Avaya Aura® Product Privacy Statements: Release 7.x through 8.1.x

March 2020

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site: http://www.avaya.com/support

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://www.support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.support.avaya.com/ThirdPartyLicense/

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 fraud intervention

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

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

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

Avaya support

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

Contents

Change History

EVENT	DOCUMENT DATE	CHANGE DESCRIPTION
Product Privacy Statements (Formerly known as GDPR Addendums document)	March 2020	Updated to include Release 8.1.2.
Syslog-over-TLS feature added	06 Jun 2019	Added this feature to satisfy the GDPR requirement that all data-in-transport can be encrypted. The documentation was corrected to more adequately describe the technique of Hardware Level Disk encryption for a solution for data-at-rest on the Avaya Aura® Application server products. The Avaya Aura® products are covered per the R8.1 release.
First GDPR Addendums Published	01 Dec 2018	Cataloged the individual product GDPR Addendum assessments into a single document with a common descriptive style. The Avaya Aura® products are covered per the R7.1.2 release.

Table 1: Document Change History

Chapter 1: Introduction to Avaya Aura® Data Privacy Controls

This document gathers the individual GDPR Data Privacy Addendums for Avaya Aura® as of Release 8.1. This information has been summarized in a common format to provide the description of:

- Data Categories Containing Personal Data (PD)
- PD Human Access Controls
- PD Programmatic/API Access Controls
- PD "At Rest" Encryption Controls
- PD "In Transit" Encryption Controls
- PD Retention Period Controls
- PD Export Controls & Procedures
- PD View, Modify, Delete Controls & Procedures
- PD Pseudo Operations Statement

In terms of responsibility for data privacy, the customer, who operates the communication solution involving Avaya Aura® equipment (servers, gateways, endpoints), has the overall responsibility for:

- Operating as the Data Controller for conducting the collection and storage of consent management. This is commonly referred to as an "opt-in" permission.
- Operating as the Data Controller to provide the administration of the personal privacy data which is configured on the communication equipment and to manage call record logs.
- Providing correct administration of the security features to ensure that all control channels, media channels, and all log transport are properly encrypted. This is known as "In-Transit encryption".
- Providing proper care and encryption of the storage of personal information for the given Avaya Aura® product. This is known as "Data-at-Rest" Encryption.

Avaya Aura® equipment will provide the necessary configuration for management of security features to facilitate the necessary encryption which the Data Controller requires. This includes:

- Providing the ability (through administrative interfaces) to configure all communication and security features, including those which address personal information.
- Providing the ability (through administrative interfaces) to support encryption of personal data both In-Transit and At-Rest.
- Providing deletion/erasure of all temporary files on a timely basis.
- Provide the ability to collect call logs and diagnostic logs per the customer's request.
- Provide the ability for the customer to delete/export log files.

Chapter 2: Data Privacy Controls Addendum for Communication Manager

This addendum applies to Avaya Aura® Communication Manager (CM), Version 7.1.2, 8.0, and 8.1.

Data Categories Containing Personal Data (PD)

Primary Category

User/station data for the various administered users on the PBX includes their name, extension number, mobile number, password, SIP URI, abbreviated dial / autodial buttons, busy indicator buttons, bridged appearance buttons, station's group membership, call logs, etc.

Location: Memory (RAM) and CM translation file at /etc/opt/defty. Backup copy of translation file is kept on the server in the same location. The translation file is regularly synchronized with all available Survivable remote (LSP) and Survivable core (ESS) servers. Memory and translations are replicated on standby server in a CM duplex configuration.

Agent data for the administered agents on Avaya CM including their login IDs, agent name, password etc.

Location: Memory (RAM) and CM translation file at /etc/opt/defty. Backup copy of translation file is kept on the server in the same location. The translation file is regularly synchronized with all available survivable remote (LSP) and survivable core (ESS) servers. Memory and translations are replicated on standby server in a CM duplex configuration.

Avaya customers can create and change **administrator profiles** (login name, password etc) to enable various level of admin access to Avaya CM.

Location: /etc/passwd, /etc/group, /etc/shadow files. Data of these administrator profiles is regularly synchronized with all available survivable remote (LSP) and survivable core (ESS) servers. The information is replicated to standby server in CM duplex configuration too.

Communication Manager generates **Call detail records (CDR)** in real time for all administered incoming, outgoing, and tandem calls, as well as for designated station to station calls, which includes details like calling party number, called party number, account codes, authorization code, duration, time of day.

Location: CDRs can be stored on server disk at (/var/home/ftp/CDR) or can be streamed to external customer server.

CTI Information – Communication Manager generates information related to its call activity on an ongoing basis. Information includes information such as phone number, call states, phone states, etc.

Location: The information is generated in real time and stored in memory to be published to the relevant API. It is held only while it valid.

Agent Information – Communication Manager also generates information relating to agent activity on an ongoing basis. Information includes agent states, agent activities, call progress, etc.

Location: The information is generated in real time and stored in memory to be published to the relevant API. It is held only while it valid.

Call Logs for H.323 endpoints are held on Communication Manager as a record of the station's activity. The Name and number of the calling party and called party is stored.

Location: The information is generated in real time and stored in memory. It is held only while it valid.

Property Management System information – Communication Manager generates information related to hotel guest activity on an ongoing basis. Information includes information such as phone number, automatic wakeup call requests, etc.

Location: The information is generated in real time and stored in memory. It is held only while it valid. The records can be streamed to an external printer or customer's log server.

Secondary Category

Logs & Events – Avaya Communication Manager generates debug and trace logs, security logs & events, command history logs, operating system logs, etc. which can contain personal data such as phone numbers, user activity, names, etc.

Location: security log (/var/log/secure); command history log (/var/log/ecs/commandhistory); Communication Manager IP events log (/var/log/messages); kernel, boot, cron, *.info, *.emerg logs (/var/log/messages); core dumps (/var/crash); mini core dumps (/var/log/defty/dumps); debug log (/var/log/ecs/*.log)

PD Human Access Controls

Human Access to administer or change user/station, agent, and administrator profile data is provided by the solution's management applications including System Manager (SMGR), Avaya Site Administrator (ASA), and System Access Terminal (SAT). Access to these interfaces is provided only to defined users who successfully authenticate themselves to the system. When used in conjunction with a third-party application, multi-factor authentication can be required. Administrator users access can also be limited through granular roles-based access controls (RBAC) that determines what elements what administrators can use.

User/station data can also be accessed by end users through the telephone's user interface. Through this information access to information such a configured cellular number and directory are enabled. Access is limited however, via the requirement to authenticate to the set via the security code.

CDR records are accessed by standard editing tools by opening the file they are stored in. Access to the file requires authentication to the hosting operating systems shell and having permissions to view the directory holding the CDR data file. Typically, this data is not accessed directly by the end user. Instead, it is typically accessed programmatically by reporting applications that provide additional analysis and formatting on the raw CDR data. Avaya Services can use the proprietary TCM interface of the System Access Terminal to access this data. As of Release 8.1, the customer may send collected logs to a remote Syslog server of his choice using TLS.

Similarly, event and debug logs are also accessed by standard editing tools by opening the files from where they are stored. Access to the file requires authentication to the hosting operating systems shell and having permissions to view the directory holding the log file. Typically, this data is not accessed directly by the end user but is instead transferred off the system to Avaya support for analysis during problem investigations. Logs can also be viewed and uploaded using the Communication Manager System Management Interface (SMI) web pages.

Call logs (e.g. missed call logs) for H.323 devices are accessed via the corresponding end devices. The user must be properly authenticated (logged in) to the device to access the logs. Avaya Services can use the proprietary TCM interface of the System Access Terminal to access this data in CM memory while the endpoint is not registered.

PD Programmatic/API Access Controls

Avaya applications and 3rd party applications can use OSSI APIs to gain access to user/station, agent, and administrator profile information for administration purposes. Access via the API, as with the case of accessing via the human interfaces noted above, requires authentication and can be limited in scope via roles-based access control feature.

Call detail recording data can be accessed programmatically using a file transfer protocol. Access to the files to transfer require authentication and would be controlled by the access level of the authenticating account.

Additionally, the data can be streamed to another server. Streaming to the other server is done via the Reliable Session Protocol which is a proprietary Avaya protocol. Streaming data requires that the destination server be explicitly configured by someone with administrator level access to the system. Avaya Services can use the proprietary TCM interface of the System Access Terminal to access CDR while it is stored in CM memory.

The ASAI interface provides access to the CTI data generated by Communication Manager. The interface or link is used to provide the information to the Application Enablement Services (AES) product and must be explicitly configured on both the CM and AES elements by someone with administrator level access to the system.

The SPI Link interface provides call traffic data, formats management reports, and provides an administrative interface to the ACD features in Communication Manager. The interface or link is used to provide the information to the Call Management System (CMS) and must be explicitly configured on both the CM and CMS elements by someone with administrator level access to the system. The link is a binary (not text-based), proprietary protocol used to communicate between the CMS system and the Communication Manager ACD switch. Access can be controlled by IP address. Communication Manager sends ACD configuration information and ACD-related events to the CMS using this communication channel. For instance, CMS systems can use the SPI link to modify CM vectors, agent and VDN assignments.

Log files can be accessed programmatically using a file transfer protocol. Access to the files to transfer require authentication and would be controlled by the access level of the authenticating account. Additionally, the system can be configured to send syslog events to an adjunct server. This must be explicitly configured by someone with administrator level access.

Avaya Services can use the proprietary TCM interface of the System Access Terminal to access call logs data for H.323 devices, stored in CM memory.

The PMS Link interface provides a way for an adjunct to change the name of the station(s) in a hotel room from a generic name (e.g. “Room 321”) to the guest name (e.g., “John Smith”) and marks the room as occupied when the guest checks in. The adjunct changes the name back to the generic name and marks the room as free when the guest checks out. While the guest is checked in and his/her name is assigned to the station, the CDR and other sections elsewhere in this document describe details about that guest’s Personal Data.

PD “at Rest” Encryption Controls

Encryption of Data at Rest using *Linux Unified Key Setup (LUKS)* OS-Level Encryption was introduced with Communication Manager Release 8.1.2.

On Communication Manager, the following Data at Rest will be encrypted when Data Encryption is enabled:

- All administrative data received from the SAT interface or the web-based SMI interface.

- All user/station/device related data Call Detail Records (CDR)
- Logs (all logs under /var/log and /var/log/audit)

The Call logs stored in CM memory (for H.323 endpoints) are not encrypted, but can only be accessed through the proprietary TCM interface of the System Access Terminal, which requires a privileged level of access on CM.

The Property management information is not encrypted but is only accessible through a property configured link to customer’s property management system.

PD “in Transit” Encryption Controls

Access to the user/station, agent, and administrator profile data through Avaya applications is secured and data is encrypted during transit from Communication Manager to the user interface using SSH. When using System Access Terminal, the user should connect to the shell of the system using SSH prior to launching the application. For System Manager and Avaya Site Administrator, the use of SSH is built into the application. When using System Manager, the transit of the information from the system manager server to the user’s browser is encrypted using TLS.

The Reliable Session Protocol that is used to transmit CDR to adjunct servers has a configuration option to allow TLS encryption for CDR1 and CDR2 serial streams. This feature became available in R8.1.2 and later releases.

The ASAI link used to transmit CTI data is encrypted with TLS. The SPI link used to transmit agent data to a CMS adjunct has a configuration option to allow TLS encryption. This feature became available in R8.1.2 and later releases.

Event logs are collected on the local disk. These log files may be transferred by one of two methods:

a) They may be transferred via Secure FTP (SFTP)
b) As of Release 8.1, the customer may direct that the log files be transmitted to the remote Syslog server(s) of his choice using TLS. The security of log files on the log servers is entirely the responsibility of the customer or customer’s service provider.

Call logs are accessed by H.323 endpoint devices and can be encrypted by setting the device to use TLS (if supported).

Property management information flows are not encrypted between the Communication Manager and the property management system.

References:

Communication Manager 7.1 Port Matrix: https://downloads.avaya.com/css/P8/documents/101041519

Communication Manager 8.0.x Port Matrix: https://downloads.avaya.com/css/P8/documents/101054177

Communication Manager 8.1.0 Port Matrix: https://downloads.avaya.com/css/P8/documents/101057187

Communication Manager 8.1.2 Port Matrix: https://downloads.avaya.com/css/P8/documents/101064557

PD Retention Period Controls

User/station, agent, and administrative profile data is persistent until manually deleted. For example, the user/station record for a user will exist as long as the user is authorized to use the system and will be removed when that user is "deleted" from the system.

Starting with Communication Manager Release 8.1, the customer may direct some of these logs to be streamed to a remote Syslog server using TLS. The categories of logs which may be reported via Syslog are:

- OS Security
- CM IP Events
- Command History of the Shell
- Kernel Events
- General OS Messages

A Log Retention feature was introduced in Communication Manager Release 8.1.2 that provides the ability to define the maximum number of days logs will reside on Communication Manager. Logs that are older than the configured log retention period will be deleted. The customer may select maximum storage by either days and/or file storage capacity. The following log categories are covered with this retention feature:

- Call Detailed Recording
  - Maximum capacity is 20 files (each of 20 Mbytes in size)
  - Range is 0 to 20 days
- Command History
  - Storage capacity is 1 Mbyte to 600 Mbyte
  - Range is 0 to 365 days
- CM Logs/MST Trace
  - Storage capacity is 100 Mbyte to 1000 Mbytes
  - Range is 0 to 30 days
- Linux Messages
  - Storage capacity is 1 Mbyte to 50 Mbytes
  - Range is 0 to 180 days

CTI and agent information exist only in memory and is persistent only while the user or agent is in the indicated state.

CM deletes the H.323 call log information stored in memory as soon as the endpoint registers. In the event of server interchange, CM does not shadow this memory on the duplicated server.

PD Export Controls and Procedures

User/station, agent, and administrator profile data can be exported via the bulk export tool in the System Manager application. Note that the data format is proprietary to Communication Manager and exports or a given user's data is not expected to be re-usable in other solutions.

Export of CDR or log file data stored on the Communication Manager Server must be done manually by accessing the file, finding the desired records, and copying. CDR records follow the Station Message Digital Record (SMDR) format. Log data follows the Syslog format. As of Release 8.1, the customer may direct these CDR files to be streamed up to the customer's remote Syslog server using TLS.

PD View, Modify, Delete Controls and Procedures

Viewing, modifying, or deleting user/station, agent, or administrator profile data is a manual task that can be accomplished through any of the management applications or via a third-party application using the OSSI interface by a properly authenticated administrative user.

When stored on the Communication Manager Server, viewing, modifying, or deleting the CDR or log file data must be done manually by accessing the file and locating the desired records.

Call logs when they are stored on CM, can only be accessed via Avaya's TCM debugging terminal available to Avaya services.

Chapter 3: Data Privacy Controls Addendum for Session Manager

This addendum applies to Avaya Aura® Session Manager, Release 7.1.2, 8.0, 8.1, and 8.1.2.

Data Categories Containing Personal Data (PD)

Primary Category

User profile data: identifies the user assigned to an extension on the Avaya Aura® system (e.g., name, handles, phone numbers, address, etc.).

Location: PostgreSQL database, replicated from System Manager. This data is created via the Avaya Aura® System Manager application in a local data base first. And then the content is transferred to the Session Manager.

Station data: associates the extension and handle of the user assigned to the station in Communication Manager

Location: PostgreSQL database, replicated from System Manager.

User contact list data: contains a list of contacts for each user. Includes the contact's name, phone numbers, address, email, etc .

Location: Cassandra database on primary and secondary Session Manager

Call history information: contains information such as phone numbers and time of day information for outgoing and incoming calls to a particular station.

Location: Cassandra database on primary and secondary Session Manager

Secondary Category

Call Detail Record (CDR) - contains call history information such as phone numbers, time of day information and length of a call for outgoing and incoming calls.

Location: /var/home/ftp/CDR/CDR_files/

System logs: used to trouble shoot the system if an issue is identified by a user. These logs may include information such as phone numbers and display names.

Location: /var/log/Avaya

PD Human Access Controls Procedures

Access to user profile data and station data is provided by the Avaya Aura® System Manager. This application creates the data locally and copies it to the Session Manager. Access to the System Manager application requires authentication as an administrative user. Additionally, users can be restricted to specific management objects using the systems fine grained, roles base access controls (RBAC).

Access to the contact list and call history is provided to end users via the Equinox soft client or Avaya telephones. The data is provided to these devices by the personal profile manager (PPM) service in the Session Manager software which provides the ability to access, edit, and delete the information. End users must be authenticating themselves via the soft client or telephone to gain access and, once authenticated, gain access only to their contact list and their call history.

Access to CDR and Log files is available via the shell interface in the operating system hosting the Session Manager software. To access the files, someone logs in through the SSH interface and navigates to the directory holding the files. CDR files are located in a directory open to anyone logged in via SSH. CDR data is also accessible to third party applications via Secure FTP (SFTP) using the user account CDR_user. The log files are in a directory requiring suser group privilege. As of Release 8.1, the logs may be streamed to a remote Syslog server using TLS. Administrative access through SSH is secured by the Avaya EASG (Enhanced Access Security Gateway) challenge-response mechanism. By default, EASG is enabled on the system, which requires challenge response to be provided by Avaya before the administrator can log into the system. Customers cannot automatically login without the challenge response from Avaya.

PD Programmatic/API Access Controls

User profile data: not available via API.

Station data: not available via API.

Contact list: available via PPM

Call history: available via PPM

Call Detail Record (CDR): can be accessed remotely via Secure FTP (SFTP) using user account CDR_user.

Logs: As of Release 8.1, some log data can be streamed to a remote Syslog server using TLS

PD “at Rest” Encryption Controls

Encryption of Data at Rest using *Linux Unified Key Setup (LUKS)* OS-Level Encryption was introduced with Session Manager Release 8.1.2.

On Session Manager, the following Data at Rest will be encrypted when Data Encryption is enabled:

- All administrative data received from System Manager
  (i.e. Postgres database, schema, tables and configuration under /data)
- All user/station/device related data
  (i.e. Casandra database, schema, tables, and configuration under /data)
- Call Detail Records (CDR)
- Logs (all logs under /var/log and /var/log/audit)
- Backups that are temporarily stored locally on Session Manager

The location of the encrypted data differs between Session Manager and Branch Session Manager.

- **Session Managers**: All data related partitions on Disk 2 are encrypted.
  - /data
  - /var/log
  - /var/log/audit
- **Branch Session Managers:** All data related partitions on Disk 1 are encrypted.
  - /data
  - /var/log partitions.

PD “in Transit” Encryption Controls Procedures

Data in transit from and to Session Manager is protected by TLS and SSH.

Call Detail Records (CDR) and logs are collected on the Session Manager’s local disk. These log files may be transferred by one of two methods:

a) CDR data may be transferred via Secure FTP (SFTP)

b) As of Release 8.1, log files may be transmitted to a remote Syslog server using TLS. The security of log files on the log servers is entirely the responsibility of the customer or customer's service provider.

References:

Session Manager 7.0 Port Matrix: https://downloads.avaya.com/css/P8/documents/101014664

Session Manager 8.0 Port Matrix: https://downloads.avaya.com/css/P8/documents/101051111

Session Manager 8.0.1 Port Matrix: https://downloads.avaya.com/css/P8/documents/101053708

Session Manager 8.1 Port Matrix: https://downloads.avaya.com/css/P8/documents/101058429

PD Retention Period Controls

User profiles, CM station data and contact lists: are persistent (stored in the database) until manually deleted. Refer to 'PD View, Modify, Delete Procedures' below for more details.

Call History entries: are retained up to a limit of 100 entries per user. On the arrival of the 101st call, the oldest record will be deleted to maintain the 100 entry size.

Call Detail Records (CDR): have a retention period of 5 days.

Debug and Trace logs: retention times are configurable. When the retention time is exceeded, the oldest logs are deleted.

As of Release 8.1, the customer may direct some of these logs to be streamed to a remote Syslog server using TLS.

A Log Retention feature was introduced in Session Manager Release 8.1.2 that provides the ability to define the maximum number of days logs will reside on Session Manager. Logs that are older than the configured log retention period will be deleted.

Session Manager provides several administrable Log Retention settings:

1. Global Log Retention setting – Applies to all Session Managers except those that have a Log Retention Override value administered.

2. Local Log Retention Override setting – Each Session Manager instance may administer a Local Log Retention value that overrides the Global Log Retention setting. This is particularly useful when diagnostics are being performed on an individual Session Manager that may require having a longer period than the Global Retention Setting.

3. Centralized Call History Retention – Defines the number of days the Personal Profile Manager (PPM) will retain the Call History Logs it maintains for Endpoint devices.

PD Export Controls and Procedures

User/station, agent, and administrator profile data can be exported via the bulk export tool in the System Manager application. Note that the data format is proprietary to Communication Manager and exports or a given user's data is not expected to be re-usable in other solutions.

Call Detail Records can be exported in an XML (Extensible Markup Language) format or several standard formats. CDR data records may be uploaded from Session Manager using Secure FTP (SFTP).

As of Release 8.1, some log data stored on Session Manager may be sent to a remote Syslog server using TLS. Log data follows the Syslog format. The customer may direct these log files to be streamed up to a remote Syslog server using TLS.

PD View, Modify, Delete Controls and Procedures

User Profile Data: View, Modify and Deletion of user profile data in the database is a manual task. An administrative user, after being properly authenticated, would access System manager to perform these actions.

Station Data: View, Modify and Deletion of station data in the database is a manual task. An administrative user, after being properly authenticated, would access System manager to perform these actions.

Contact Data: can be viewed, modified and deleted by the owning user on the device they are currently using.

Call History entries: can be viewed by the owning user on their device. However, these records cannot be modified or deleted in this manner. However, they can be manually deleted with root access. How??

Call Detail Record (CDR) can be accessed, modified, and via Linux based text file editors by a user connected and authenticated via SSH. CDR data may also be accessed via Secure FTP (SFTP).

Logs: can be accessed, modified, and via Linux based text file editors by a user connected – an authenticated – via SSH

Chapter 4: Data Privacy Controls Addendum for System Manager

This addendum applies to Avaya Aura® System Manager(SMGR), Version 7.1.2, 8.0.x, and 8.1.x.

Most Personal Data items are stored in a database which is access controlled and only accessible from the local host via certificate authentication. Some Personal Data items relating to administrative users are stored in a LDAP directory which is also access controlled. Data backups can optionally be encrypted. When Personal Data is transmitted over a network, it is secured with TLS and/or SSH.

Data Categories Containing Personal Data (PD)

Primary Category

End user profile data that identifies an administered user on the system including the user's name, handles, phone numbers, postal address, mailbox number, conference room number, participant security code, moderator security code, presenter security code, etc.

Location: PostgreSQL database. The database is replicated to the standby SMGR server if any.

Contacts data including name, phone numbers, postal address, etc. Contacts include private contacts that end users create and use via their telephones and desktop client applications, as well as public contacts that administrators create for use by all users in common.

Location: PostgreSQL database. The database is replicated to the standby SMGR server if any.

Agent list which includes login IDs and names that identify Communication Manager agent profiles.

Location: PostgreSQL database. The database is replicated to the standby SMGR server if any.

Secondary Category

Administrative user profile data including their name, email address etc. Role based access control (RBAC) provides organizations with the ability to assign application access permissions based on the job function or role of an administrative user.

Location: PostgreSQL database and internal LDAP directory. The database and directory are replicated to the standby SMGR server if any.

Application and operating system level logs. Some of the log entries, for example audit logs, can include information from the primary category above.

Location: $AVAYA_LOG and /var/log/messages folders

PD Human Access Controls

Human Access to end user profiles, contacts data, agent lists, and administrator user profiles is enabled via the web base user interface to the System Manger application. To access the data, a user must be authenticated to the applications. Note also, that access permissions – or controls of who accesses what – can be managed through the products role-based access control feature.

Access to the logs is enabled through administration level logins at the operating system level via the SSH interface. Administrative access through SSH is secured by the EASG (Enhanced Access Security Gateway) challenge-response mechanism and can optionally be secured by multi-factor authentication through the use of an access card as well.

End users have access to user contact data through Personal Profile Manager (a component of Session Manager) if the user is authenticated at the phone user interface.

PD Programmatic/API Access Controls

Programmatic access (to user and routing data) through REST APIs is via TLS (encrypted) communication links.

PD “at Rest” Encryption Controls

By default, the databases and log files containing PD items are not encrypted.

Encryption of Data at Rest using *Linux Unified Key Setup (LUKS)* OS-Level Encryption was introduced with System Manager Release 8.1.2.

On System Manager, the following Data at Rest will be encrypted when Data Encryption is enabled:

- All administrative data including the Primary and Secondary category data
  (i.e. Postgres database, schema, tables and configuration under /var/lib/pgsql/data and internal LDAP directory data under /var/opt/nortel/cnd/)
- Logs (all logs under /var/log and /var/log/audit)

PD “in Transit” Encryption Controls

Access to end user profiles, contacts data, agent lists, and administrator user profiles via the web-based interface is protected by TLS encryption on the connection using HTTPs.

Programmatic access through REST APIs is also protected by TLS encryption through HTTPS.

Event logs are collected on the local disk. These log files may be transferred by one of two methods:

a) They may be transferred via Secure FTP (SFTP)
b) As of Release 8.1, log files may be transmitted to a remote Syslog server using TLS. The security of log files on the log servers is entirely the responsibility of the customer or customer’s service provider.

References:

System Manager 7.0 Port Matrix: https://downloads.avaya.com/css/P8/documents/101014650

System Manager 7.1.3 Port Matrix: https://downloads.avaya.com/css/P8/documents/101047775

System Manager 8.0.1 Port Matrix: https://support.avaya.com/css/P8/documents/101053839

System Manager 8.1 Port Matrix: https://downloads.avaya.com/css/P8/documents/101055783

PD Retention Period Controls

The end user profiles, contacts data, agent lists, and administrator user profiles are persistent until manually deleted.

Retention times for logs are configurable. When the retention time is exceeded, the oldest logs are deleted..

A Log Retention feature was introduced in System Manager Release 8.1.2 that provides the ability to define the maximum number of days logs will reside on System Manager. Logs that are older than the configured log retention period will be deleted.

System Manager Log Retention setting can be change from the Graphical User Interface and Command Line Interface.

PD Export Controls and Procedures

SMGR supports export of user records for all or selected users. It is also possible to provide search criteria with the advanced search function and export the user records that match the criteria.

The exported user data is stored in archive files that remain on System Manager until explicitly deleted by the administrator through the Graphical User Interface or Command Line Interface. The exported data could have also been downloaded by SMGR administrators to their machines.

SMGR supports taking backup of all the administrative data stored in its Database, LDAP directory and file system. This backup can be stored locally on SMGR itself or remotely. The remote backup file is transferred to the remote machine via SCP or FTP.

For message lines in logs that contain (administrator) userids, it is possible to search for a given userid using the SMGR log viewer, locate the set of lines that contain it, and export those lines.

SMGR can be used to harvest log files from SMGR itself or from other connected products like Session Manager. The harvested log files are stored on SMGR and can also be downloaded (via GUI) by SMGR administrators to their machines.

PD View, Modify, Delete Controls and Procedures

View, Modify, and Deletion of end user profiles, contacts data, agent lists, and administrator user profiles is a manual task. An administrative user would access the administration web pages provided by the product to perform these actions.

User contacts can also be deleted by the owning user from their end device through the Personal Profile Manager (a component of Session Manager).

The locally stored backup files can be manually deleted by the logging into the SMGR command line console. The path in which the backup files are stored is displayed on the SMGR 'backup and restore' UI screen.

The remotely stored backup files will have to be manually deleted by logging into the remote machine's command line console. The path, in which the backup files are stored, is displayed on the SMGR 'backup and restore' UI screen.

Log files must also be manually deleted. Log files generally are not modified but could be via a standard editing tool launched on the file in the correct directory.

The harvested log files, stored locally on SMGR, can be deleted by logging into the SMGR command line console. The path, at which the harvested files are stored, is displayed in the SMGR 'Log Harvester' UI screen.

Chapter 5: Data Privacy Controls Addendum for Web License Manager (Web LM)

This addendum applies to Avaya Web License Manager, Version 7.1.2, 8.x.

Data Categories Containing Personal Data (PD)

Primary Category

Administrative Information including userids and their passwords. These IDs and passwords are utilized by WebLM administrator to place license files on WebLM for use in the associated system.

Location (Release 7.x): $CATALINA_HOME/webapps/WebLM/admin

Location (Release 8.0 onwards): $JBOSS_HOME/avmgmt/configuration/weblm/admin

Note: Do not use any personal information in the userid and password fields. This will ensure that there is no personal data stored on WebLM.

PD Human Access Controls

Human Access to Web License Manager is through the administration web pages that the product provides. The administrator must be authenticated with a valid password to gain access to the application and the ability to access the administrative information.

PD Programmatic/API Access Controls

There is no programmatic/API access to the administrative information.

PD “at Rest” Encryption Controls

The file containing administrative information is not encrypted. Hardware Level Encryption may be provided by the Server platform and its storage device(s). This is done without the knowledge of the Operating System of Virtual Machine residing upon it. This is provided by the Server vendor (HP or Dell) and has the following properties:

- License(s) are required for the key management, and the individual drives typically required licenses for encryption use.

- These techniques can be employed across a RAID controller managed disk cluster.
- The encryption can be enabled to operate on certain disk pairs or it can be globally administered across multiple disk pairs. The two disk drives are usually managed as a single virtual disk.
- The passphrase for encryption may be stored locally or remotely by the central Encryption management.
- The Encryption key may be managed by:
    - Local server based key management application
    - Remote central server key management application
    - It should be noted that some customers (such as JITC for Government sector customers) desire a local server with manual key entry.
- A product example is:
    - HPE Smart Array controller w/HPE Secure Encryption
      Reference: https://h20195.www2.hpe.com/V2/GetPDF.aspx/c04318075.pdf

Since this feature is really a part of the Server product, the performance impact must be measured by both the customer and Avaya as the Solution integrator.

PD “in Transit” Encryption Controls

Access to the administrative information is via a web-based interface or shell access and protected by TLS and/or SSH.

References:

Web LM 8.1.0 Port Matrix: https://downloads.avaya.com/css/P8/documents/101055691

PD Retention Period Controls

Administrative information stored in Web License Manager is persistent until manually deleted.

PD Export Controls and Procedures

Web License Manager does not provide an automated export capability for the administrative information. To provide the information, one just logs in and manually extract it from the administrative interface.

PD View, Modify, Delete Controls and Procedures

View, Modify, and Deletion of administrative information is a manual task performed by a user via the product’s administration web pages following proper authentication.

Chapter 6: Data Privacy Controls Addendum for Application Enablement Services (AES)

This addendum applies to Product Application Enablement Services, Ver. 8.1.2

Data Categories Containing Personal Data (PD)

The Private Data collected by AE Services comprises users' extension numbers, names, IP-Address and UUI. This data is stored in the form of logs at /var/log/avaya. This data is mainly used for troubleshooting purposes and can be deleted upon request. Each service, such as TSAPI, DMCC, SMS, generates its own log files within /var/log/avaya.

Station data: associate's/Agent's extension, fax, modem, ACD, VDN, agent ID, Work station hostname and IP address are stored on AES server in locally hosted postgres database

The location and content of the log files is available in the Maintaining Avaya Aura® Application Enablement Services in Chapter 5: Location of AE Services log files

PD Human Access Controls

The call log files only accessible to administrators and privileged users as read only. Human access to these log files is via SSH, port 22. Access to data available in log files is allowed to system pre-defined users only. System administrator has privileges to add more users to the system for log access.

Access to station data is via AES OAM Web Page

PD Programmatic/API Access Controls

Programmatic/API Access Controls are accessible by administrators and privileged users. Human access to these logs is via SSH, port 22

PD "at Rest" Encryption Controls

On AE Services, postgres database and log data is not encrypted however stored under encrypted partition.

Encryption of Data at Rest using Linux Unified Key Setup (LUKS) OS-Level Encryption was introduced with Application Enablement Services Release 8.1.2. On AES, the following Data at Rest will be encrypted when Data Encryption is enabled:

All administrative data available on AES.
(i.e. Postgres database, schema, tables and configuration under /var/mvap/database)

- All user/station/device related data
  (i.e. LDAP data under /var/lib/data)
- Logs (all logs under /var/log and /var/log/audit)
- Backups that are temporarily stored locally on AES

PD “in Transit” Encryption Controls

Call Log files are not encrypted on the server. The log files can be transferred to remote server via secured TLS 1.2 protocol and stored in encrypted format at the destination.

Other than DLG service all the services (CVLAN, DMCC, JTAPI, TSAPI, TR/87 and Web services) support secure link.

AES OAM (admin web page) use HTTPS service.

AES supports secure link to establish connection with Avaya Aura® Communication Manager.

SNMPv3 supports data encryption.

References:

AES 8.1.0 Port Matrix: https://downloads.avaya.com/css/P8/documents/101057887

PD Retention Period Controls

The Log Retention feature gives ability to define a Log Retention Policy that specifies the maximum number of days logs that may contain privacy and/or operational related data will reside on AE Services. Logs that are older than the configured log retention period will be deleted.

AE Services’ Log Retention period represents the *maximum* number of days that logs will be retained. It is not a guarantee that logs will be retained for the full period. To avoid consuming of full log disk space, automatic log deletion utility has been implemented. This utility will free up space till 75% or below by deleting older logs and trace if the log disk occupancy reaches 90%.

Careful consideration should be given to what log retention period is used. Generally, logs should only be retained on AE Services for the minimum time needed. However, longer retention times may be required if/when diagnostics need to be performed.

AE Services provides two administrable Retention settings.

1) Log Retention setting
2) Traces Retention setting

The range for logs and traces retention Range can be set between 0 to 180 days and the default value is 30 days.

PD Export Controls and Procedures

There is no export facility provided for exporting call logs.

PD View, Modify, Delete Controls and Procedures

Modification and deletion of station data can be done via AES OAM page.

On Demand Deletion of Logs and traces can be done from AES command prompt and AES OAM page.

No database objects can be accessed/modified/deleted by manually modifying the call logs files.

PD Pseudonymization Operations Statement

AE Services does not provide a capability to automatically anonymize or pseudonymize user data. If pseudonymization is desired, the Data Privacy Administrator may manually pseudonymize.

Chapter 7: Data Privacy Controls Addendum for AVP Utilities

This addendum applies to Avaya Aura® AVP Utilities (AVP-U) Version 8.1.2.

Data Categories Containing Personal Data (PD)

Primary Category:

- **Administrator profiles** include the login name and password of each AVP Utilities administrator.

  Location: /etc/passwd, /etc/group, /etc/shadow files
  There is no other private data stored on AVP Utilities.

Secondary Category:

- **Logs**:
- AVP Utilities generates logs during its operation. The logs do not contain any personal information.

- Location: /var/log

PD Human Access Controls

Human Access for the purposes of administering data stored in AVP Utilities is controlled by administrator authentication. The choice of authentication mechanisms includes Linux local authentication, Remote Authentication Dial-In User Service (RADIUS), and Lightweight Directory Access Protocol (LDAP) authentication. Once authenticated, the capabilities of the role are the same regardless of the authentication mechanism. Only the administrator can access the backup files and logs.

As of release 8.1 a customer may send logs forwarded from AVP and logs from AVP Utilities to up to 5 external Syslog servers over a TLS connection.

PD Programmatic/API Access Controls

N/A

PD “at Rest” Encryption Controls

Encryption of Data at Rest using *Linux Unified Key Setup (LUKS)* OS-Level Encryption was introduced with AVP Utilities Release 8.1.2.

On AVP Utilities, the following Data at Rest will be encrypted when Data Encryption is enabled:

- Backup files created under /tmp partition.
- Logs under /var/log and /var/log/audit

PD “in Transit” Encryption Controls

Data (such as backups, etc.) can be downloaded securely from the Utility Services by using the Secure Copy Protocol which runs over Secure Shell (SSH).

Logs can optionally be forwarded to external syslog server(s). Logs forwarded to an external syslog server (relevant only to AVP log harvesting and alarming) are not encrypted.

As of Release 8.1, AVP utilities has introduced the capability of forwarding its own syslog and AVP 8.1’s syslog to up to 5 external syslog servers using the TLS transport. The security of log files on the log servers is entirely the responsibility of the customer or customer’s service provider.

References:

AVP Utilities 8.1 Port Matrix: https://downloads.avaya.com/css/P8/documents/101057979

PD Retention Period Controls

AVP Utilities 8.1.2 and above allows a data privacy administrator to configure log retention to minimize sensitive data on the system. AVP Utilities provides the following logs to be configured under log retention feature:

/var/log/messages

/var/log/secure

/var/log/commandhistory

/var/log/remote.log

The retention can be configured between 0 and 180 days.

PD Export Controls and Procedures

NA

PD View, Modify, Delete Controls and Procedures

Logs roll over when they are full and can be manually deleted as well.

Chapter 8: Data Privacy Controls Addendum for Device Adapter Snap-In

This addendum applies to **Avaya Device Adapter Snap-In, Ver. 8.0, 8.1**

Avaya Device Adapter Snap-in is a modular, reusable solution that enables UNIStim IP, digital, and analog phones working with Avaya Communication Server 1000 (CS 1000) to migrate to Avaya Aura® without significant investment on the existing infrastructure. Device Adapter offers a feasible solution to CS 1000 customers to take advantage of Avaya Aura® features while minimizing expenses on the cables and hardware. Device Adapter is deployed on the Avaya Breeze® platform. A Device Adapter instance runs on an Avaya Breeze® platform cluster that can have one or more Avaya Breeze® platform servers. A standard deployment solution has one or more Avaya Breeze® platform clusters. Implementing Device Adapter does not introduce any new hardware. Device Adapter works as a part of the Avaya Breeze® platform solution.

Data Categories Containing Personal Data (PD)

System Manager User Data and Communication Manager Station Data are stored in the System Manager replica database that can be found at /var/lib/pgsql/9.6/data. This data is mastered in System Manager and replicated via HTTPS to Breeze.

Log and trace files are stored in various directories under /var/log/Avaya. These files include users' phone numbers and display names.

Breeze has a Cluster Database that Snap-Ins can use to store their own specific code, in the case of the Device Adaptor this would include Personal Directory's. This data is stored at /var/lib/pgsql/9.6/data. The Cluster Database runs on 2 Breeze nodes in the cluster in an active/standby fashion. Data is replicated from the master to the standby using industry standard Transport Layer Signaling (TLS). The manner of data that is stored in the Cluster Database includes Personal Directory data i.e. a person's phone number and name.

Primary Category:

- User & Station Data (in memory) including Virtual Office credentials– Location: Memory – Linux process
- User & Station Data (on disk - DRS) – Location: Disk – DRS on Breeze Platform
- Personal Directory (on disk - Cluster DB) – Location: Disk - Cluster DB on Breeze platform
- Device&Registration Data (Extension, config data, menu options used for Branch SM scenarios, PPM data cashing) - on disk in Cluster DB – Location: Disk - Cluster DB on Breeze platform

Secondary Category:

- User & Station Data (in logs) – Location: logs in /var/log on Breeze platform

PD Human Access Controls

Human access to the System Manager replica database and Breeze Cluster Database is tightly restricted. The files can only be read by the “postgres” user, or by root. A human would have to have root level access to access the files.

There is no restriction on access to log and trace files. Any human with shell access on Breeze (usually cust or EASG-based logins) can access the log and trace files. By default, no logs will be produced with personal data (though some personal data may be logged in the event of software errors). In general, personal data will only appear in log and trace files if debug logging / tracing is enabled by a human.

- User & Station Data (in memory) – Administrator: Read, thru CLI, privileged user access
- User & Station Data (on disk - DRS) – Controlled by Breeze Platform
- Personal Directory (on disk - Cluster DB) – Controlled by Breeze Platform
- Device&Registration Data (on disk - Cluster DB) – Controlled by Breeze Platform
- User & Station Data (in logs) – Controlled by Breeze Platform

PD Programmatic/API Access Controls

There are 2 ways that the System Manager replica database is accessed programmatically:

- Via HTTPS from System Manager to replicate the data via Data Replication Service (DRS).
- Via TLS from the Breeze platform and the Device Adaptor Snap-In in order to access the replicated data. These connections are secured using mutual TLS: the entity accessing the data must have a certificate signed by a trusted Certificate Authority (CA), which is usually the System Manager CA.

Log and trace files are generally not accessed programmatically.

The Breeze Cluster Database is accessed only by the Snap-Ins that are leveraging that facility. Access to the Breeze Cluster Database is protected. This authentication is certificate-based.

- User & Station Data (in memory) – NA
- User & Station Data (on disk - DRS) – Controlled by Breeze Platform
- Personal Directory (on disk - Cluster DB) – Controlled by Breeze Platform
- User & Station Data (in logs) – Controlled by Breeze Platform
- Device&Registration Data (on disk - Cluster DB) – Controlled by Breeze Platform

PD “at Rest” Encryption Controls

None of the System Manager replica database, log/trace files, or Breeze Cluster Database are encrypted on disk. Breeze team plans to take care of this in Release 3.7. Customers sensitive to this fact should consider encrypting the entire disk, perhaps by use of a Storage Area Network (SAN).

- User & Station Data (in memory) – NA
- User & Station Data (on disk - DRS) – Controlled by Breeze Platform
- Personal Directory (on disk - Cluster DB) – Controlled by Breeze Platform
- Device&Registration Data (on disk - Cluster DB) – Controlled by Breeze Platform
- User & Station Data (in logs) – Controlled by Breeze Platform

PD “in Transit” Encryption Controls

PD in transit is protected by TLS.

Breeze has several identity certificates that can be managed from the System Manager Inventory Management page. The ones that are used to encrypt data are:

1. The “mgmt” certificate. This is used to encrypt the link between System Manager and the JBoss Management Agent running on Breeze. All traffic across this link is secured using HTTPS.
2. The “postgres” certificate. This certificate is used for all access to the System Manager Replica Database. This traffic is all TLS based. All of these entities access the replica database using this certificate: The JBoss Management Agent, WebSphere, GigaSpaces.
3. The “cdb” certificate. This certificate is used for the Device Adaptor Snap-In access to the Breeze Cluster Database from Snap-In code running in WebSphere or GigaSpaces. This traffic is all TLS- based.
4. The “Security Module SIP” certificate. This certificate is used for TLS encryption / authentication of SIP signaling between Breeze and Session Manager. TLS is optional but strongly encouraged.

- User & Station Data (in memory) – TLS 1.2
- User & Station Data (on disk - DRS) – Controlled by Breeze Platform
- Personal Directory (on disk - Cluster DB) – Controlled by Breeze Platform
- User & Station Data (in logs) – Controlled by Breeze Platform
- Device&Registration Data (on disk - Cluster DB) – Controlled by Breeze Platform

References:

Device Adapter Snap-In 8.1.2 Port Matrix: https://downloads.avaya.com/css/P8/documents/101063599

PD Retention Period Controls

There are no provisioned retention policies for any personal data on Breeze.

Some PD (Logs) will remain permanent until deleted by the System Administrator.

Some PD will exist until the user is deleted from the system (User&Station Data). Other PD (Device&Registration data) will be automatically removed 24h after unregistration of ADA endpoint.

- User & Station Data (in memory) – Present during an endpoint login "session"
- User & Station Data (on disk - DRS) – Permanent unless the user/station is deleted by the administrator
- Personal Directory (on disk - Cluster DB) – Present until purged by the administrator
- User & Station Data (in logs) – Controlled by Breeze Platform
- Device&Registration Data (on disk - Cluster DB) – Removed 24 hours after ADA set is unregistered

PD Export Controls and Procedures

Only authorized administrators can export System Manager data or Breeze Cluster Database data. Log and trace files can be retrieved by any human that has shell access to Breeze.

- User & Station Data (in memory) – None
- User & Station Data (on disk - DRS) – Controlled by Breeze Platform
- Personal Directory (on disk - Cluster DB) – DB Backup/Restore which is controlled by the Breeze Platform
- User & Station Data (in logs) – Controlled by Breeze Platform
- Device&Registration Data (on disk - Cluster DB) – Controlled by Breeze Platform

PD View, Modify, Delete Controls and Procedures

Only authorized administrators can view, modify or delete System Manager data or Cluster Database data. Log and trace files can be viewed or deleted by any human that has shell access to Breeze.

- User & Station Data (in memory) –
  - Modify: Administrator can modify the user/station and force the endpoint to re-login
  - Delete: Administrator can delete the station and force the endpoint to log-out
- User & Station Data (on disk - DRS) – Controlled by Breeze Platform
- Personal Directory (on disk - Cluster DB) – Present until purged by the administrator
- User & Station Data (in logs) – Controlled by Breeze Platform
- Device&Registration Data (on disk - Cluster DB) – Controlled by Breeze Platform since the data is in clusterDB (for View/Modify/Delete controls).

Chapter 9: Data Privacy Controls Addendum for Avaya Aura® Messaging

This addendum applies to Avaya Aura® Messaging, Version 7.x.

AAM release 7.1 is based on the CM R7.1 platform.

Personal Data is stored in the database that is accessible only as a privileged system user.

Data Categories Containing Personal Data (PD)

Primary Category: User data (Name, Phone Number, preferred Messaging configuration options, etc) – Location: Database (OpenLDAP 2.4.40).

User media content (Voicemail messages and greetings) – Location: IMAP.

Secondary Category: Software Log files located in var/log/avaya directory

PD Human Access Controls

Human access to AAM product is role based via login/password. Login configuration is through the Administrator Accounts SMI Web page (HTTPS://<AAM_server>/cgi-bin/cm/secAdminAccnt/w_adminAccnt).

Documentation of the access levels can be found in “Administering Avaya Aura® Messaging” guide located in https://downloads.avaya.com/css/P8/documents/101033961

Log files are located in the /var/log/avaya/mango(messaging) directories and accessible by administrators and privileged users as read only. Human access to these logs is via SSH, port 22.

PD Programmatic/API Access Controls

Programmatic access to PD is via TLS (encrypted) internal communication links to trusted sources only. Examples are Avaya clients such as the Avaya Web Client or 3rd Party clients like Mutare and Unimax and Starfish.

Programmatic access to log files is internal through an encrypted communication link.

PD “at Rest” Encryption Controls

If the AAM 7.x software is running on an Avaya provided HP DL360 G9 server with hard drive encryption enabled, then the entire hard drive and all its data is encrypted. If not using this server with encryption enabled, then:

User data: Only passwords are encrypted using 3DES algorithm.

Log files and User media content are not encrypted.

Hardware Level Encryption may be provided by the Server platform and its storage device(s). This is done without the knowledge of the Operating System of Virtual Machine residing upon it. This is provided by the Server vendor (HP or Dell) and has the following properties:

- License(s) are required for the key management, and the individual drives typically required licenses for encryption use.
- These techniques can be employed across a RAID controller managed disk cluster.
- The encryption can be enabled to operate on certain disk pairs or it can be globally administered across multiple disk pairs. The two disk drives are usually managed as a single virtual disk.
- The passphrase for encryption may be stored locally or remotely by the central Encryption management.
- The Encryption key may be managed by:
    - Local server based key management application
    - Remote central server key management application
    - It should be noted that some customers (such as JITC for Government sector customers) desire a local server with manual key entry.
- A product example is:
    - HPE Smart Array controller w/HPE Secure Encryption
      Reference: https://h20195.www2.hpe.com/V2/GetPDF.aspx/c04318075.pdf

Since this feature is really a part of the Server product, the performance impact must be measured by both the customer and Avaya as the Solution integrator.

PD “in Transit” Encryption Controls

User media and signaling data in transit occurs over a TLS encrypted link, so is always encrypted while “in transit”.

Event logs are collected on the local disk. These log files may be transferred by SSH access and then by a secure FTP transfer.

References:

AAM 7.0 Port Matrix: https://downloads.avaya.com/css/P8/documents/101047408

AAM 7.1 Port Matrix: https://downloads.avaya.com/css/P8/documents/101056533

PD Retention Period Controls

AAM has no retention policy thus no automatic deletion of PD. Refer to 'PD View, Modify, Delete Procedures' below for manual delete procedure.

Log retention period cannot be configured. Only the Log size can be configured via the "log_size" CLI command.

PD Export Controls and Procedures

AAM does not provide an export capability for a single User's contact data.

There's no single-user export from the debug or application log files.

PD View, Modify, Delete Controls and Procedures

View, Modify, and Deletion of PD is a manual task. User data can be modified through Admin web pages (SMI). This can also be done through the SMGR Messaging Admin Web page SMGR Messaging Element Manager administration Web page.

PD Pseudonymization Operations Statement

NA

Chapter 10: Data Privacy Controls Addendum for Presence Services

This addendum applies to Presence Services, Ver. 7.1

Data Categories Containing Personal Data (PD)

Primary Category

Presence (Auto) states (in memory) – Location: Memory - (GS datagrid)

Presence (Manual) states (in memory) – Location: Memory - (GS datagrid)

Users data - (In memory) – Location: Memory - (GS datagrid) and memory - (Websphere)

Presence (Manual) states (on disk) – Location: Cluster DB on Breeze platform

IM - (on Disk) – Location: Cluster DB on Breeze platform

Users data - (on Disk) – Location: Cluster DB on Breeze platform

Secondary Category: Log data

Presence (Auto) states (in logs) – Location: logs in /var/log on Breeze platform

Presence (Manual) states (in logs) - Location: logs in /var/log on Breeze platform

IM details - (In logs) - Location: logs in /var/log on Breeze platform

Users data - (In logs) - Location: logs in /var/log on Breeze platform

PD Human Access Controls

Access via: Administrator: Read, thru SMGR PS admin Web page

Presence (Auto) states (in memory) – Location: Memory - (GS datagrid)

Presence (Manual) states (in memory) – Location: Memory - (GS datagrid)

Users data - (In memory) – Location: Memory - (GS datagrid) and memory - (Websphere)

Access controlled by Breeze Platform

Presence (Manual) states (on disk) – Location: Cluster DB on Breeze platform

IM - (on Disk) – Location: Cluster DB on Breeze platform

Users data - (on Disk) – Location: Cluster DB on Breeze platform

Presence (Auto) states (in logs) – Location: logs in /var/log on Breeze platform

Presence (Manual) states (in logs) - Location: logs in /var/log on Breeze platform

IM details - (In logs) - Location: logs in /var/log on Breeze platform

Users data - (In logs) - Location: logs in /var/log on Breeze platform

PD Programmatic/API Access Controls

Access via GS API - Controlled by the Breeze Platform – Internally consumed, no external access.

Presence (Auto) states (in memory) – Location: Memory - (GS datagrid)

Presence (Manual) states (in memory) – Location: Memory - (GS datagrid)

Users data - (In memory) – Location: Memory - (GS datagrid) and memory - (Websphere)

Access controlled by Breeze Platform – Internally consumed, no external access

Presence (Manual) states (on disk) – Location: Cluster DB on Breeze platform

IM - (on Disk) – Location: Cluster DB on Breeze platform

Users data - (on Disk) – Location: Cluster DB on Breeze platform

Presence (Auto) states (in logs) – Location: logs in /var/log on Breeze platform

Presence (Manual) states (in logs) - Location: logs in /var/log on Breeze platform

IM details - (In logs) - Location: logs in /var/log on Breeze platform

Users data - (In logs) - Location: logs in /var/log on Breeze platform

PD “at Rest” Encryption Controls

Hardware Level Encryption may be provided by the Server platform and its storage device(s). This is done without the knowledge of the Operating System of Virtual Machine residing upon it. This is provided by the Server vendor (HP or Dell) and has the following properties:

- License(s) are required for the key management, and the individual drives typically required licenses for encryption use.
- These techniques can be employed across a RAID controller managed disk cluster.
- The encryption can be enabled to operate on certain disk pairs or it can be globally administered across multiple disk pairs. The two disk drives are usually managed as a single virtual disk.
- The passphrase for encryption may be stored locally or remotely by the central Encryption management.
- The Encryption key may be managed by:
    - Local server based key management application
    - Remote central server key management application
    - It should be noted that some customers (such as JITC for Government sector customers) desire a local server with manual key entry.
- A product example is:
    - HPE Smart Array controller w/HPE Secure Encryption
      Reference: https://h20195.www2.hpe.com/V2/GetPDF.aspx/c04318075.pdf

Since this feature is really a part of the Server product, the performance impact must be measured by both the customer and Avaya as the Solution integrator.

PD at Rest encryption controls not applicable for:

Presence (Auto) states (in memory) – Location: Memory - (GS datagrid)

Presence (Manual) states (in memory) – Location: Memory - (GS datagrid)

Users data - (In memory) – Location: Memory - (GS datagrid) and memory - (Websphere)

PD at Rest Encryption controls managed by the Breeze Platform for:

Presence (Manual) states (on disk) – Location: Cluster DB on Breeze platform

IM - (on Disk) – Location: Cluster DB on Breeze platform

Users data - (on Disk) – Location: Cluster DB on Breeze platform

Presence (Auto) states (in logs) – Location: logs in /var/log on Breeze platform

Presence (Manual) states (in logs) - Location: logs in /var/log on Breeze platform

IM details - (In logs) - Location: logs in /var/log on Breeze platform

Users data - (In logs) - Location: logs in /var/log on Breeze platform

PD “in Transit” Encryption Controls

PD in transit encryption controls use TLS 1.2 for:

Presence (Auto) states (in memory) – Location: Memory - (GS datagrid)

Presence (Manual) states (in memory) – Location: Memory - (GS datagrid)

Users data - (In memory) – Location: Memory - (GS datagrid) and memory - (Websphere)

PD in transit encryption controls managed by the Breeze Platform for:

Presence (Manual) states (on disk) – Location: Cluster DB on Breeze platform

IM - (on Disk) – Location: Cluster DB on Breeze platform

Users data - (on Disk) – Location: Cluster DB on Breeze platform

Presence (Auto) states (in logs) – Location: logs in /var/log on Breeze platform

Presence (Manual) states (in logs) - Location: logs in /var/log on Breeze platform

IM details - (In logs) - Location: logs in /var/log on Breeze platform

Users data - (In logs) - Location: logs in /var/log on Breeze platform

References:

Presence Services 8.1 Port Matrix: https://downloads.avaya.com/css/P8/documents/101057373

PD Retention Period Controls

Presence (Auto) states (in memory) – Location: Memory - (GS datagrid)

- Until reboot as long as the client is active. Data for inactive client expires in 20 mins.

Presence (Manual) states (in memory) – Location: Memory - (GS datagrid)

- Permanent unless the user is deleted by the administrator.

User’s data - (In memory) – Location: Memory - (GS datagrid) and memory - (Websphere)

- Permanent unless the user is deleted by the administrator.

Presence (Manual) states (on disk) – Location: Cluster DB on Breeze platform

- Permanent unless the user is deleted by the administrator.

IM - (on Disk) – Location: Cluster DB on Breeze platform

- Present until delivered to recipient (administrable). Archiving can be enabled by the administrator (present until offloaded)

User's data - (on Disk) – Location: Cluster DB on Breeze platform

- Permanent unless the user is deleted by the administrator.

Presence (Auto) states (in logs) – Location: logs in /var/log on Breeze platform

- Controlled by Breeze Platform

Presence (Manual) states (in logs) - Location: logs in /var/log on Breeze platform

- Controlled by Breeze Platform

IM details - (In logs) - Location: logs in /var/log on Breeze platform

- Controlled by Breeze Platform

User's data - (In logs) - Location: logs in /var/log on Breeze platform

PD Export Controls and Procedures

Presence (Auto) states (in memory) – Location: Memory - (GS datagrid)

- None

Presence (Manual) states (in memory) – Location: Memory - (GS datagrid)

- None

Users data - (In memory) – Location: Memory - (GS datagrid) and memory - (Websphere)

- None

Presence (Manual) states (on disk) – Location: Cluster DB on Breeze platform

- DB Backup/Restore which is controlled by the Breeze Platform

IM - (on Disk) – Location: Cluster DB on Breeze platform

- DB Backup/Restore which is controlled by the Breeze Platform

User's data - (on Disk) – Location: Cluster DB on Breeze platform

- DB Backup/Restore which is controlled by the Breeze Platform

Presence (Auto) states (in logs) – Location: logs in /var/log on Breeze platform

- Controlled by Breeze Platform

Presence (Manual) states (in logs) - Location: logs in /var/log on Breeze platform

- Controlled by Breeze Platform

IM details - (In logs) - Location: logs in /var/log on Breeze platform

- Controlled by Breeze Platform

Users data - (In logs) - Location: logs in /var/log on Breeze platform

PD View, Modify, Delete Controls and Procedures

Presence (Auto) states (in memory) – Location: Memory - (GS datagrid)

- Administrator can view, delete the data.

Presence (Manual) states (in memory) – Location: Memory - (GS datagrid)

- Administrator can view, delete the data.

User's data - (In memory) – Location: Memory - (GS datagrid) and memory - (Websphere)

- Administrator can view, delete the data.

Presence (Manual) states (on disk) – Location: Cluster DB on Breeze platform

- Administrator can view, delete the data.

IM - (on Disk) – Location: Cluster DB on Breeze platform

- For Offline messages the administrator can delete the users. For Archived messages (if enabled) it is up to the administrator to manage the retention period.

User's data - (on Disk) – Location: Cluster DB on Breeze platform

- Administrator can view, delete the data.

Presence (Auto) states (in logs) – Location: logs in /var/log on Breeze platform

- Controlled by Breeze Platform

Presence (Manual) states (in logs) - Location: logs in /var/log on Breeze platform

- Controlled by Breeze Platform

IM details - (In logs) - Location: logs in /var/log on Breeze platform

- Controlled by Breeze Platform

User's data - (In logs) - Location: logs in /var/log on Breeze platform

PD Pseudonymization Operations Statement

Presence (Auto) states (in memory) – Location: Memory - (GS datagrid)

- None

Presence (Manual) states (in memory) – Location: Memory - (GS datagrid)

- None

User's data - (In memory) – Location: Memory - (GS datagrid) and memory - (Websphere)

- None

Presence (Manual) states (on disk) – Location: Cluster DB on Breeze platform

- None

IM - (on Disk) – Location: Cluster DB on Breeze platform

- None

User's data - (on Disk) – Location: Cluster DB on Breeze platform

- None

Presence (Auto) states (in logs) – Location: logs in /var/log on Breeze platform

- None

Presence (Manual) states (in logs) - Location: logs in /var/log on Breeze platform

- None

IM details - (In logs) - Location: logs in /var/log on Breeze platform

- None

User's data - (In logs) - Location: logs in /var/log on Breeze platform

- None

Chapter 11: Data Privacy Controls Addendum for Avaya Aura® Media Server

This addendum applies to Avaya Aura® Media Server, Version 7.8

Data Categories Containing Personal Data (PD)

Primary Category:

- User's audio packets are temporarily stored in memory while they are mixed and transmitted.
- User's video packets are temporarily stored in memory while they are relayed.

Secondary Category

- System Logs may include information about DTMF tones received from users. These DTMF tones may include personal information such as passcode, credit card information, or other personal passcode information depending on the business solution where AAMS is deployed. Note that if AAMS' data masking feature is enabled, the DTMF information is not logged.
  Location: Stored on the filesystem.

PD Human Access Controls

End users do not have access to the information saved in memory or logs saved on the filesystem.

Administrators can access to the log files on the filesystem using Operating system root access through SSH interface.

PD Programmatic/API Access Controls

There is an external programmatic access over HTTPs/TLS v1.2 (REST APIs) or SIPs/TLS (MSML protocol) to create, modify and remove media sessions. Media sessions are identified by unique ids consisting of random strings that do not contain personal information.

PD "at Rest" Encryption Controls

Filesystem is not encrypted, but there is no personal data stored on the system, except DTMF tones information in the logs when the data masking feature is turned off.

PD “in Transit” Encryption Controls

Media packets, including DTMF tone entries, can be encrypted based on the system configuration. AES-128/256 HMAC 32/80 are supported for media encryption.

Logs can be download over a TLS 1.2 connection from the AAMS Element Manager UI or via secure file transfer using scp on port 22.

References:

Aura Media Services 8.0 Port Matrix: https://downloads.avaya.com/css/P8/documents/101051297

PD Retention Period Controls

Log retention period cannot be configured. The system of the log file can be configured causing the oldest records to be erased when space is not available to write new records.

PD Export Controls and Procedures

The product does not provide an export capability for downloading information pertaining to a specific user.

The product does not provide an export capability for downloading the logs relating to a specific user. The full log file can be accessed and downloaded from the Element Manager and the ssh interface discussed above.

PD View, Modify, Delete Controls and Procedures

None

PD Pseudonymization Operations Statement

Media sessions associated with users are identified by Real Time Protocol (RTP) Synchronization Source (SSRC) or Contributing Source (CSRC) fields. Similarly, media sessions are identifiable through unique random ids at the REST/MSML API level when an external server creates, modifies and deletes media sessions in AAMS.

Chapter 12: Data Privacy Controls Addendum for Avaya Aura® Appliance Virtualization Platform (AVP)

This addendum applies to Avaya Aura® Appliance Virtualization Platform (AVP), Version 8.1.2.

Data Categories Containing Personal Data (PD)

Primary Category:

- AVP by itself does not contain any user data. However, Virtual Machines running on AVP Host may contain user data. Please consult the guides for that product for the appropriate information.
- SSH userids and their passwords. These identify administrative users of AVP, which can be local or Active Directory users.

  Location: Configuration file

PD Human Access Controls

Human Access to Appliance Virtualization Platform to add, modify or delete an SSH userid is through the AVP host command line interface. The administrator must be authenticated with a valid password.

PD Programmatic/API Access Controls

AVP has programmatic access available via the SMGR Solution Deployment Manager (SDM) and Windows based SDM client. This programmatic access control does not have any access to PD items described above.

PD “at Rest” Encryption Controls

AVP does not provide any mechanisms for encryption at Rest. The OVAs being deployed on AVP should be deployed with encryption enabled to protect private and sensitive data.

PD “in Transit” Encryption Controls

While in transit from and to AVP, the PD items described above are protected by SSH.

Event logs are collected on the local disk. These log files may be transferred by one of two methods:

a) They may be transferred via secure FTP
b) As of Release 8.1, the customer may direct that the log files be transmitted to the AVP Utilities (which acts as a remote Syslog Server) using TLS. AVP Utilities can then forward the syslog to up to 5 external syslog servers using TLS. The security of log files on the log servers is entirely the responsibility of the customer or customer's service provider.

References:

AVP 8.1 Port Matrix: https://downloads.avaya.com/css/P8/documents/101057977

PD Retention Period Controls

No personal data is stored on AVP. However, snapshots for Virtual Machines deployed on AVP host may remain on the system unless explicitly deleted. These snapshots may contain personal information. Hence AVP 8.1.2 offers a feature to automatically delete snapshots on the system. The automatic deletion for snapshots can be configured between 1 and 30 days.

PD Export Controls and Procedures

N/A

PD View, Modify, Delete Controls and Procedures

N/A

PD Pseudonymization Operations Statement

N/A

Chapter 13: Data Privacy Controls Addendum for G430 and G450 Media Gateways

This document describes how Personal Data (PD) is managed by the G430 and G450 Media Gateways.

Data Categories Containing Personal Data (PD)

Personal Data (PD) may be stored on the G430 / G450 gateway only if the Standard Local Survivability (SLS) feature is configured on the gateway. SLS is an optional feature that provides limited call processing functionality if the master call controller (i.e. Aura Communication Manager) is inaccessible.

If SLS is configured, PD can be included within SLS's station configuration data. This PD may subsequently be viewed in SLS station configuration data, Call Record Detail (CDR) logs, and in the syslog cache. The PD stored may include name, extension, called number, or IP address.

All G430 and G450 Media Gateway data is stored in flash memory that is not directly accessible by a user. Instead, this data can only be accessed via gateway specific CLI commands and/or SNMP.

PD Human Access Controls

PD may only be configured and viewed by:

1) Logging into the gateway using ssh or telnet and manually invoking the gateway's CLI commands.
2) Accessing the gateway through SNMP commands.

PD can be viewed via CLI commands by any user with login privileges (i.e. read access) and

may be administered or cleared by any user with admin privileges (i.e. read-write access).

PD can be viewed via SNMP by any user with read access and may be administered or cleared by any user read-write access

For further details see the following documentation at https://support.avaya.com:

- G430 Administration Guide
- G450 Administration Guide
- G430 CLI Reference Guide

- G450 CLI Reference Guide.
- G430 SNMP MIB
- G450 SNMP MIB

PD Programmatic/API Access Controls

PD can only be configured and viewed programmatically by:

1) Accessing the gateway through SNMP.
2) Creating an application that can automate logging into the gateway using ssh or telnet and invoking the gateway's CLI commands.

For further details see the following documentation at https://support.avaya.com:

- G430 Administration Guide
- G450 Administration Guide
- G430 CLI Reference Guide
- G450 CLI Reference Guide.
- G430 SNMP MIB
- G450 SNMP MIB

PD "at Rest" Encryption Controls

N/A

Communication Manager collects statistics (from the gateway) for call detail recording.

If the Syslog feature is enabled, then the issue of temporary storage of log events is not an issue since this data is streamed to the customer's log server.

PD "in Transit" Encryption Controls

Only SCP or SNMPv3 should be used to provide encrypted transmission of PD.

Only SSH should be used to provide encrypted login sessions when invoking CLI commands.

Event logs are collected on the local disk. Syslog maintained log files may be transferred by one of two methods:

a) They may be transferred via SCP.
b) As of Release 8.1, the customer may direct that the log files be transmitted to remote log Server(s) using Syslog over TLS. The security of log files on the log servers is entirely the responsibility of the customer or customer's service provider.

References:

G430 & G450 8.1 Port Matrix: https://downloads.avaya.com/css/P8/documents/101056833

PD Retention Period Controls

Station Configuration is retained permanently until manually erased by the administrator.

A Log Retention feature was introduced in Release 8.1.2 that provides the ability to define the maximum number of days syslog logs will retained on the gateway. Logs that are older than the configured log retention period will not be available.

As of Release 8.1.2, the following two CLI commands provide the ability to view and set the duration that syslog logs are retained:

- show logging file retention
- set logging file retention <retention_days>
  retention_days defines the period of time in days that log content will be retained.

It must be either a value between 1 and 9999, inclusive (default value is 30 days) or "unlimited" CDR and syslog data is retained permanently but is limited by the syslog cache size (72 hours capacity for normal traffic).

PD Export Controls and Procedures

PD may be exported via SNMP or by using the following CLI commands to transfer the data using scp, ftp, tftp, or usb:

Station Configuration commands:

- copy running-config – copy gateway's running configuration (including station configuration)
- copy startup-config – copy gateway's startup configuration (including station configuration)
- backup config – backup gateway's configuration (including station configuration)

CDR data:

- copy cdr-file – copy CDR data

Syslog data:

- copy syslog-file – copy syslog data

PD View, Modify, Delete Controls and Procedures

Station Configuration commands:

- set sls – enable / disable sls
- sls – enter sls configuration
  - show station – view SLS station configuration
  - station – set SLS station extension
    - set name – set / change SLS Station name
  - clear station – clear SLS station configuration
- show running-config – view gateway's running configuration (including station configuration)
- show startup-config – view gateway's startup configuration (including station configuration)

CDR data:

- show logging cdr file content – view CDR content

- clear logging cdr file – clear CDR content

Syslog data:

- set logging file - enable/disable/filter syslog content
- show logging file content – view syslog content
- clear logging file – clear syslog content

PD Pseudonymization Operations Statement

N/A

Index