager Information (Required)
# -----
# The System Manager Fully Qualified Domain Name. For example:
SMGR_FQDN=smgr.avaya.com
SMGR_FQDN=smgr.avaya.arg.lab
# The System Manager administrator user. For example: SMGR_USER=admin-
smgr
SMGR_USER=admin-smgr-user
# The System Manager administrator user's password. For example:
SMGR_PASS=admin-smgr-pass
SMGR_PASS=admin-smgr-pass
# -----
# Web License Manager Information (Required)
# -----

```

```

# The Web License Manager Fully Qualified Domain Name. For example:
WEBLM_FQDN=weblm.avaya.com
WEBLM_FQDN=weblm.avaya.arg.lab
# The Web License Manager Port. For example: WEBLM_PORT=443 or
WEBLM_PORT=52233
WEBLM_PORT=443
# -----
# AES Information (Optional)
# -----
# Flag to indicate if AES will be used. For example: AES_ENABLED=true
AES_ENABLED=true
# The Application Enablement Services Fully Qualified Domain Name. For
example: AES_FQDN=aes.avaya.com
AES_FQDN=135.20.200.100;135.20.200.101
# -----
# POM Information (Optional)
# -----
# Flag to indicate if POM will be used. For example: POM_ENABLED=true
POM_ENABLED=true
# The Proactive Outreach Manager Fully Qualified Domain Name. For
example: POM_FQDN=pom.avaya.com
POM_FQDN=135.20.200.101
# The Proactive Outreach Manager Web Service user. For example:
POM_USER=pom-ws-user
POM_USER=pom-ws-user
# The Proactive Outreach Manager Web Service user's password. For
example: POM_PASSWORD=pom-ws-pass
POM_PASS=pom-ws-pass

# -----
# Oceana Information (Optional)
# -----

# Flag to indicate if Oceana will be used. For example:
OCEANA_ENABLED=true
OCEANA_ENABLED=true

```

```

# The Oceana Fully Qualified Domain Name. For example:
OCEANA_HOST=oceana.avaya.com
OCEANA_HOST=135.20.201.34

# The Oceana Port Number. For example: OCEANA_HOST=8080
OCEANA_PORT=443

# The Oceana Protocol. For example: OCEANA_HOST=http (possible values
"http" or "https")
OCEANA_PROTOCOL=https

# The Oceana Web Service user. For example: OCEANA_USER=oceana-ws-user
OCEANA_USER=user

# The Oceana Web Service user's password. For example:
OCEANA_PASS=oceana-ws-pass
OCEANA_PASS=password

#
*****
# End
#
*****

```

Installation

Prior to the installation please check the [OS network configuration](#)

About this task

All steps are performed from the installation path (INSTALL_DIR)

Procedure

1. Navigate to the installation root directory where the following files and directories are listed.

```

total 44K
drwx-----, 16 root root 4.0K Feb 27 15:43 .
drwxrwxrwt, 28 root root 4.0K Feb 27 15:43 ..
drwxr-xr-x, 2 root root 4.0K Feb 26 16:21 bin
drwxr-xr-x, 2 root root 54 Feb 27 15:43 breeze
drwxr-xr-x, 2 root root 138 Feb 27 15:43 certificates
drwxr-xr-x, 2 root root 4.0K Feb 27 15:43 compose
drwxr-xr-x, 2 root root 58 Feb 27 15:43 configuration
drwxr-xr-x, 2 root root 4.0K Feb 27 15:43 containers
drwxr-xr-x, 2 root root 4.0K Feb 27 15:44 docker-images
drwxr-xr-x, 2 root root 134 Feb 27 15:44 documentation
drwxr-xr-x, 2 root root 22 Feb 27 15:44 eula
drwxr-xr-x, 2 root root 21 Feb 27 15:44 info
-rwxr-xr-x, 1 root root 4.2K Feb 26 16:04 install.sh
drwxr-xr-x, 2 root root 26 Feb 27 15:44 licenses
drwxr-xr-x, 2 root root 88 Feb 27 15:44 properties
drwxr-xr-x, 2 root root 108 Feb 27 15:44 smgr
-rwxr-xr-x, 1 root root 4.4K Feb 26 16:04 uninstall.sh
-rwxr-xr-x, 1 root root 1.7K Feb 26 16:04 update-smgr-config-file.sh
drwxr-xr-x, 2 root root 38 Feb 27 15:44 userentry

```

Figure 1: The root directory

2. Run the install.sh script: `./install.sh`
3. After running the install script, you must accept the End User License Agreement (EULA).
4. Wait until the installation finishes when the following text is displayed: `**** [Installation SUCCESS] ****`

Post-Installation Steps

Adding a certificate to the System Manager

Procedure

1. Log in to System Manager and navigate to Services > Inventory > Manage Elements.
2. Select the **System Manager** element and from the **More Actions** drop down menu, select the option **Configure Trusted Certificates**.

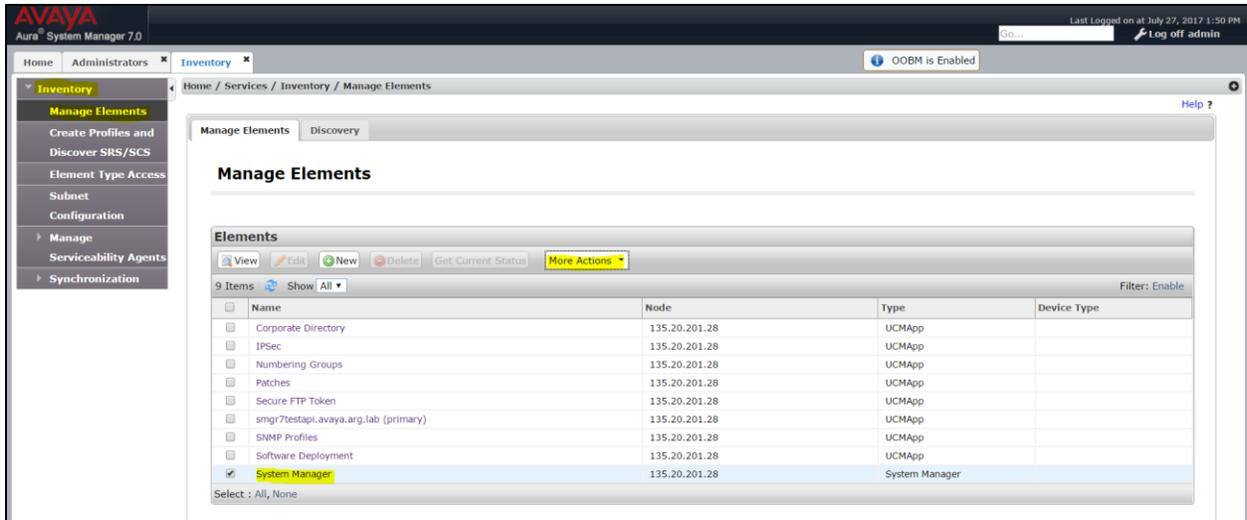


Figure 2: Adding a certificate to the System Manager

3. Click the **Add** button to add a new trusted certificate.

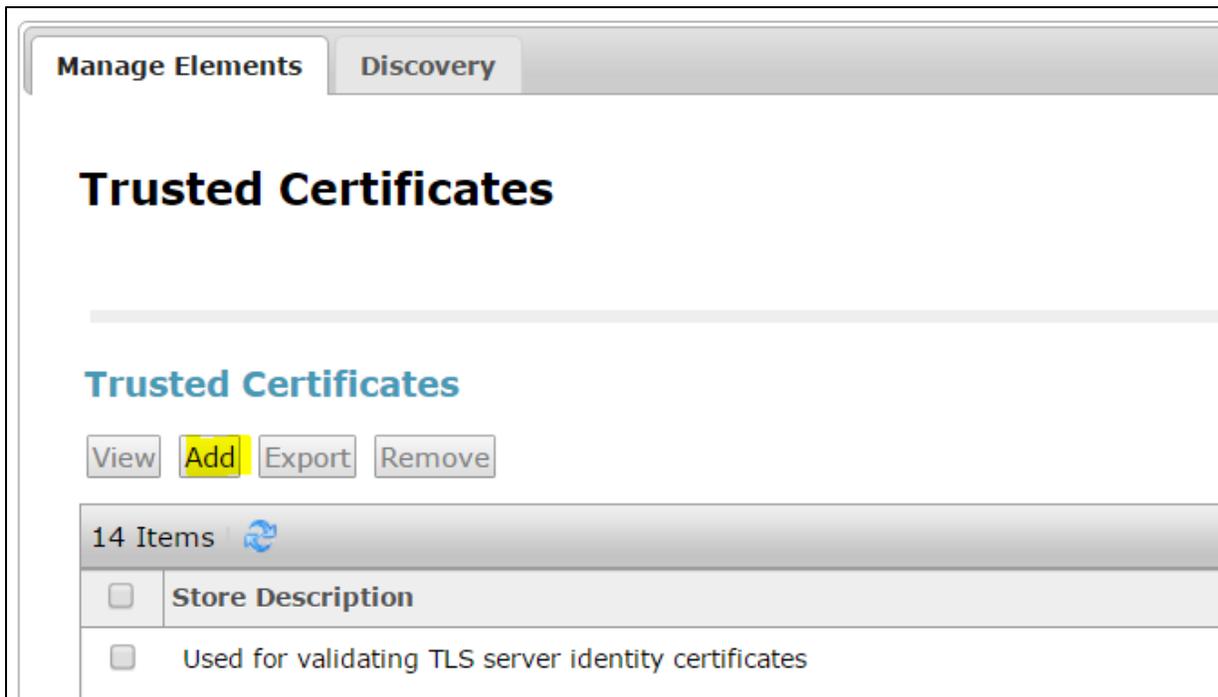


Figure 3: Trusted certificates

4. Select store type **All** and import from the file.
5. Import the file:
`/opt/avaya/survey/installer/certificates/myserver.crt`

Add Survey Assist as System Manager Element

About this task

To support SSO on SMGR, you need to configure Survey Assist on SMGR.

Procedure

Copy the files at `INSTALL_DIR/smgr` (`SurveyAssist.properties`, `com.avaya.ept.SurveyAssist.xml`) to the SMGR server using SSH to the directory `/tmp/smgr`.

1. Log in to SMGR server with SSH.
2. To assign read permission to all users, run: `chmod a+r <FILE_NAME_1> <FILE_NAME_2>`
3. Change the ownership of the files in `/tmp/smgr`: `chown admin:admin <FILE_NAME_1> <FILE_NAME_2>`
4. Copy the file located under `/tmp/smgr/SurveyAssist.properties` to:
`/opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/conf/elementRegistry/messages/`
5. Copy the file located under `/tmp/smgr/com.avaya.ept.SurveyAssist.xml` to:
`/opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/conf/elementRegistry/elementType.`
If the file is properly copied, the system moves the file to the **deployed** directory.
6. Check the SMGR log for details.
7. There should be two additional Roles on SMGR:
 - Survey User
 - Survey Assist Administration.
8. Delete the directory `/tmp/smgr` and the files within it: `rm -rf /tmp/smgr`

Note:

For SMGR 8.0, the Element Registry path has changed:

```
/opt/Avaya/JBoss/wildfly-10.1.0.Final/avmgmt/configuration/quantum/elementRegistry
```

The system displays all three folders in the above path:

- Messages
- ElementType
- NavigationMenuItem

Sample Log Output of Successful Install

Check the log file named quantum.log at /opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/log/ or at /var/log/Avaya/jboss/log/

```
2017-11-14 12:00:00,371 ERROR
[com.nortel.quantum.log.EndUserLoggerImpl] Failed to log message :
secureObjectType : com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,372 INFO
[com.nortel.ems.mgmt.quantum.element.registry.impl.ElementRegistryFile
SystemImpl] Element type com.avaya.ept.SurveyAssist.xml is published.

2017-11-14 12:00:00,476 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils]
Installing en localization properties for com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,533 INFO
[com.nortel.ems.mgmt.quantum.common.utils.web.WebUtils] Server
returned HTTP response code: 302 for URL: https://smgr7-testapi-
2.avaya.arg.lab/quantum-web-client/messages/files/SurveyAssist_en

2017-11-14 12:00:00,533 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils] Cannot
load localization properties from https://smgr7-testapi-
2.avaya.arg.lab/quantum-web-client/messages/files/SurveyAssist_en

2017-11-14 12:00:00,533 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils]
Specified localization properties are not provided - using the default
properties instead.

2017-11-14 12:00:00,534 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils]
Installing en_US localization properties for
com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,579 INFO
[com.nortel.ems.mgmt.quantum.common.utils.web.WebUtils] Server
returned HTTP response code: 302 for URL: https://smgr7-testapi-
2.avaya.arg.lab/quantum-web-client/messages/files/SurveyAssist_en_US

2017-11-14 12:00:00,579 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils] Cannot
load localization properties from https://smgr7-testapi-
2.avaya.arg.lab/quantum-web-client/messages/files/SurveyAssist_en_US

2017-11-14 12:00:00,579 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils]
Specified localization properties are not provided - using the default
properties instead.

2017-11-14 12:00:00,579 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils]
Installing default localization properties for
com.avaya.ept.SurveyAssist
```

2017-11-14 12:00:00,581 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Registering new resource type definition:
com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,797 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Registration of new resource type definition complete:
com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,798 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Registering base line policy for:
com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,800 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Adding built-in role: Survey.20User

2017-11-14 12:00:00,858 SECURITY
[com.nortel.ems.mgmt.quantum.log.CS1000LogHandler] Info: User:
id=Internal, Role Survey User(id=Survey.20User) has been created
successfully.

2017-11-14 12:00:00,923 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Adding built-in role: Survey.20Administrator

2017-11-14 12:00:00,932 SECURITY
[com.nortel.ems.mgmt.quantum.log.CS1000LogHandler] Info: User:
id=Internal, Role Survey Administrator(id=Survey.20Administrator) has
been created successfully.

2017-11-14 12:00:01,037 SECURITY
[com.nortel.ems.mgmt.quantum.log.CS1000LogHandler] Info: User:
id=Internal,
com.avaya.ept.SurveyAssist:survey.20administrator|dc=nortel,dc=com

2017-11-14 12:00:01,072 SECURITY
[com.nortel.ems.mgmt.quantum.log.CS1000LogHandler] Info: User:
id=Internal, com.avaya.ept.SurveyAssist:survey.20user|dc=nortel,dc=com

2017-11-14 12:00:01,073 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Finished registering base line policy for:
com.avaya.ept.SurveyAssist

2017-11-14 12:00:01,074 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Flag cleared post schema update process termination for
type: com.avaya.ept.SurveyAssist

2017-11-14 12:00:10,491 INFO
[com.nortel.ems.mgmt.quantum.element.registry.impl.ElementRegistryFile

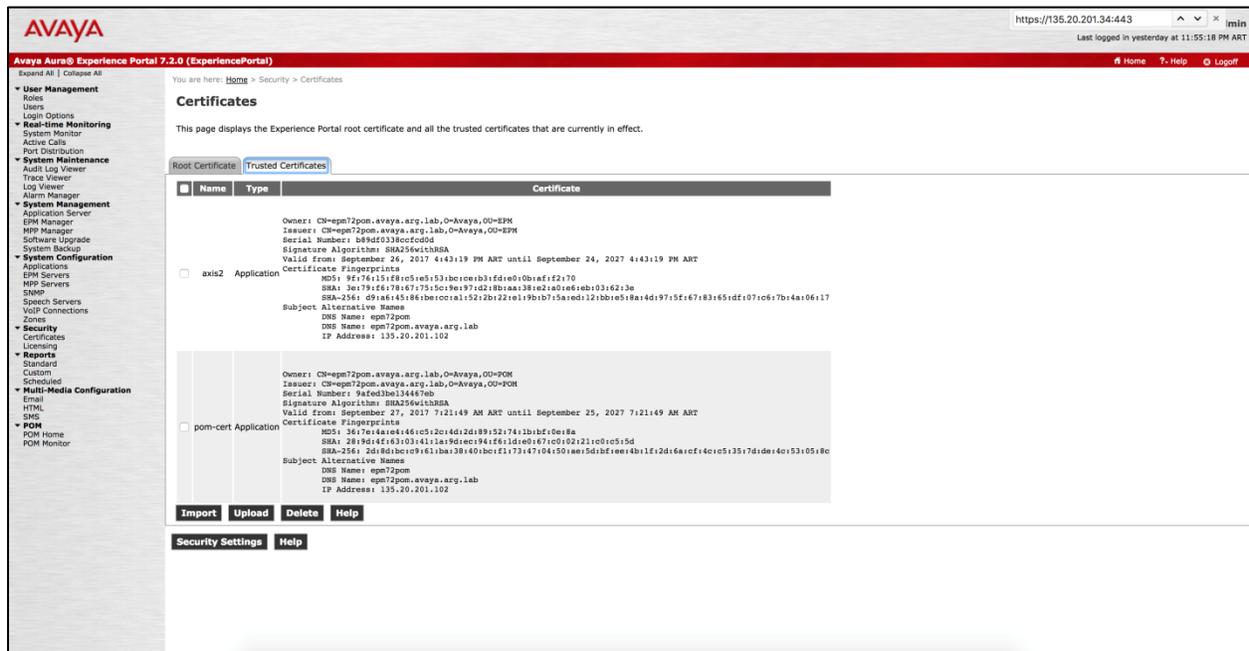
SystemImpl] Element type(s) schema registration completed in security server.

Importing Survey Assist certificates into the Experience Portal

Procedure

1. Log in to Experience Portal (AAEP) Web Administration and navigate to **Certificates** menu.
2. Click the **Trusted Certificates** tab.
3. Click on **Import** button.

The system displays a new page titled **Import Trusted Certificate**.



The screenshot shows the Avaya Experience Portal interface. The left sidebar contains a navigation menu with categories like User Management, Real-time Monitoring, System Maintenance, System Configuration, and Security. The main content area is titled 'Certificates' and displays a table of trusted certificates. The table has columns for Name, Type, and Certificate details. Two certificates are listed: 'axis2' and 'pom-cert', both of type 'Application'. Each certificate entry shows its name, type, and a detailed view of its properties, including issuer, serial number, signature algorithm, valid from/to dates, and subject information. At the bottom of the table, there are buttons for 'Import', 'Upload', 'Delete', and 'Help'. Below the table, there are also buttons for 'Security Settings' and 'Help'.

Figure 4: Importing certificates

4. Type in SurveyAssist on the **name** field and select **Application** as type.
5. Type in `https://<SURVEY_FQDN>:443/` as location.
6. Replace SURVEY_FQDN with the Survey server FQDN that is, hostname and domain.

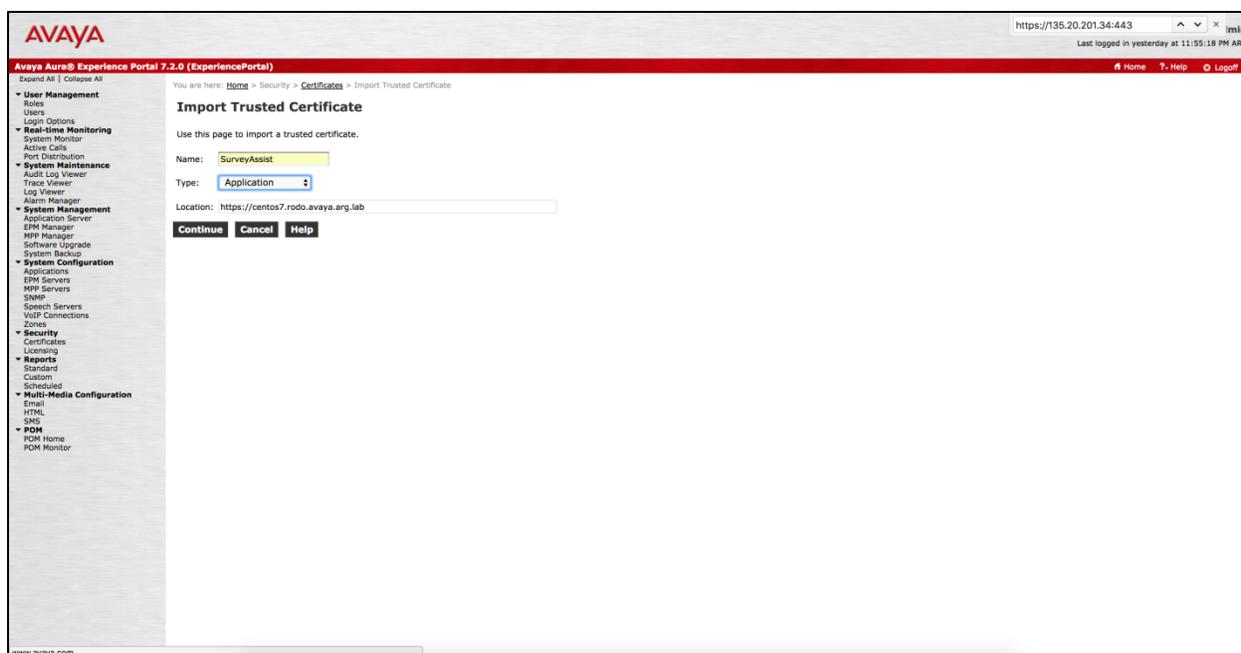


Figure 5: Import trusted certificate

7. Click **Continue**.

The SurveyAssist certificate gets listed as Trusted Certificate.

Configuring WebLM URL in Orchestration Designer Runtime

About this task

By default, OD uses the same WebLM used by AAEP. If you want to use a different WebLM server, you need to follow the steps for both OD applications in ports 9080 and 9180.

Run the following for each port in a SingleBox installation:

- For SMS: `https://<IP>:9080/runtimeconfig`
- For Voice: `https://<IP>:9180/runtimeconfig`

Run the following for each port in a Cluster installation:

- For SMS:
 - `https://<IP>:31100/runtimeconfig`
 - `https://<IP>:31101/runtimeconfig`
- For Voice:
 - `https://<IP>:31000/runtimeconfig`

- `https://<IP>:31001/runtimeconfig`

Configuring the WebLM URL Address

Procedure

1. Log in to the OD Runtime Config for the Voice OD Module via browser. The port number is **9080** and the username is `ddadmin`.
2. You may receive a notification to change the default password. The password is `ddadmin`.
3. After you are logged in, click **License Server**, on the left menu.

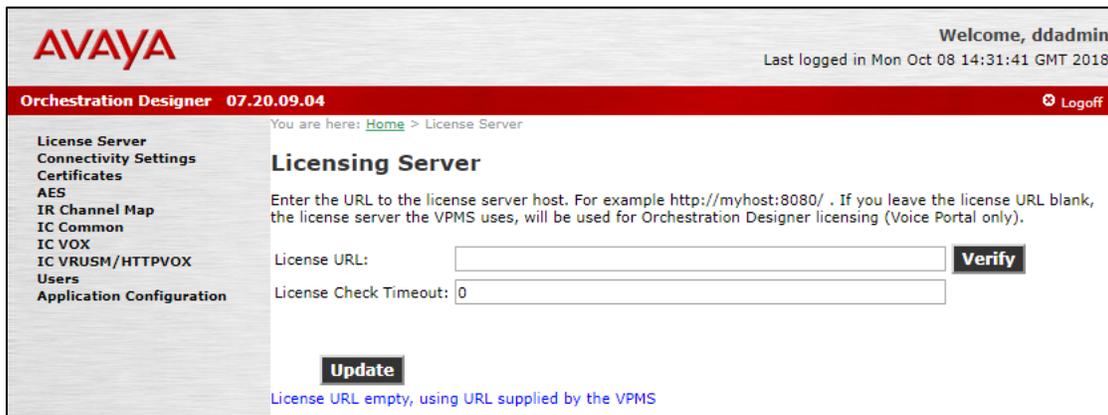


Figure 6: Licensing server

4. In the **License URL**, enter the WebLM URL you want to use.
5. Click Update.
6. Restart the OD Services.

- **Note:**

Run these steps on port 9180 too.

Restarting the OD Services

Procedure

1. To restart the Voice Channel Service, use the following:
`docker restart od-voice`
2. To restart the SMS Channel Service, use the following:
`docker restart od-sms`

- **Note:**

Before logging in for the first time, you must create a new Survey User in System Manager (check “*Adding new Survey user*” in the *Administration and Configuration Guide*)

Upgrade Single Box Deployments

Upgrade from Previous Versions

When upgrading from Survey Assist Release 4.0 or any 4.0.x release, the process automatically identifies the version, upgrades the software and maintains all existing data except the following:

- **Important:**
 - New certificate from a trusted CA must be provided.
 - Existing TLinks must be recreated manually after upgrade.

Upgrade from 4.1 Versions

Warnings

If an upgrade starts during the installation, and the process to upgrade the callinfo configuration cannot re-create your AES Configuration, the installation shows a warning message like this:

```
--- Upgrade callinfo containers ---
(17:03:13) Running docker-service <callinfo-init> version <4.0.9-SNAPSHOT>
Creating callinfo-init ... done
Waiting for <callinfo-init> service to finish loading...

*** ERROR ***: <callinfo-init> finish with errors and status-exitcode <exited-2>

*** ERROR ***: Upgrading callinfo containers

---. Upgrading callinfo containers: WARNING
```

Figure 7: Warning

If the system displays a warning, the installation generates additional information.

The information is stored at `/opt/avaya/survey/docker_volumes/logs`, in the following files:

- `callinfo-init.log`

This file has information about the process and the errors.

- **callinfo-init-errors-information.log**

This file has the AES Configuration information that cannot be re-created.

Use that information to manually re-create your previous AES Configuration, by using that information.

A sample of **callinfo-init-errors-information.log**:

```
--- The following Callinfo container could not be created ---
{
  "id" : "c13511ca-011a-4741-86a1-207c705f60a9",
  "name" : "TlinkName",
  "containerInformation" : {
    "containerId" : "43f2197054d06905f6c5b62464619d3503a000ada01",
    "containerHostname" : "43f2197054d0"
  },
  "jtapiConfiguration" : {
    "jtapiProperties" : {
      "CONNECTION_PRIMARY_AES_ADDRESS" : "10.10.10.10",
      "CONNECTION_PRIMARY_AES_SERVICE_NAME" : "AES-SERVICE#NAME"
      "CONNECTION_PRIMARY_AES_USERNAME" : "aes-user",
      "CONNECTION_PRIMARY_AES_PASSWORD" : "aes-pass",
      "CONNECTION_SECONDARY_AES_ADDRESS" : "",
      "CONNECTION_SECONDARY_AES_SERVICE_NAME" : "",
      "CONNECTION_SECONDARY_AES_USERNAME" : "",
      "CONNECTION_SECONDARY_AES_PASSWORD" : "",
      "CONNECTION_AES_TRUSTED_LICENSES" : "false",
      "TASK_SKILL_MONITOR_SKILLS" : "48498,48499",
      "TASK_VDN_MONITOR_VDNS" : "48398,48399,48414",
      "CONNECTION_RECONNECT_TIMEOUT_MILLIS" : "60000"
    }
  }
}
```

How to upgrade

Unpacking the Distribution Bundle

Procedure

1. Decompress the file at `/tmp/survey-installer/`. This directory is `<INSTALL_DIR>`

```
mkdir /tmp/survey-installer/
```

```
tar -vxf omsurvey-bundle-singlebox-4.2.0.tar.gz -C /tmp/survey-installer/
```

Generate Certificate Keystore

Procedure

1. Create SSL Key as explained on Chapter 2: Before you begin.
2. Once the keystore was generated, rename it to `<HOSTNAME>.p12` where is the server hostname provided by command:

```
hostname -s
```

3. Copy the keystore file `<HOSTNAME>.p12` to `<INSTALL_DIR>/certificates`

- **Note:**

Do not delete any existing files.

Upgrade

About this task

All steps are performed from the installer path (`INSTALL_DIR`).

Procedure

1. Navigate to the installation root directory
2. Run the `install.sh` script

```
./install.sh
```
3. After running the install script, you must accept the End User License Agreement (EULA)
4. Wait until the upgrade finishes

Chapter 4: Installing Survey Assist Software on Cluster Deployments

Pre-Installation Steps

Configuring NTP on cluster

About this task

Set up time synchronization between the nodes. Configure the controller node (MASTER) to synchronize the time from more accurate (lower stratum) NTP servers and then configure the other nodes (NODES) to synchronize the time from the controller node.

Procedure

On the master node, configure the `chronyd` service to synchronize time from a pool of NTP servers and set the `allow` directive to enable it to act as NTP server for the other nodes.

The NTP servers can be public NTP servers or private local NTP servers.

To serve time even if not synchronized to a time source the `local` keyword is used to allow `chronyd` to appear synchronized to real time from the viewpoint of clients polling it, even if it has no current synchronization source. This option is normally used on the "master" computer in an isolated network, where several computers are required to synchronize to one another, and the "master" is kept in line with real time by manual input.

On Master node:

1. Edit the `chrony` file `/etc/chrony.conf` and change the following properties

```
# Use public servers from the pool.ntp.org project.
server controll1.example.com iburst
# Allow NTP client access from local network.
allow <SUBNET>
# Serve time even if not synchronized to a time source
local stratum 10
```

Note: Replace the `<SUBNET>` with your cluster information (format: `x.y.z.0/24`)

2. Save the file

- Restart chrony daemon and configure it to start following a system reboot, by using the following commands:

```
# systemctl restart chronyd
# systemctl enable chronyd
```

- The UDP port number 123 needs to be open in the firewall in order to allow the client access:

```
# firewall-cmd --permanent --zone=public --add-port=123/udp
# firewall-cmd --reload
```

On the other nodes:

- Edit the chrony file `/etc/chrony.conf` and change the following properties

```
# Use public servers from the pool.ntp.org project.
server <MASTER FQDN> iburst
```

Note: Replace the <MASTER FQDN> with your cluster information

- Save the file
- Restart chrony daemon and configure it to start following a system reboot, by using the following commands:

```
# systemctl restart chronyd
# systemctl enable chronyd
```

On Master and Nodes:

- Verify that chronyd is accessing the correct time sources.

```
# chronyc -a sources
```

On the controller node, the Name/IP address column in the command output should list the configured pool of NTP servers.

```
[root@survey50-ubum ~]# chronyc -a sources
210 Number of sources = 4
MS Name/IP address          Stratum Poll Reach LastRx Last sample
=====
^? 23.152.160.126           0 10    0    -    +0ns[ +0ns] +/- 0ns
^? triton.ellipse.net      0 10    0    -    +0ns[ +0ns] +/- 0ns
^? varuna.ga-group.nl      0 10    0    -    +0ns[ +0ns] +/- 0ns
^? ntp.jaxxnet.org          0 10    0    -    +0ns[ +0ns] +/- 0ns
```

On all other nodes, it should list the controller nodes.

```
[root@survey51-ubuw1 ~]# chronyc -a sources
210 Number of sources = 1
MS Name/IP address          Stratum Poll Reach LastRx Last sample
=====
^* survey50-ubum.avaya.arg.> 10 10 377 999 +36us[ +37us] +/- 235us
```

2. Ensure that the time is synchronized on all nodes.

Use the `chronyc -a tracking` command to check the offset (the Last offset row)

Use the `date +%F %T,%3N` to check the datetime

```
# chronyc -a tracking
```

```
# date +%F %T,%3N"
```

Example: Master and Node 1

<pre>[root@survey50-ubum ~]# chronyc -a tracking Reference ID : 7F7F0101 () Stratum : 10 Ref time (UTC) : Wed May 27 19:24:59 2020 System time : 0.000000000 seconds fast of NTP time Last offset : +0.000000000 seconds RMS offset : 0.000000000 seconds Frequency : 0.000 ppm slow Residual freq : +0.000 ppm Skew : 0.000 ppm Root delay : 0.000000000 seconds Root dispersion : 0.000000000 seconds Update interval : 0.0 seconds Leap status : Normal</pre>	<pre>[root@survey51-ubuw1 ~]# chronyc -a tracking Reference ID : 8714C932 (survey50-ubum.avaya.arg.lab) Stratum : 11 Ref time (UTC) : Wed May 27 19:10:06 2020 System time : 0.000002115 seconds fast of NTP time Last offset : +0.000000792 seconds RMS offset : 0.000001347 seconds Frequency : 0.000 ppm slow Residual freq : +0.000 ppm Skew : 0.001 ppm Root delay : 0.000250426 seconds Root dispersion : 0.000900212 seconds Update interval : 1036.6 seconds Leap status : Normal</pre>
--	--

```
[root@survey50-ubum ~]# date +%F %T,%3N"
2020-05-27 15:29:45,329
```

```
[root@survey51-ubuw1 ~]# date +%F %T,%3N"
2020-05-27 15:29:45,322
```

Creating Experience Portal Web Services User for POM Integration

About this task

This user is only required if Survey Assist is integrated with Proactive Outreach Manager (POM). If not, skip this step.

Before you begin

Create a new user on Experience Portal with web services role so Survey Assist can use POM Web Services.

Procedure

1. Log in to the Experience Portal Web Interface with an administrator user.
2. Go to User Management > Users and click **Add** button.
3. For the respective fields, do the following:
 - In the field **Name**, type in `surveypom`.
 - In **Enable**, select Yes.

- In **Roles**, select **Web Services, POM Campaign Manager and POM Administration** roles.
 - In the field **password**, type in a password.
 - In the field **Verify Password**, repeat the password.
 - Uncheck **Enforce Password Longevity**.
4. Click **Save**.
 5. Save the username and password for later usage.

Create System Manager Administrator User

About this task

It is required to create a new System Manager user so Survey Assist can use System Manager Web Services for authentication purposes.

Procedure

1. Log in to System Manager Web Interface with an Administrator user.
2. Go to **Users > Administrators** and click the **Add** button.
3. In the respective fields, type in the following:
 - In the field **User ID**, type in surveyservices.
 - In the field **Authentication**, type in select Local.
 - In the field **Full Name**, type in surveyservices.
 - In the field **Temporary password**, type in a password.
 - In the field **Re-enter password** repeat the password.
4. Click **Commit and Continue**.
5. In **Assign Role(s)**, select the role **System Administrator** and click **Commit**.
6. Log out from System Manager.
7. Log in using the new user surveyservices.
System Manager notifies you to change the password.
8. Type in a new password and click **Change**.
9. Test the new password by logging in to System Manager again.
10. Save the username and password for later usage.

Create System Manager User for AACC CCT Connector

About this task

This user is only required if Survey Assist is integrated with AACC using the AACC CCT Connector. If not, skip this step.

Procedure

1. Log in to System Manager Web Interface with an Administrator user.
2. Go to Home > **Users** Management > **Manager Users** and click the **New** button.
3. In the respective fields, type in the following:
 - In the field **Last Name**, type in surveycctservice (or the name of your choice).
 - In the field **First Name**, type in surveycctservice (or the name of your choice).
 - In the field **Login Name**, type in surveycctservice@<domain> (e.g. surveycctservice@avaya.com).
 - In the field **Temporary password**, type in a password.
 - In the field **Re-enter password** repeat the password.
4. Click on **Commit and Continue**.
5. In **Assign Role(s)**, select the role **Survey User** and click **Commit**.
6. Log out from System Manager.
7. Log in using the new user surveycctservice@<domain>. System Manager notifies you to change the password.
8. Type in a new password and click **Change**.
9. Test the new password by logging in to System Manager again.
10. Save the username and password for later usage.

Installation Steps

Unpacking the Distribution Bundle

Procedure

1. Decompress the file at `/tmp/survey-installer/`. This directory is `<INSTALL_DIR>`

```
mkdir /tmp/survey-installer/  
tar -vxf omsurvey-bundle-cluster-4.1.1.tar.gz -C /tmp/survey-installer/
```

- **Note:**

On Cluster deployments, download the bundle and decompress it on the first VM that becomes the Master Node.

Editing the Configuration File

Before you begin

Before running the main installation script, edit the configuration file with the following information:

- **Note:**
 - This step is not required when performing an upgrade.
 - This file is removed after successful installation.

Procedure

1. Go to `INSTALL_DIR/userentry`.
2. Edit the file `configuration.properties` with the following information:

Parameters	Explanation	Sample	Required
DOCKER_REPOSITORY_HOST	Master VM FQDN	master.avaya.com	yes
DOCKER_REPOSITORY_PORT	Host machine port for image download	8999	yes
INSTALLATION_MODE	Type of installation	cluster	yes
KEYSTORE_PATH	Path to the keystore file provided by the customer or generated for the installation	/home/myserver.p12	yes
KEYSTORE_PASS	Password defined for the keystore file being used	k3y\$t0r3_pa\$\$w0rd	yes
SMGR_FQDN	System Manager Fully Qualified Domain Name	smgr.avaya.com	yes
SMGR_USER	System Manager administrator user	admin-smgr	yes
SMGR_PASS	System Manager administrator user's password	admin-smgr-pass	yes
WEBLM_FQDN	Web License Manager Fully Qualified Domain Name	weblm.avaya.com	yes

Parameters	Explanation	Sample	Required
WEBLM_PORT	Web License Manager Port	443 or 52233	yes
AES_ENABLED	Flag to indicate if AES will be used	true or false	
AES_FQDN	Application Enablement Services ; Fully Qualified Domain Name	aes.avaya.com or aes1.avaya.com;aes2.avaya.com	
POM_ENABLED	Flag to indicate if POM will be used	true or false	
POM_FQDN	Proactive Outreach Manager Fully Qualified Domain Name	pom.avaya.com	
POM_USER	Proactive Outreach Manager Web Service username	pom-ws-user	
POM_PASSWORD	Proactive Outreach Manager Web Service username password	pom-ws-pass	
OCEANA_ENABLED	Flag to indicate if Oceana will be used	true or false	
OCEANA_HOST	The Oceana Core Data Services (OCDS) Fully Qualified Domain Name	oceana.cds.avaya.com	
OCEANA_PORT	The Oceana Core Data Services (OCDS) Port number	443	
OCEANA_PROTOCOL	The Oceana Core Data Services (OCDS) Protocol	https OR http	
OCEANA_USER	The Oceana Core Data Services (OCDS) Username	oceana-username	
OCEANA_PASS	The Oceana Core Data Services (OCDS) Password	oceana-password	

SAMPLE FILE

```
#
*****
*****

# Survey Assist SSL Certificates and Configuration
#
# -----
-----

# IMPORTANT: THIS FILE WILL BE AUTOMATICALLY REMOVED AFTER A
SUCCESSFULL INSTALLATION
# -----
-----

#
#
*****
*****

# -----
# Kubernetes Information
# -----

DOCKER_REPOSITORY_HOST=master.avaya.com

DOCKER_REPOSITORY_PORT=8999

INSTALLATION_MODE=cluster

# -----
# Certificates Information (Required)
# -----
# The keystore path.
KEYSTORE_PATH=/path/to/keystore.p12
# The keystore password.
KEYSTORE_PASS=your_pass
# -----
# System Manager Information (Required)
```

```

# -----
# The System Manager Fully Qualified Domain Name. For example:
SMGR_FQDN=smgr.avaya.com
SMGR_FQDN=smgr.avaya.arg.lab
# The System Manager administrator user. For example: SMGR_USER=admin-
smgr
SMGR_USER=admin-smgr-user
# The System Manager administrator user's password. For example:
SMGR_PASS=admin-smgr-pass
SMGR_PASS=admin-smgr-pass
# -----
# Web License Manager Information (Required)
# -----
# The Web License Manager Fully Qualified Domain Name. For example:
WEBLM_FQDN=weblm.avaya.com
WEBLM_FQDN=weblm.avaya.arg.lab
# The Web License Manager Port. For example: WEBLM_PORT=443 or
WEBLM_PORT=52233
WEBLM_PORT=443
# -----
# AES Information (Optional)
# -----
# Flag to indicate if AES will be used. For example: AES_ENABLED=true
AES_ENABLED=true
# The Application Enablement Services Fully Qualified Domain Name. For
example: AES_FQDN=aes.avaya.com
AES_FQDN=135.20.200.100;135.20.200.101
# -----
# POM Information (Optional)
# -----
# Flag to indicate if POM will be used. For example: POM_ENABLED=true
POM_ENABLED=true
# The Proactive Outreach Manager Fully Qualified Domain Name. For
example: POM_FQDN=pom.avaya.com
POM_FQDN=135.20.200.101

```

```

# The Proactive Outreach Manager Web Service user. For example:
POM_USER=pom-ws-user
POM_USER=pom-ws-user
# The Proactive Outreach Manager Web Service user's password. For
example: POM_PASSWORD=pom-ws-pass
POM_PASS=pom-ws-pass

# -----
# Oceana Information (Optional)
# -----

# Flag to indicate if Oceana will be used. For example:
OCEANA_ENABLED=true
OCEANA_ENABLED=true

# The Oceana Fully Qualified Domain Name. For example:
OCEANA_HOST=oceana.avaya.com
OCEANA_HOST=135.20.201.34

# The Oceana Port Number. For example: OCEANA_HOST=8080
OCEANA_PORT=443

# The Oceana Protocol. For example: OCEANA_HOST=http (possible values
"http" or "https")
OCEANA_PROTOCOL=https

# The Oceana Web Service user. For example: OCEANA_USER=oceana-ws-user
OCEANA_USER=user

# The Oceana Web Service user's password. For example:
OCEANA_PASS=oceana-ws-pass
OCEANA_PASS=password
#
*****
# End

```

#

Installation

About this task

All steps are performed from the installer path (INSTALL_DIR).

MASTER references the main server, the server from where the installation is executed.

NODE_IP refers to each of the secondary servers IP Addresses.

Procedure

1. Navigate to the installation root directory where the following files and directories are listed.

```
[root@survey50-ubum installer]# ll
total 60
drwxrwxrwx 23 root root 4096 Jul 25 16:19 bin
drwxrwxrwx 2 root root 54 Jul 25 16:19 breeze
drwxrwxrwx 2 root root 138 Jul 25 16:19 certificates
-rwxrwxrwx 1 root root 3885 Jul 25 15:52 cleanup-docker-images.sh
-rwxrwxrwx 1 root root 4008 Jul 25 15:52 collect-logs.sh
drwxrwxrwx 2 root root 58 Jul 25 16:19 configuration
-rwxrwxrwx 1 root root 5317 Jul 25 15:52 create-docker-repository.sh
drwxrwxrwx 2 root root 59 Jul 25 16:19 docker
drwxrwxrwx 2 root root 4096 Jul 25 16:19 docker-images
drwxrwxrwx 2 root root 134 Jul 25 16:19 documentation
drwxrwxrwx 2 root root 22 Jul 25 16:19 eula
drwxrwxrwx 2 root root 21 Jul 25 16:19 info
-rwxrwxrwx 1 root root 4549 Jul 25 16:19 install.sh
drwxrwxrwx 2 root root 88 Jul 25 16:19 k8s-configuration
drwxrwxrwx 2 root root 38 Jul 25 16:19 licenses
-rwxrwxrwx 1 root root 2093 Jul 25 15:52 pods-status-functions.sh
drwxrwxrwx 2 root root 67 Jul 25 16:19 properties
-rwxrwxrwx 1 root root 1130 Jul 25 15:52 README
drwxrwxrwx 2 root root 115 Jul 25 16:19 regenerate-certificates
drwxrwxrwx 2 root root 108 Jul 25 16:19 smgr
-rwxrwxrwx 1 root root 6463 Jul 25 15:52 uninstall.sh
-rwxrwxrwx 1 root root 2768 Jul 25 15:52 update-pom-credentials.sh
-rwxrwxrwx 1 root root 1723 Jul 25 15:52 update-smgr-config-file.sh
-rwxrwxrwx 1 root root 2563 Jul 25 15:52 update-smgr-credentials.sh
drwxrwxrwx 2 root root 6 Jul 25 17:03 userentry
```

Figure 8: The root directory

2. Copy the Docker Daemon file and script to the other two Survey Assist nodes by running these commands:

```
scp docker/docker-configure-daemon.sh survey@<NODE_IP>:/tmp/
```

```
scp docker/daemon.json survey@<NODE_IP>:/tmp/
```

- **Note:**
Replace <NODE_IP> with your cluster information
Repeat this step for each secondary server

3. On MASTER, run the following command to update the daemon.json file:

```
./docker/docker-configure-daemon.sh
```

4. On each of the Nodes, run the following command to update the daemon.json file:

```
cd /tmp/  
./docker-configure-daemon.sh
```

5. Enable NFS on the MASTER Node by running these commands:

```
mkdir /nfs  
echo "/nfs <MASTER_IP>(rw, sync, no_root_squash)  
<NODE_IP>(rw, sync, no_root_squash)  
<NODE_IP>(rw, sync, no_root_squash)" > /etc/exports  
systemctl enable rpcbind  
systemctl start rpcbind  
systemctl enable nfs  
systemctl start nfs
```

- **Note:**
Replace the <MASTER_IP> and <NODE_IP> with your cluster information.
You can verify that the echo command was successful with `cat /etc/exports`.

6. Validate NFS by running this command:

```
systemctl status nfs
```

- **Note:**
Service output must shown "Active" state

7. Generate TLS certificate and registry for node service image download:

```
./create-docker-repository.sh
```

8. Copy and add certificate to the other two Survey Assist nodes by running this command:

```
scp /docker-registry/cert/docker-server.crt  
survey@<NODE_IP>:/tmp/
```

- **Note:**
Repeat this step for each secondary server
Replace <NODE_IP> with your cluster information

9. On the other nodes, run these commands to add the newly generated certificate:

```
cp /tmp/docker-server.crt /etc/pki/ca-trust/source/anchors/  
update-ca-trust enable  
update-ca-trust extract  
service docker restart
```

10. Initialize Cluster by running these commands:

```
kubeadm init --kubernetes-version=v1.13.3 --pod-network-  
cidr=192.168.0.0/16
```

- **Note:**

Copy the line with the output that has the “kubeadm join...” command, it is used later.

```
mkdir -p $HOME/.kube  
cp -i /etc/kubernetes/admin.conf $HOME/.kube/config  
chown $(id -u):$(id -g) $HOME/.kube/config  
kubectl apply -f /etc/kubernetes/etcd.yaml  
kubectl apply -f /etc/kubernetes/calico.yaml  
kubectl taint nodes --all node-role.kubernetes.io/master-
```

11. Add each node to the Cluster by running the join command on the other two nodes:

```
kubeadm join <HASH>
```

- **Note:**

Command previously copied from console as output of kubeadm init.

12. Validate the initialization by checking that all nodes are Ready:

```
kubectl get nodes -o wide
```

13. Run the install.sh script

```
./install.sh
```

14. After running the install script, you must accept the End User License Agreement (EULA).

15. Wait until the installation finishes.

Post-Installation Steps

Adding a certificate to the System Manager

Procedure

1. Log in to System Manager and navigate to Services > Inventory > Manage Elements.

2. Select the **System Manager** element and from the **More Actions** drop down menu, select the option **Manage Trusted Certificates**.

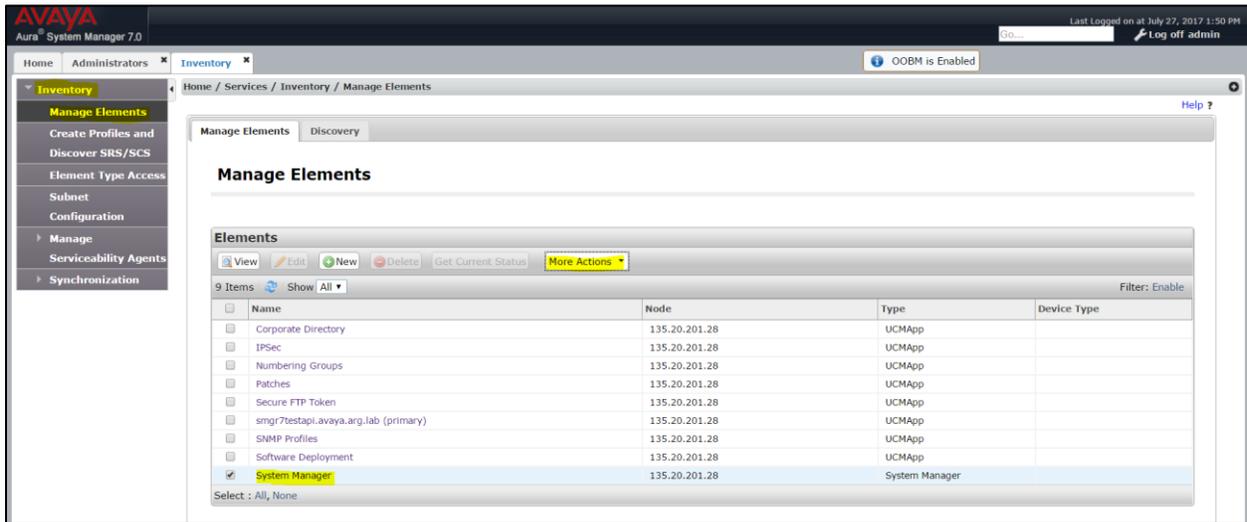


Figure 9: Adding a certificate to the System Manager

3. Click the **Add** button to add a new trusted certificate.

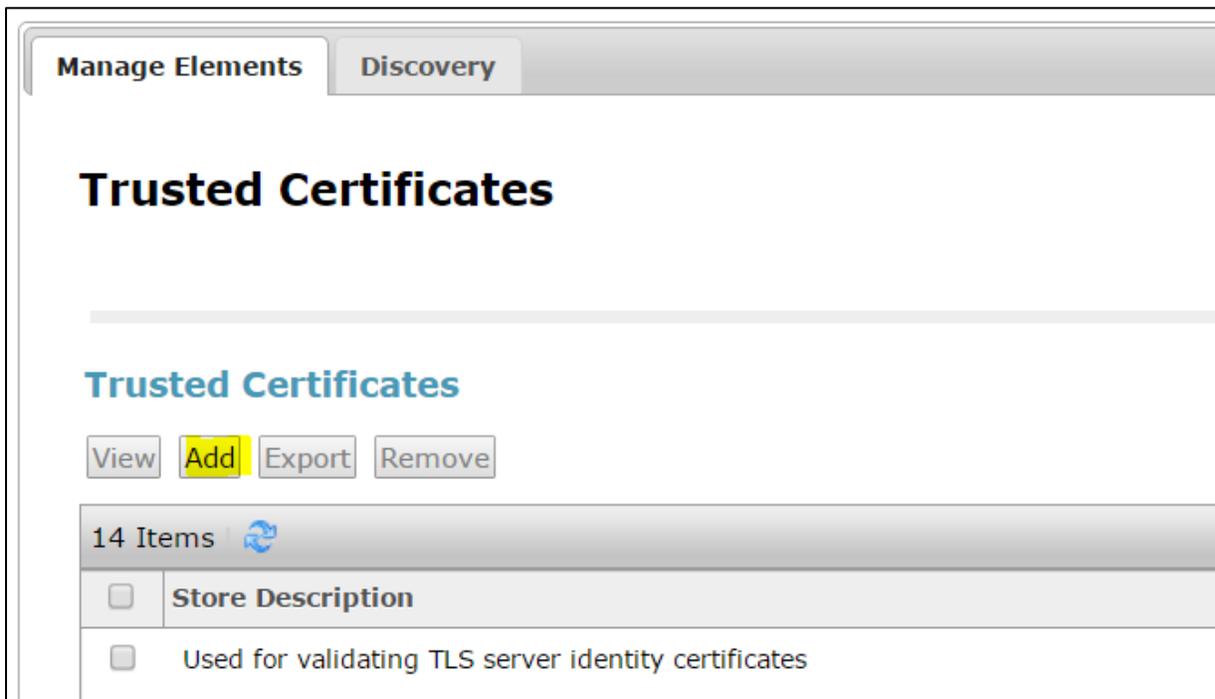


Figure 10: Trusted certificates

4. Select store type **All** and import from the file.
5. Import the file `/opt/avaya/survey/installer/certificates/myserver.crt`

Add Survey Assist as System Manager Element

About this task

To support SSO on SMGR, you need to configure Survey Assist on SMGR.

Procedure

Copy the files at `INSTALL_DIR/smgr` (`SurveyAssist.properties`, `com.avaya.ept.SurveyAssist.xml`) to the SMGR server using SSH to the directory `/tmp/smgr`.

1. Log in to SMGR server with SSH.
2. To assign read permission to all users, run: `chmod a+r <FILE_NAME_1> <FILE_NAME_2>`
3. Change the ownership of the files in `/tmp/smgr`: `chown admin:admin <FILE_NAME_1> <FILE_NAME_2>`
4. Copy the file located under `/tmp/smgr/SurveyAssist.properties` to:
`/opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgt/conf/elementRegistry/messages/`
5. Copy the file located under `/tmp/smgr/com.avaya.ept.SurveyAssist.xml` to:
`/opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgt/conf/elementRegistry/elementType.`
If the file is properly copied, the system moves the file to the **deployed** directory.
6. Check the SMGR log for details.
7. There should be two additional Roles on SMGR:
 - Survey User
 - Survey Assist Administration.
8. Delete the directory `/tmp/smgr` and the files within it: `rm -rf /tmp/smgr`

Note:

For SMGR 8.0, the Element Registry path has changed:

```
/opt/Avaya/JBoss/wildfly-10.1.0.Final/avmgt/configuration/quantum/elementRegistry
```

The system displays all three folders in the above path:

- Messages
- ElementType
- NavigationMenuItem

- Note:

For SMGR 8.0, the Element Registry path has changed:

```
/opt/Avaya/JBoss/wildfly-  
10.1.0.Final/avmgmt/configuration/quantum/elementRegi  
stry
```

The system displays all three folders in the above path:

- Messages
- ElementType
- NavigationMenuItem

Sample Log Output of Successful Install

Check the log file named `quantum.log` at `/opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/log/` or at `/var/log/Avaya/jboss/log/`

```
2017-11-14 12:00:00,371 ERROR  
[com.nortel.quantum.log.EndUserLoggerImpl] Failed to log message :  
secureObjectType : com.avaya.ept.SurveyAssist  
  
2017-11-14 12:00:00,372 INFO  
[com.nortel.ems.mgmt.quantum.element.registry.impl.ElementRegistryFile  
SystemImpl] Element type com.avaya.ept.SurveyAssist.xml is published.  
  
2017-11-14 12:00:00,476 INFO  
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils]  
Installing en localization properties for com.avaya.ept.SurveyAssist  
  
2017-11-14 12:00:00,533 INFO  
[com.nortel.ems.mgmt.quantum.common.utils.web.WebUtils] Server  
returned HTTP response code: 302 for URL: https://smgr7-testapi-  
2.avaya.arg.lab/quantum-web-client/messages/files/SurveyAssist_en  
  
2017-11-14 12:00:00,533 INFO  
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils] Cannot  
load localization properties from https://smgr7-testapi-  
2.avaya.arg.lab/quantum-web-client/messages/files/SurveyAssist_en  
  
2017-11-14 12:00:00,533 INFO  
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils]  
Specified localization properties are not provided - using the default  
properties instead.  
  
2017-11-14 12:00:00,534 INFO  
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils]  
Installing en_US localization properties for  
com.avaya.ept.SurveyAssist
```

2017-11-14 12:00:00,579 INFO
[com.nortel.ems.mgmt.quantum.common.utils.web.WebUtils] Server returned HTTP response code: 302 for URL: https://smgr7-testapi-2.avaya.arg.lab/quantum-web-client/messages/files/SurveyAssist_en_US

2017-11-14 12:00:00,579 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils] Cannot load localization properties from https://smgr7-testapi-2.avaya.arg.lab/quantum-web-client/messages/files/SurveyAssist_en_US

2017-11-14 12:00:00,579 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils] Specified localization properties are not provided - using the default properties instead.

2017-11-14 12:00:00,579 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.I18nUtils] Installing default localization properties for com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,581 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Registering new resource type definition: com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,797 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Registration of new resource type definition complete: com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,798 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Registering base line policy for: com.avaya.ept.SurveyAssist

2017-11-14 12:00:00,800 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Adding built-in role: Survey.20User

2017-11-14 12:00:00,858 SECURITY
[com.nortel.ems.mgmt.quantum.log.CS1000LogHandler] Info: User: id=Internal, Role Survey User(id=Survey.20User) has been created successfully.

2017-11-14 12:00:00,923 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchemaListener] Adding built-in role: Survey.20Administrator

2017-11-14 12:00:00,932 SECURITY
[com.nortel.ems.mgmt.quantum.log.CS1000LogHandler] Info: User: id=Internal, Role Survey Administrator(id=Survey.20Administrator) has been created successfully.

2017-11-14 12:00:01,037 SECURITY
[com.nortel.ems.mgmt.quantum.log.CS1000LogHandler] Info: User:

```
id=Internal,
com.avaya.ept.SurveyAssist:survey.20administrator|dc=nortel,dc=com
2017-11-14 12:00:01,072 SECURITY
[com.nortel.ems.mgmt.quantum.log.CS1000LogHandler] Info: User:
id=Internal, com.avaya.ept.SurveyAssist:survey.20user|dc=nortel,dc=com
2017-11-14 12:00:01,073 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchem
aListener] Finished registering base line policy for:
com.avaya.ept.SurveyAssist
2017-11-14 12:00:01,074 INFO
[com.nortel.ems.mgmt.quantum.security.admin.element.OpenSsoPolicySchem
aListener] Flag cleared post schema update process termination for
type: com.avaya.ept.SurveyAssist
2017-11-14 12:00:10,491 INFO
[com.nortel.ems.mgmt.quantum.element.registry.impl.ElementRegistryFile
SystemImpl] Element type(s) schema registration completed in security
server.
```

Importing Survey Assist certificates into the Experience Portal

Procedure

1. Log in to Experience Portal (AAEP) Web Administration and navigate to **Certificates** menu.
2. Click the **Trusted Certificates** tab.
3. Click **Import** button.

The system displays a new page titled **Import Trusted Certificate**.

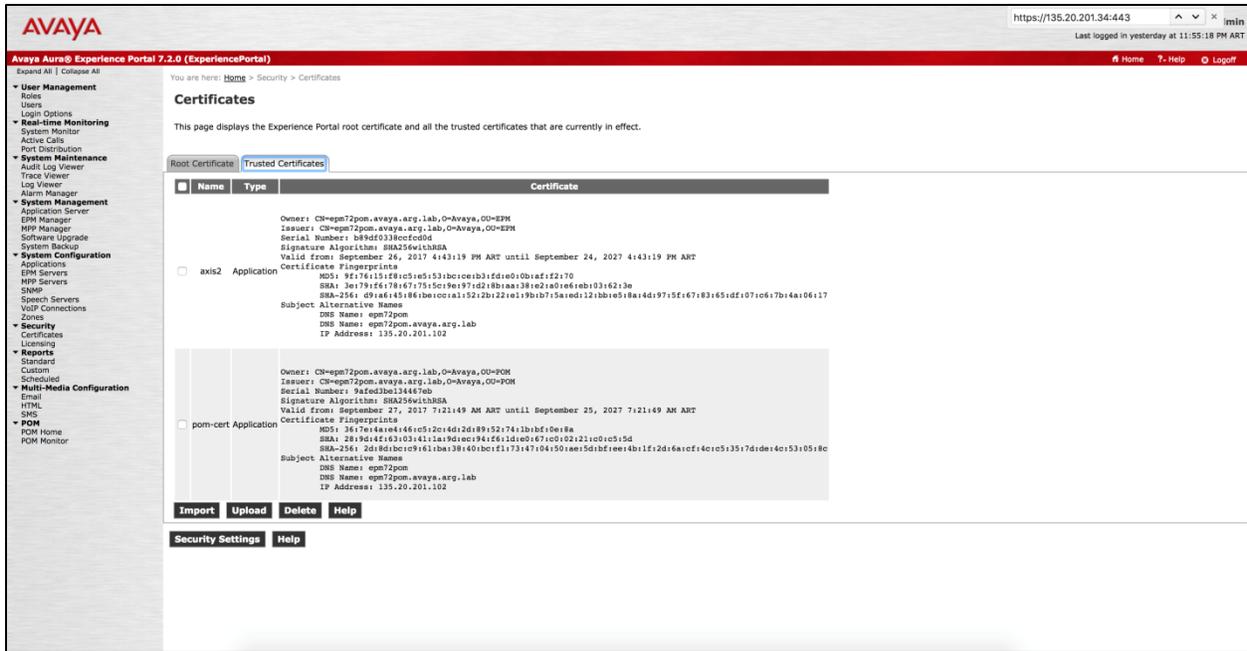


Figure 11: Importing certificates

4. Type in SurveyAssist on the **name** field and select **Application** as type.
5. Type in `https://<SURVEY_1_FQDN>:443/` as location.
6. Replace SURVEY_FQDN with the Survey Node #1 FQDN that is, hostname and domain.

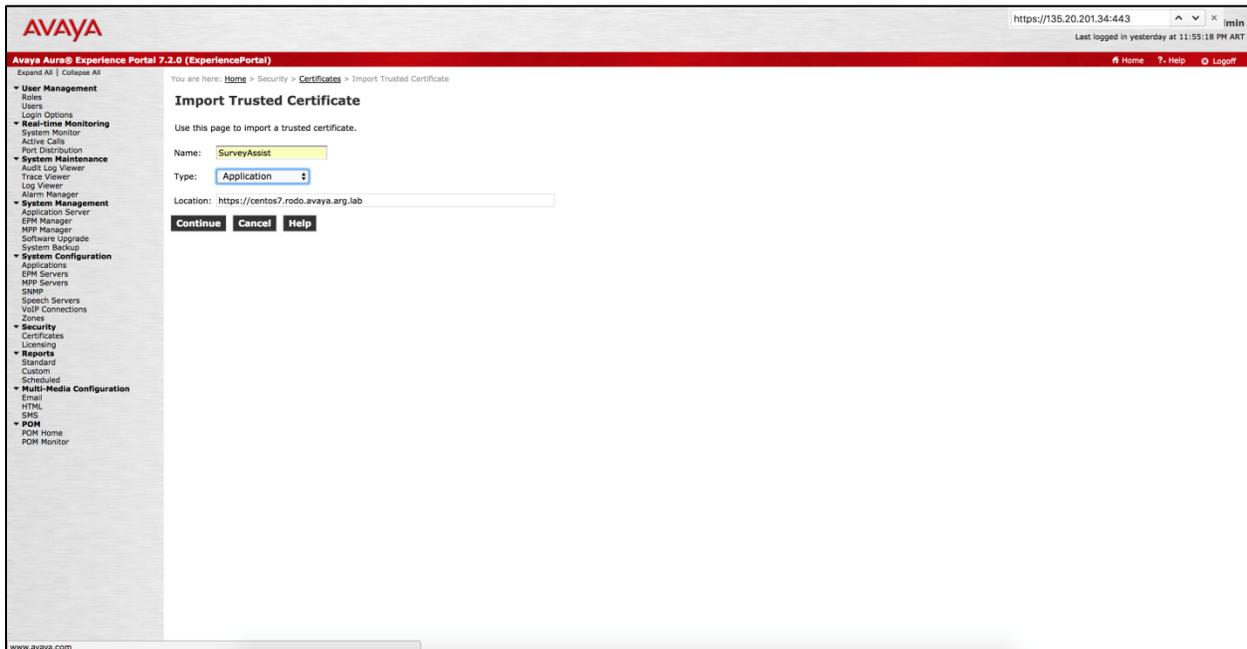


Figure 12: Import trusted certificate

7. Click **Continue**.

The SurveyAssist certificate gets listed as Trusted Certificate.

Configuring WebLM URL in Orchestration Designer Runtime

About this task

By default, OD uses the same WebLM used by AAEP. If you want to use a different WebLM server, you need to follow these steps for both Channel applications and each instance.

Run the following for each port:

- For SMS:
 - `https://<SERVER_1_FQDN>:31100/runtimeconfig`
 - `https://<SERVER_1_FQDN>:31101/runtimeconfig`
- For Voice:
 - `https://<SERVER_1_FQDN>:31000/runtimeconfig`
 - `https://<SERVER_1_FQDN>:31001/runtimeconfig`

Configuring the WebLM URL Address

Procedure

1. Log in to the OD Runtime Config for the Voice OD Module via browser. The username is ddadmin and default password is ddadmin.
2. You may receive a notification to change the default password.
3. After you are logged in, click **License Server**, on the left menu.

The screenshot shows the Avaya Orchestration Designer web interface. At the top left is the Avaya logo. At the top right, it says "Welcome, ddadmin" and "Last logged in Mon Oct 08 14:31:41 GMT 2018". Below the header is a red navigation bar with "Orchestration Designer 07.20.09.04" and a "Logoff" button. The main content area has a left sidebar with a menu: "License Server", "Connectivity Settings", "Certificates", "AES", "IR Channel Map", "IC Common", "IC VOX", "IC VRUSM/HTTPVOX", "Users", and "Application Configuration". The "License Server" menu item is selected. The main content area is titled "Licensing Server" and contains the following text: "Enter the URL to the license server host. For example http://myhost:8080/. If you leave the license URL blank, the license server the VPMS uses, will be used for Orchestration Designer licensing (Voice Portal only)." Below this text are two input fields: "License URL:" and "License Check Timeout: 0". There is a "Verify" button next to the "License URL:" field and an "Update" button below the "License Check Timeout:" field. At the bottom of the form, it says "License URL empty, using URL supplied by the VPMS".

Figure 13: Licensing server

4. In the **License URL**, enter the WebLM URL you want to use.
5. Click **Update**.

6. Restart the OD Services.

- **Note:**
Remember to run these steps on the other ports too.

Upgrade Cluster Deployments

Upgrade from Previous Versions

- **Important:**
Upgrade from 4.0.x releases is not supported.

Upgrade from 4.1 Versions

When upgrading from Survey Assist Release 4.1 or any 4.1.x release, the process automatically identifies the version, upgrades the software and maintains all existing data.

- **Important:**
Before upgrading, we strongly recommend taking a snapshot from each node (master and workers).

Upgrade Steps

Unpacking the Distribution Bundle

Procedure

1. Decompress the file at `/tmp/survey-installer/`. This directory is `<INSTALL_DIR>`

```
mkdir /tmp/survey-installer/
```

```
tar -vxf omsurvey-bundle-cluster-4.2.0.tar.gz -C /tmp/survey-installer/
```

- **Note:**
On Cluster deployments, download the bundle and decompress it on the first VM that becomes the Master Node.

Upgrade

About this task

All steps are performed from the installer path (INSTALL_DIR).

Procedure

1. Navigate to the installation root directory
2. If upgrading from 4.1.x releases, then run this command on each node:
 - a. Copy the Docker Daemon file and script to the other two Survey Assist nodes by running these commands:

```
scp docker/docker-configure-daemon.sh survey@<NODE_IP>:/tmp/
scp docker/daemon.json survey@<NODE_IP>:/tmp/
```

 - Note: Repeat this step for each secondary server
 - b. On MASTER, run the following command to update the daemon.json file:

```
./docker/docker-configure-daemon.sh
```
 - c. On each of the Nodes, run the following command to update the daemon.json file:

```
cd /tmp/
./docker-configure-daemon.sh
```
3. Run the install.sh script

```
./install.sh
```
4. After running the install script, you must accept the End User License Agreement (EULA)
5. Wait until the upgrade finishes

Sample logs

- Success example:

```
[root@survey50-ubum installer]# ./install.sh
*****
****

Survey Assist 4.2.0 Installer Tool
*****
****

Setting sh files as executables
Mon Sep  9 14:36:39 EDT 2019 - --- Load Survey Script Variables ---
Mon Sep  9 14:36:39 EDT 2019 - Setting global variables...
```

```

...
Mon Sep  9 14:36:39 EDT 2019 - ---. Loading Survey Script Variables:
SUCCESS
--- Check Preconditions ---
(14:36:39) Checking User privileges...
(14:36:39) Checking Hostname...
...
Current Docker version: 17.03.2-ce
(14:36:39) Checking if Docker daemon.json file is correctly
configured...
--- Checking preconditions: SUCCESS
--- EULA Acceptance ---
...
Do you accept the End User License Agreement? [yes/no]:
--- End User License Agreement Accepted: SUCCESS
--- Check installed version ---
Already installed Survey version      : 4.1.5
Running installer for Survey version : 4.2.0
--- A lower version of Survey is already installed: SUCCESS
upgrade
*** Upgrading into Survey Assist [4.2.0] ***
Mon Sep  9 14:36:43 EDT 2019 - Current version: 4.1.5
Mon Sep  9 14:36:43 EDT 2019 - Installation mode: cluster
Mon Sep  9 14:36:43 EDT 2019 - Docker repository: survey50-
ubum.avaya.arg.lab:8999
...
(15:00:21) Removing configuration file...
*** [ Installation SUCCESS ] ***

```

- Failure example:

```

...
*** Upgrading into Survey Assist [4.2.0] ***

```

```
Mon Sep 9 14:35:50 EDT 2019 - Current version: 4.1.5
Mon Sep 9 14:35:50 EDT 2019 - Installation mode: cluster
Mon Sep 9 14:35:50 EDT 2019 - Docker repository: survey50-
ubum.avaya.arg.lab:8999
...
---. There was an error during the upgrade: ERROR
*** [ Installation ERROR ] ***
```

- **Important:**

If an error occurs, restore the nodes with the snapshots taken previously and send the logs to the support team.

Chapter 5: Installing Breeze Snap-in

This chapter is to be referred when installing Survey for Oceana Integration OR for AACC Integration.

Snap-in Installation

Loading the snap-in

This task describes how to load a snap-in to System Manager from your development environment or alternate location

Procedure

1. On the System Manager web console, click **Elements** → **Avaya Breeze**.
2. In the left navigation pane, click **Service Management**.
3. Select **Services** and click **Load**.
4. On the Load Service page, click **Browse** and go to the snap-in file location.
In this case, the file is located in <INSTALL_DIR>/breeze/survey-redirection-1.0.0.1.00000000.svar
5. Click **Open**.
6. On the Load Service page, click **Load**.
The **survey-redirection** snap-in displays on the Service Management page with a **State of Loaded**.

Installing the snap-in

Procedure

1. On System Manager web console, click **Elements** → **Avaya Breeze**.
2. In the left navigation pane, click **Service Management**.
3. Select **Services**
4. Select the **survey-redirection** snap-in.
5. Click **Install**.
6. Select the cluster where you want the snap-in to reside and click **Commit**.
7. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.

- Note:

Installed with a green check mark indicates that the snap-in has completed installation on all Breeze Platform servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed the installation on all the servers.

8. To track the progress of a snap-in installation, on the Server Administration page, click the **Service Install Status** for Breeze Platform Server.

The system displays the Service Status page with the installation status of all the snap-ins installed on that server.

Snap-in Configuration

Snap-in attributes

Procedure

1. On System Manager web console, navigate to **Home** → **Elements** → **Avaya Breeze** → **Configuration** → **Attributes**.
2. On the **Service Globals** tab, select **survey-redirectation** from the drop-down list.
3. Complete the **DNIS:Survey Mapping** field with one or more pair of:
 - a. **DNIS**: the Oceana Ingress VDN (DNIS) OR the AACC CDN (DNIS) handling incoming calls.
 - b. **Survey Mapping**: the DNIS/VDN/Route that will launch the Survey application in AAEP (Survey Mapping);

- **Note:**

More than one DNIS:Survey Mapping can be added. Separate them by comma (",").

Examples.:

- Oceana: If the Ingress VDN is 6009981 and the DNIS reaching AAEP is 6054002, set **DNIS:Survey Mapping** to **6009981:6054002**
 - AACC: if the AACC CDN is 800449887 and the DNIS reaching AAEP is 5000, set **DNIS:Survey Mapping** to **800449887:5000**
4. Complete **Lab Domain** with the domain used in the environment; e.g.: **avaya.com**
 5. The remaining parameters are not used.

Service Profiles | Service Clusters | **Service Globals**

Service:

DEFAULT_GROUP

7 Items

Name	Override Default	Effective Value	Description
Customer Dial back Enabled	<input type="checkbox"/>	false	Customer dial out to take the survey enabled
DNIS:Survey Mapping	<input checked="" type="checkbox"/>	<input type="text" value="6009981:6054002"/>	DNIS:Survey Mapping creates one to one mapping for each DNIS to each external Survey
Endpoint Extension	<input type="checkbox"/>	15040	Endpoint Extension for initiating calls
Lab Domain	<input checked="" type="checkbox"/>	<input type="text" value="avaya.lab"/>	Lab Domain for endpoint extensions
Play Prompt to Customer	<input type="checkbox"/>	false	Play prompt to Customer for Survey
Survey Prompt	<input type="checkbox"/>	Would you like to participate in a post call Survey? Press one for yes or zero for no	Survey Prompt to be played to ask customer to participant in Survey
Survey Prompt Percentage	<input type="checkbox"/>	100	Percentage of Calls to be Prompted for Survey (numeric value from 0 to 100)

Figure 14: Attributes Configuration

6. Click **Commit**.

Sequencing the DNIS for Survey Redirection

Service Profile in Avaya Breeze for Survey Redirection Snap-in

Before you begin

Create a Service Profile (e.g: SurveyRedirectionProfile) in Avaya Breeze section for the Survey Redirection snap-in. Any sequence intercepted by this service invokes Survey Redirection snap-in (**survey-redirection**).

Procedure

1. On System Manager web console, navigate to Home → Elements → Avaya Breeze → Configuration → Service Profiles.
2. Click **New**.
3. Set **Name** and **Description**, e.g: SurveyRedirectionProfile.

4. Add **survey-redirection** to the **Services** in the Service Profile.
5. Click **Commit**.

Implicit User Profile in Avaya Breeze for Survey Redirection Snap-in

Procedure

1. On System Manager web console, navigate to Home → Elements → Avaya Breeze → Configuration → Implicit User Profile
2. Click **New**.
3. Select previously created profile: SurveyRedirectionProfile.
4. Set **Pattern** to the incoming DNIS that is being used. This can be a pattern if there are more than one DNIS.
5. Set **Min** and **Max** to adjust to the Pattern.
6. Enter description (OPTIONAL).
7. Click **Commit**.

Create Application in Session Manager for Survey Redirection Snap-in

Procedure

1. On System Manager web console, navigate to Home → Elements → Session Manager → Application Configuration → Applications
2. Click **New**.
3. Enter Name: SurveyRedirectionApplication
4. On SIP Entity, select Breeze Cluster where the snap-in was installed.
5. Click **Commit**.

Create Application Sequence in Session Manager for Survey Redirection Snap-in

Procedure

1. On System Manager web console, navigate to Home → Elements → Session Manager → Application Configuration → Application Sequences
2. Click **New**.
3. Enter Name: SurveyRedirectionSequence

4. Add application created on previous step.
5. Click **Commit**.

Create Implicit User dial pattern in Session Manager for the Inbound DNIS

Before you begin

Create an Implicit User dial pattern in Session Manager section for the inbound DNIS to be sequenced to Avaya Breeze. This dial pattern represents the inbound DNIS sequenced to the Avaya Breeze only for the termination that is, where the dialed number or the called party matches this sequence. This is set only for the termination because these DNIS are Inbound.

Procedure

1. On System Manager web console, navigate to Home → Elements → Session Manager → Application Configuration → Implicit Users.
2. Click **New**.
3. Set **Pattern** to the incoming DNIS that is being used. This can be a pattern if there are more than one DNIS.
4. Set **Min** and **Max** to adjust to the Pattern.
5. SIP Domain: ALL or select the one being used.
6. Set **Termination Application Sequence** to **SurveyRedirectionSequence**.
7. Click **Commit**.

Implicit User Rule Editor Commit Cancel

Implicit User Rule

*Pattern

*Min

*Max

Description

SIP Domain

Origination Application Sequence

Termination Application Sequence

Emergency Origination Application Sequence

Emergency Termination Application Sequence

***Required** Commit Cancel

Figure 15: Implicit User Rule

Chapter 6: Installing AACC CCT Connector Service

This chapter is to be referred when installing Survey for AACC Integration.

CCT Connector Service Installation

Installing the service

This task describes how to install the CCT Connector in the provided Microsoft Windows virtual machine.

Procedure

1. Log in with an Administrator account to Microsoft Windows virtual machine.
2. Copy CCTConnectorService_4.2.0_15.zip file from Survey Assist bundle under directory <INSTALL_DIR>/cct-service.
3. Extract zip file to the installation directory of your choice.
4. In order to register the CCT Connector as Windows Service, run the install.bat file.
5. Go to Start button → Administrative Tools → Services
6. Check that the service AACC AAT CCT Connector is listed.
7. Start the service.

Configuring the service

This task describes how to configure the CCT Connector in the provided Microsoft Windows virtual machine in order to monitor AACC calls and publish information to Survey Assist application.

Procedure

1. Log in with an Administrator account to Microsoft Windows virtual machine.
2. Go to CCTConnectorService installation directory.
3. Open file WinService.exe.config with text editor of your choice.
4. There are two sections to configure:
 - a. ApplicationSettings

Tag	Attribute	Description	Default value
-----	-----------	-------------	---------------

CCTServer	Ip	AACC CCMS server IP	
CCTServer	port	TCP port	29373
CCUser	username	Service CCT user name	
CCUser	domain	Service CCT User Windows domain (server name if user is not a domain user)	
CCUser	password	Service CCT user password encrypted (see below)	

b. AgentActivityTrackerSettings

Tag	Attribute	Description	Default value
Breeze	Ip	Survey Assist server IP	
Breeze	port	Survey Assist HTTPS port	443
Breeze	Path	Survey Assist Open Cache API path	/api/v1/cache/path
Breeze	Secure	True if using HTTPS or false for HTTP	true
Breeze	cert_check	Check certificate domain	false
Breeze	username	Survey Assist username	
Breeze	password	Survey Assist password encrypted (see below)	

5. Save the file.
6. Restart the service.

Sample configuration file:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="ApplicationSettings" type="CCTConnector.Common.Settings.ApplicationSettings, CCTConnector.Common"/>
    <section name="AgentActivityTrackerSettings" type="AgentActivityTrackerAddIn.Settings.AgentActivityTrackerSettings, AgentActivityTrackerAddIn"/>
  </configSections>
</configuration>
```

```

</configSections>

<startup>
  <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4
.6.2"/>
</startup>

<ApplicationSettings>
  <CCTServer ip="127.0.0.1" port="29373" campus="" geographic=""
/>
  <CCTUser username="Administrator" domain="AACC703" password="E
NC(MwXUabKHvCZMwgMiGQDzcg==)" />
</ApplicationSettings>

<AgentActivityTrackerSettings>
  <!-- PONTING TO THE OPEN-CACHE MOCK -->
  <Breeze ip="135.20.201.34" port="443" path="/api/v1/cache/" se
cure="true" username="user" password="ENC(tIjPMpD/+IEGOD4DcirChQ==)" c
ert_check="false"/>

</AgentActivityTrackerSettings>
</configuration>

```

Password Encryption

About this task

Data encryption is performed by using AES cipher. For interactive encryption of passwords, the `PasswordEncryptor.exe` utility is used.

To create and use an encrypted password, follow the below procedure.

Procedure

1. Launch `PasswordEncryptor.exe` utility located in the installation directory.
2. Enter password you want to encrypt and follow the wizard instructions.

Example:

```
Type password and press Enter
```

secret-value

Please copy the following string to config file:

```
ENC(zY1WszGpHbj2IxFMaLsx8w==)
```

Press Enter to exit...

3. Copy the output to the password/s field in WinService.exe.config file.
4. Save your changes and close the file.
5. Restart the service.

Chapter 7: Regenerating and reimporting certificates

Before you begin

In case of having changes applied to product certificates or Survey certificate expiration, run the following steps to regenerate and reimport the certificates.

This is a **service affecting** process:

- Single-Box: every service will be re-started.
- Cluster: every service affected by the changing certificates, will be re-started.

Procedure

1. Navigate to the directory `/opt/avaya/survey/regenerate-certificates`
2. Set the `certificates.properties` file with environment details.
3. Run `regenerate-certificates.sh` script.

This creates new certificates under `/opt/avaya/survey/regenerate-certificates/autogenerated_certificates` directory.

4. Run `update-certificates.sh` to apply the new certificates on the system. This script receives one argument, the certificate to apply:

```
update-certificates.sh:usage:
```

```
[-smgr] to update certificate from smgr.
```

```
[-weblm] to update licensing certificate.
```

```
[-aes] to update aes certificates.
```

```
[-integrations] to update integrations certificates (POM, Oceana).
```

```
[-survey] to update internal services certificates.
```

```
[-all] to update all certificates.
```

- **Note:**

In case of '-survey' or '-all' execution, follow these two indications sets in Chapter 4, Post-Installation Steps:

- [Adding a certificate to the System Manager](#) (replacing `myserver.crt`)
- [Importing Survey Assist certificates into the Experience Portal](#)

Chapter 8: Update Credentials

System Manager Credentials

About this task

Use this procedure to update Survey Assist's System Manager user credentials

Procedure

1. Navigate to the directory `/opt/avaya/survey/installer/support/`
2. Run `update-smgr-credentials.sh` script, passing the user name and password as parameters

```
./update-smgr-credentials.sh <username> <password>
```

E.g.:

```
./update-smgr-credentials.sh surveyservices admin-smgr-pass
```

- **Note:**

If the username or the password includes characters like `*`, `$` or spaces, you should use single quotes when defining it.

E.g: `./update-smgr-credentials.sh 'u$er' 'pa$$'`

POM Credentials

About this task

Use this procedure to update Survey Assist's POM user credentials

Procedure

1. Navigate to the directory `/opt/avaya/survey/installer/support/`
2. Run `update-pom-credentials.sh` script, passing the user name and password as parameters

```
./update-pom-credentials.sh <username> <password>
```

E.g.:

```
./update-pom-credentials.sh surveypom pom-ws-pass
```

- **Note:**

If the username or the password includes characters like `*`, `$` or spaces, you should use single quotes when defining it.

E.g: `./update-pom-credentials.sh 'u$er' 'pa$$'`

Chapter 9: Troubleshooting

Log files

Collecting Log files

Survey Assist provides a script for collecting and compressing the log files.

Procedure

1. Navigate to the directory `/opt/avaya/survey/installer/support/`
2. Run `collect-logs.sh` script

```
./collect-logs.sh
```
3. Log files are compressed into a `tar.gz` file located in the `/opt/avaya/survey/logs/` directory. Each file will be named `logs-YYYY-MM-DD-hh-mm-ss.tar.gz`, where `YYYY-MM-DD-hh-mm-ss` indicates the year, month, day, hour, minutes and seconds of the time the script was ran.

Log files description

File Name	Location	Created on	Purpose
<code>omsurvey-installation.log</code>	<code>/tmp/omsurvey/</code>	Installation	Includes the information displayed during installation
<code>start-survey-on-reboot.log</code>	<code>/opt/avaya/survey/logs/</code>	Operation	Logs with information regarding cron restarts
<code>admin-rest-api.log</code>	<code>/opt/avaya/survey/docker_volumes/logs</code>	Operation	Administrarion API logs
<code>auth-rest-api.log</code>	<code>/opt/avaya/survey/docker_volumes/logs</code>	Operation	Authentication Service logs
<code>configuration-init.log</code>	<code>/opt/avaya/survey/docker_volumes/logs</code>	Installation	Content is generated during

File Name	Location	Created on	Purpose
			internal configuration initialization
core-execution-rest-api.log	/opt/avaya/survey/docker_volumes/logs	Operation	Survey execution log
licensing-rest-api.log	/opt/avaya/survey/docker_volumes/logs	Operation	License service log
mail-sender-rest-api.log	/opt/avaya/survey/docker_volumes/logs	Operation	email Service log
media-cache-rest-api.log	/opt/avaya/survey/docker_volumes/logs	Operation	Media cache Service log
notification-rest-api.log	/opt/avaya/survey/docker_volumes/logs	Operation	Notification engine log
storage-rest-api.log	/opt/avaya/survey/docker_volumes/logs	Operation	Data Access log
omsurvey-od-application.log	/opt/avaya/survey/docker_volumes/od/sms/logs and/or /opt/avaya/survey/docker_volumes/od/voice/logs	Operation	Application runtime log
omsurvey-od-context.log	/opt/avaya/survey/docker_volumes/od/sms/logs and/or /opt/avaya/survey/docker_volumes/od/voice/logs	Operation	Application start-up log

Survey services

List of services

The following is a list of all the services which are part of Survey Assist

Service	Provided Functionality
licensing-rest	Licensing related functionality

Service	Provided Functionality
storage-rest	Data access functionality
admin-rest	Administration and Configuration functionality
auth-rest	Authentication and Validation functionality
media-cache-rest	Media caching
core-execution-rest	Functionality required for survey offering execution
Ui	Web User Interface for administration and configuration
od-sms	SMS survey offering application for AAEP
od-voice	Voice survey offering application for AAEP
kafka	Kafka service
database	Database service
zookeeper	Service registry and distributed configuration
redis	Distributed cache
notification-rest	Notification evaluation functionality
mail-sender-rest	email functionality

Service commands

The following commands are available to be used from the command line:

Command	Used for
service survey status	Provide the status of all the Survey services. Status may be "RUNNING" or "STOPPED"
service survey stop	Stops all the services
service survey start	Starts all the services
service survey restart	Stops and then Starts all the services
service survey help	Provides information of the commands available

Common issues

Symptom	Solution
Cannot connect to the UI	Make sure port 443 is open in the firewall.
Cannot verify OD apps from AAEP	Make sure ports 9080 and 9180 are open in the firewall.

Chapter 10: Security

Firewall Logs

Enabling Firewall Denied Logs

About this task

With the LogDenied option in the firewall, it is possible to add a simple logging mechanism for denied packets.

The default setting is off, and the possible values for this setting are: all, unicast, broadcast, multicast, and off

Procedure

1. Check firewall denied-log configuration

```
firewall-cmd --get-log-denied
```

2. If the setting is off, set this as all using this command:

```
firewall-cmd --set-log-denied=all
```

Displaying Firewall Denied Logs

You can display the denied logs by using:

```
sudo cat /var/log/messages | grep FINAL_REJECT
```

Sample Log

For this sample we tried to access a closed port: 9999, and these are the REJECTED logs

```
Aug 26 10:23:39 omsurvey-server kernel: FINAL_REJECT: IN=ens192 OUT=
MAC=00:52:56:a6:c6:c2:3c:b1:5b:f3:b4:ae:08:00 SRC=135.105.193.51
DST=10.133.31.10 LEN=52 TOS=0x00 PREC=0x00 TTL=116 ID=9937 DF
PROTO=TCP SPT=52335 DPT=9999 WINDOW=65280 RES=0x00 SYN URGP=0
```

Encryption Algorithms

Encryption Algorithms used for credentials

The algorithm used to encrypt/decrypt credentials is: **Advanced Encryption Standard (AES) 256 bits.**

User Profiles

Avaya User Profiles matching

The following table describes the matching between Avaya User Profiles and Survey Assist Users

Avaya Profile	Survey Assist
Auditor	Not Available
Security Administrator	Covered by default users with EASG access to Survey Assist's servers.
FIPS140-2 Crypto Officer	Covered by default users with EASG access to Survey Assist's servers.
Backup Administrator	Not Available
Avaya Services Administrator	Covered by default users with EASG access to Survey Assist's servers.
Avaya Services Maintenance and Support	Covered by default users with EASG access to Survey Assist's servers.
Application Administrator	Users with Survey System Administrator role in System Manager.
System Administrator	Covered by default users with EASG access to Survey Assist's servers.

ROOT privileges

Components running with root user

For specific conditions, there are certain internal components running with root access privileges as part of the Survey Assist solution, and only in the Survey Assist Servers

Auditing file changes

Linux provides a service to log file changes and track security-relevant information on the system, the Linux Audit system. Installing and enabling the service (auditd) would allow tracking changes made to the Survey Assist system or any file in the Linux file system.

This is an optional feature that must be enabled manually, this document provides a basic guide to add files to the Linux Audit system, which generates log entries to record the events that are happening on your system. This information is useful to determine violations of the security policies and tracking security-relevant information on your system.

Using the auditd service to log file changes

Checking if the auditd service is installed

To check if the service is installed execute the following command:

```
$ systemctl list-unit-files | grep enabled | grep auditd.service
```

If the service is installed next line will be outputted by the command:

```
auditd.service                               enabled
```

If the service is not installed, it can be installed with the following command:

```
$ yum install audit
```

- **Note:**

This procedure requires the server to have access to internet

Enabling the service

After enabling the service, run the following command to check that a symlink is created and the service will be started on every reboot:

```
$ ls -lha /etc/systemd/system/multi-user.target.wants/auditd.service
```

This will output the symlink as follows:

```
lrwxrwxrwx 1 root root 38 Sep  4 12:11 /etc/systemd/system/multi-  
user.target.wants/auditd.service ->  
/usr/lib/systemd/system/auditd.service
```

Starting the service

To start the service run the following command:

```
$ systemctl start auditd.service
```

After starting the service, check if the service is running:

```
$ systemctl status auditd.service
```

The output from the previous command is the service status, for example:

```
● auditd.service - Security Auditing Service  
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled;  
   vendor preset: enabled)  
   Active: active (running) since Tue 2019-08-20 16:31:25 EDT; 2 weeks  
     0 days ago  
     Docs: man:auditd(8)  
           https://github.com/linux-audit/audit-documentation  
   Main PID: 5517 (auditd)  
     Tasks: 2  
    Memory: 37.7M  
    CGroup: /system.slice/auditd.service  
            └─5517 /sbin/auditd
```

The line with the "Active" legend should display the service in the running state.

Adding file system rules

To log file changes is necessary to add file system rules, by adding them to a file or by executing a command using the following syntax:

```
$ auditctl -w path_to_file -p permissions -k key_name
```

Example:

Adding a file system rule to log all write access and attribute changes on the "/etc/passwd" file.

```
$ auditctl -w /etc/passwd -p wa -k passwd_changes
```

Where "passwd_changes" is the key name, "/etc/passwd" is the path to the file

Command syntax:

```
$ auditctl -w path_to_file -p permissions -k key_name
```

Where:

- path_to_file is the file or directory that is audited.
- permissions are the permissions that are logged:
 - r — read access to a file or a directory.
 - w — write access to a file or a directory.
 - x — execute access to a file or a directory.
 - a — change in the file's or directory's attribute.
- key_name is an optional string that helps you identify which rule or a set of rules generated a particular log entry.

The auditctl command does not make persistent changes, the configurations will not be available after a system reboot. The next section shows how to make the changes persistent.

Persisting the rules after a reboot

In order to save the rules and have them loaded every time the system is restarted the rules need to be added to a file with ".rules" extension. The file could be either the global rules configuration file "/etc/audit/rules.d/audit.rules" or a file added in the "/etc/audit/rules.d/" directory.

For example, to add the rule for the "/etc/passwd" file, the following line should be added to a file, which will be located in the "/etc/audit/rules.d/" directory under the name "30-survey.rules". The file contents will be just one line:

```
-w /etc/passwd -p wa -k passwd_changes
```

This is similar to the parameters of the command previously mentioned to add the rule:

```
$ auditctl -w /etc/passwd -p wa -k passwd_changes
```

Loading the rules in the file

After the rules have been added to the file, the "augenrules" command must be executed, it will merge all the rules files in the "/etc/audit/rules.d/" directory, into the file "/etc/audit/audit.rules", and it will load the rules.

```
$ augenrules --load
```

Removing a file system rule

To remove a persistent rule, it must be removed from the rules file, and then the rules have to be reloaded with the following command:

```
$ augenrules --load
```

If the rule has not been persisted, it can be removed using just the auditctl command. To list the loaded rules, use:

```
$ auditctl -l
```

This will output the loaded rules in the following way:

```
-w /etc/passwd -p wa -k passwd_changes
```

To remove the rule, use the following command:

```
$ auditctl -W /etc/passwd -p wa -k passwd_changes
```

Notice that the letter W is in uppercase, that is the only difference to the output from the invocation to "auditctl -l" and will cause the removal of the rule.

An option to disable a persistent rule temporarily is commenting out the line with a "#" character and then running the "augenrules --load" command.

Verify that the changes are logged

There are specialized tools to navigate the log files produced by the auditd service, but a quick way to check if the rules are being applied is to use the following commands after modifying file being tracked:

```
$ tail -n 200 /var/log/audit/audit.log | grep /etc/passwd
```

Where "/etc/passwd" should be replaced by the name of file being tracked and "-n 200" is used to specify the number of lines (200 in this example) that should be read from the audit log file, "/var/log/audit/audit.log".

The output lines containing the `"/etc/passwd"` string will show the file changes logged.

Appendix I

Related resources

The following table lists the documents related to Avaya Survey Assist. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Use this resource to:	Audience
Maintenance		
<i>Administration and Configuration Guide</i>	Configure the admin part of the Survey Assist product.	System administrators or support personnel.
<i>Hardware and Software Specifications Guide</i>	Configure the Survey Assist hardware and software requirements during deployment.	

Appendix II

System Manager Trust Management

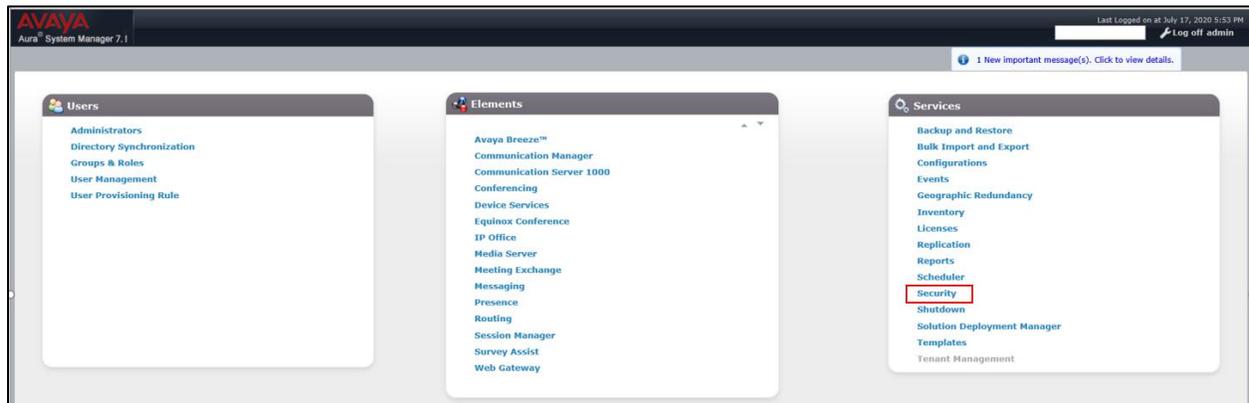
Using Avaya Aura System Manager (SMGR) as a Certificate Authority (CA) to generate signed certificates, follow next steps on how to use System Manager's Trust Management feature as your PKI.

Create an "End Entity Profile" for the Survey server

Procedure

Go to Home > "Security" > "Certificates" > "Authority" > "End Entity Profiles":

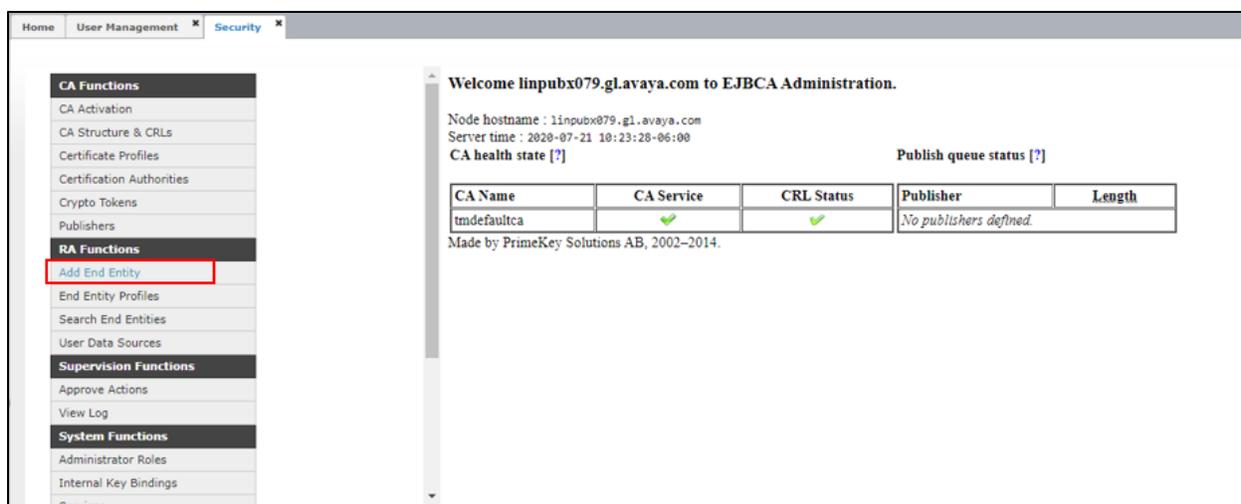
Using the SMGR web console, navigate to "Security" (under Services)



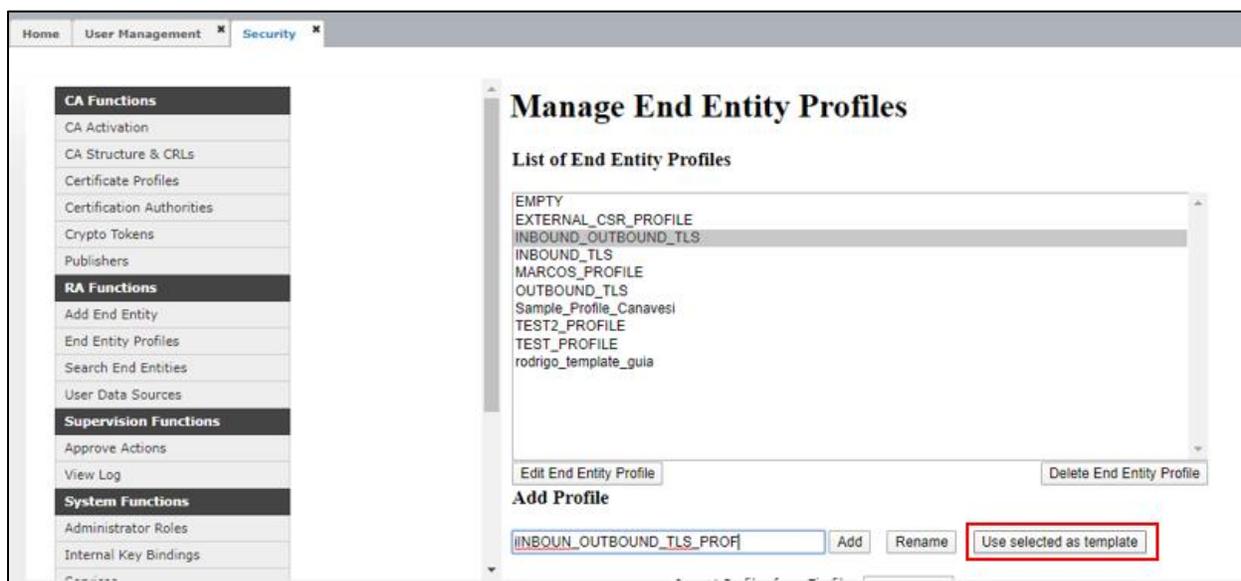
Then click the "Authority" button (under "Certificates")



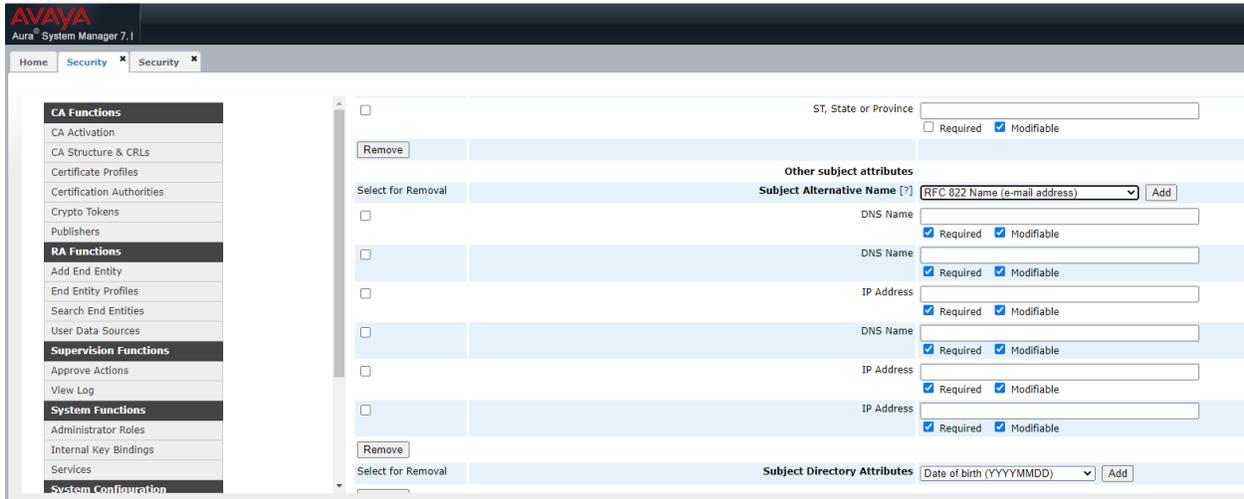
Then click "End Entity Profiles" (under RA functions).



1. Create new Profile:
 - a. Select profile -> INBOUND_OUTBOUND_TLS
 - b. Add Profile:
 - Profile_Name = YOUR_PROFILE_NAME
 - Click on "Use selected as template"



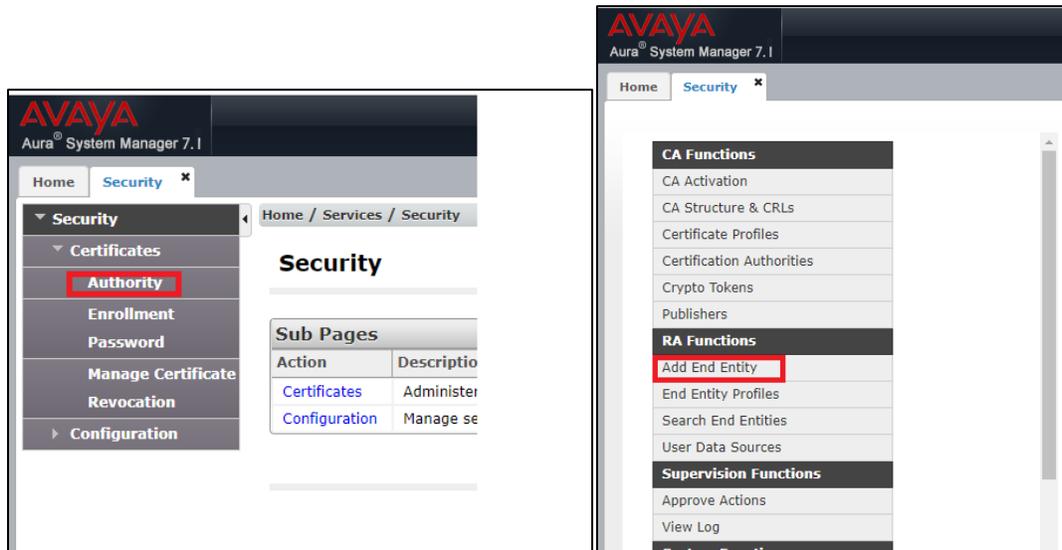
2. Edit Profile: **This step is required for Cluster Survey Assist installations and must be ignored for Single Box installations.**
 - a. Select profile -> YOUR_PROFILE_NAME
 - b. Click on "Edit End Entity Profiles"
 - c. Check require and modifiable for three fields with the name "IP Address" and "DNS Name" on "Other subject attributes". These items are required (**you will have 3 of each in total**). You could also add the DNS Names and the IP Addresses in the profile although those will change with every End Entity created with the profile.
 - d. Scroll down and click the Save button.



Create an “End Entity” for the Survey server

Procedure

Using the SMGR web console, navigate to “Security” (under Services) > “Certificates” > “Authority” > “Add End Entity” (under RA functions).



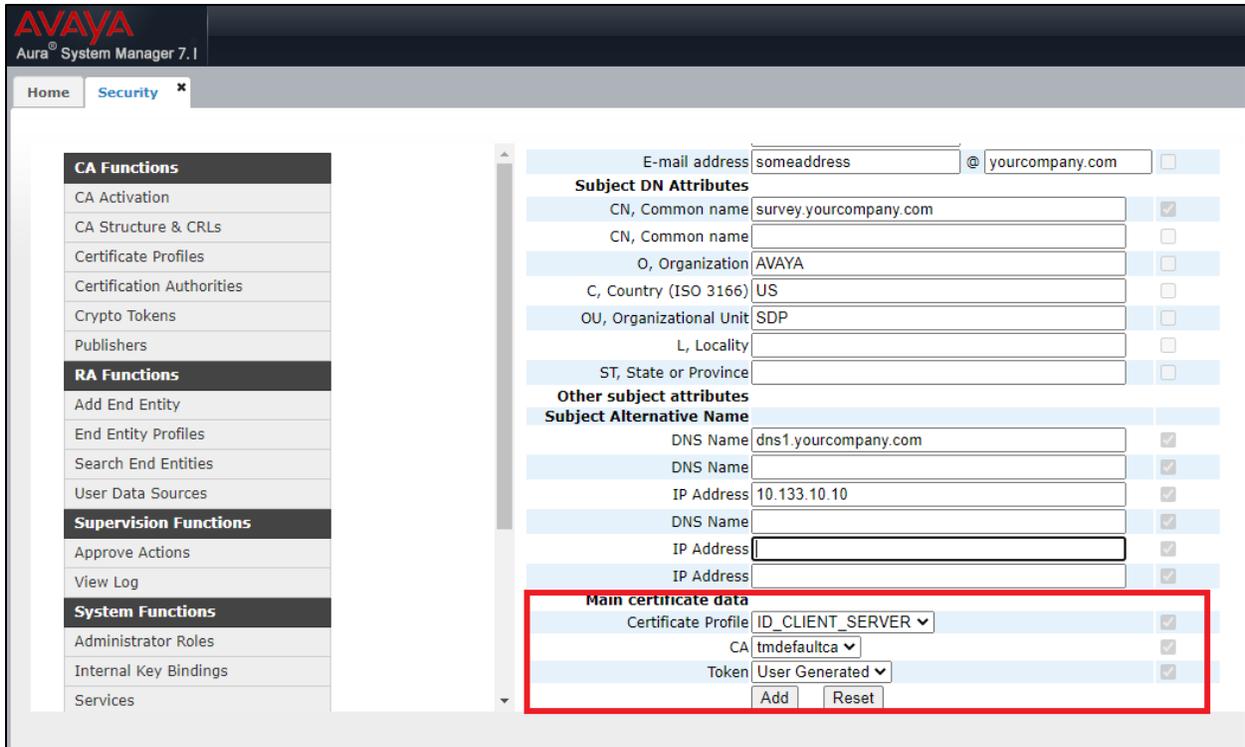
1. In the “End Entity Profile” field, click YOUR_PROFILE_NAME.
2. Type a username and password. This password is used to encrypt the P12 trust store file (see below). Make sure you remember the username and password, you will need those later.
3. Complete the fields that you want in your certificate
 - a. E-mail address: labmanager@yourcompany.com (choose an e-mail)
 - b. CN, Common name: survey.yourcompany.com (Required)
 - c. OU, Organizational Unit: IT

- d. O, Organization: Your Company Name
- e. L, Locality: Denver
- f. ST, State or Province: CO
- g. C, Country: US

The screenshot shows the Avaya System Manager 7.1 interface. On the left is a navigation menu with categories: CA Functions, RA Functions, Supervision Functions, and System Functions. The 'Add End Entity' form is the main focus, highlighted with a red border. It contains the following fields:

Field	Value	Required
End Entity Profile	TEST_PROFILE	Required
Username	someuser	<input checked="" type="checkbox"/>
Password (or Enrollment Code)	*****	<input checked="" type="checkbox"/>
Confirm Password	*****	
E-mail address	someuser @ yourcompany.com	<input type="checkbox"/>
Subject DN Attributes		
CN, Common name	dns1.yourcompany.com	<input checked="" type="checkbox"/>
CN, Common name		<input type="checkbox"/>
O, Organization	AVAYA	<input type="checkbox"/>
C, Country (ISO 3166)	US	<input type="checkbox"/>
OU, Organizational Unit	SDP	<input type="checkbox"/>
L, Locality		<input type="checkbox"/>
ST, State or Province		<input type="checkbox"/>
Other subject attributes		
Subject Alternative Name		
DNS Name	dns1.yourcompany.com	<input checked="" type="checkbox"/>
DNS Name		<input type="checkbox"/>
DNS Name		<input type="checkbox"/>
IP Address	10.133.10.10	<input checked="" type="checkbox"/>

4. Complete the DNS and IP Address for each of the Survey Assist servers (**1 for Single Box, 3 for Cluster installations**)
5. In the "Certificate Profile" drop down menu select ID_CLIENT_SERVER
6. In the "CA" drop down menu select "tmdefaultca"
7. In the "Token" drop down menu select "P12 file"



8. Click **Add** button.

Note:

On the top of the page the system displays the message **End Entity added successfully**.

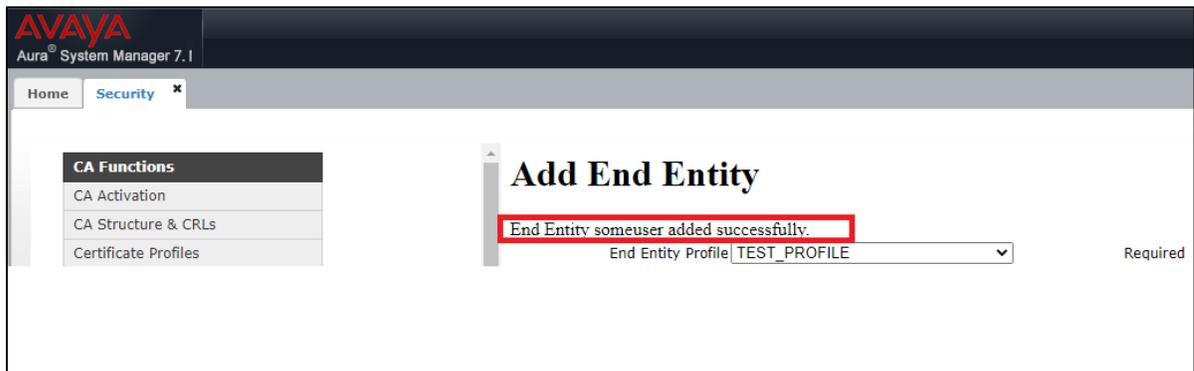
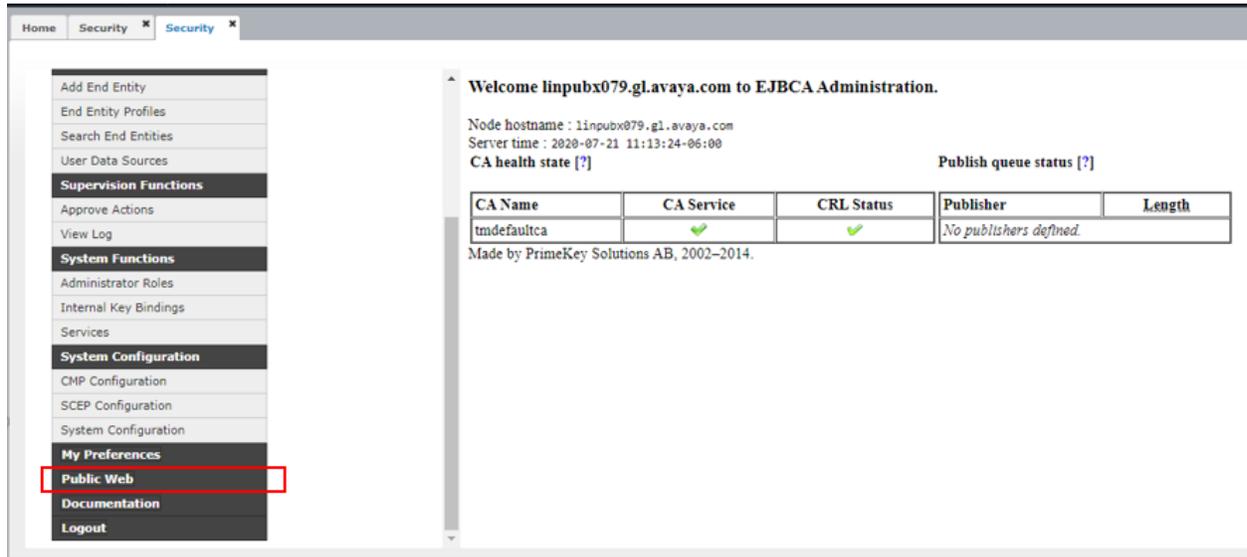


Figure 16: Adding End Entity

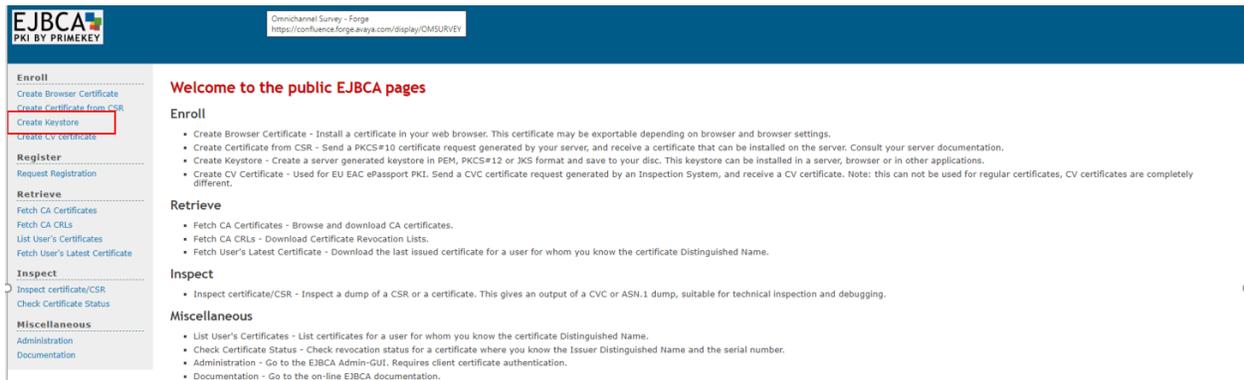
Create the keystore

Procedure

1. Using the SMGR web console, navigate to “Security” (under Services) > “Certificates” > “Authority”.



2. In the left-hand navigation pane near the bottom of the screen, click on “Public Web”. A new window will open.
3. On the “Public Web” screen click on “create key store”



4. Enter the username and password previously defined while *Creating the End Entity* and click “OK”
 - a. Select the certificate key length 2048
 - b. Click on “Enroll”
 - c. Save the server certificate to a known location

- **Note:**

This is the keystore in P12 format you will use on Survey installation.

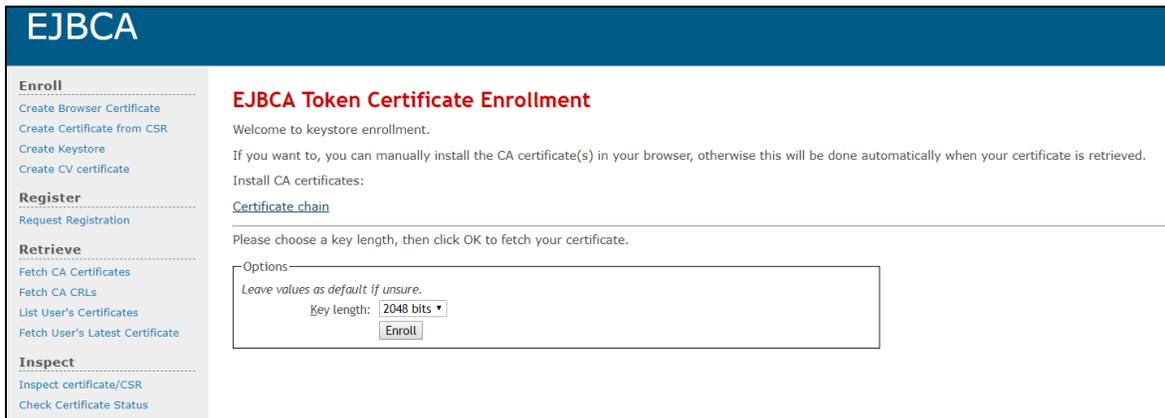


Figure 17: EJBCA Token Certificate Enrollment

Change keystore alias

Procedure

In order to use the keystore for the Survey installation, you need to complete these steps:

1. Copy the file you downloaded in the “Create keystore” step to the Survey box (to the master server if it is a cluster installation)
2. Change the alias by running the following command:


```
keytool -changealias -alias <DEFAULT_CN> -destalias
"survey-https" -keystore /path/to/<USERNAME>.p12 -storepass
<PASSWORD>
```
3. Replacing:
 - a. <DEFAULT_CN> with the “CN, Common Name” value, as it was defined in the “Add End Entity” step, while generating the keystore.
 - b. <USERNAME> with the username you defined in the “Add End Entity” step, while generating the keystore.
 - c. <PASSWORD> with the password you defined in the “Add End Entity” step, while generating the keystore.

Change keyStore password

Procedure

1. Change the password by running the following command:

```
keytool -noprompt -importkeystore -deststorepass changeit -
destkeypass changeit -destkeystore server-new.p12 -srckeystore
```

```
<YOUR_KEYSTORE_FILE.p12> -srcstorepass <YOUR_KEYSTORE_PASS> -  
srcstoretype PKCS12 -deststoretype PKCS12
```

2. **Note:** Replace in the above command

<YOUR_KEYSTORE_FILE.p12> with the complete path of the provided keyStore.

<YOUR_KEYSTORE_PASS> with the password of the provided keyStore

This command generates a new p12 file which is to be used on the **configuration.properties** file specifying:

<KEYSTORE_PATH> the path of the new file "*server-new.p12*"

<KEYSTORE_PASS> as "*changeit*"

Appendix III

OS network configuration

Before the installation of the application certain network parameters of the Linux operating system must be set in order to fulfill the security requirements. This configuration is performed by a script that must be executed manually.

In the case of cluster deployments, the script file must be copied from the master node to rest of nodes and executed.

Running the Linux network configuration script

Single box deployments

Procedure

1. Navigate to the directory `/tmp/survey-installer/bin`
2. Run the `network-sysctl-config.sh` script.

```
./network-sysctl-config.sh
```

Cluster deployments

Procedure

1. Navigate to the directory `/tmp/survey-installer/bin`, in the master node
2. Run the `network-sysctl-config.sh` script.

```
./network-sysctl-config.sh
```
3. Copy the script into the other nodes and run the script as in the previous step.

After installing Survey Assist the script file will be copied into the directory `/opt/avaya/survey/installer/support`, if the `network-sysctl-config.sh` script was not executed before installing it could be executed after, to apply the network configuration changes.