Avaya Subscription Reference

Release 1.0
Issue 13
July 2023

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA LLC, 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 LLC OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

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

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only 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.

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya

including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Java is a registered trademark of Oracle and/or its affiliates.


Java
POWERED

Contents

Chapter 1: Introduction 9
Purpose 9
Change history 10
Intended audience 17
Chapter 2: Overview and architecture 18
Overview of Avaya OneCloud™ Subscription 18
Overview of Usage Metering 19
Usage Metering components 19
Supported browsers 20
New in this release 21
Avaya OneCloud™ Subscription architecture 21
Application sharing between two or more Avaya OneCloud™ Subscription systems 23
License and software enablement 24
Avaya OneCloud™ Subscription system process flow 25
Obtaining the Access key and Secret key 28
Avaya UC and CC applications supported by Avaya OneCloud™ Subscription 30
Order type and associated available features 33
Avaya OneCloud™ Subscription system deployment models 33
Considerations for configuring Avaya OneCloud™ Subscription systems of the same subscription offer in multiple Usage Metering Collectors 36
Avaya OneCloud™ Subscription service usage reports 37
Chapter 3: Usage Metering Collector installation 38
Checklist for installing Usage Metering Collector 38
Planning and pre-installation configuration 39
Prerequisite knowledge and application for installing and using Usage Metering Collector 39
System requirements to deploy Usage Metering 40
Required URLs for Usage Metering Collector 42
Disk partition encryption for Data Privacy 42
Configuring the non-transparent proxy details in the bash_profile file 43
Setting the time zone 44
Installing Usage Metering Collector 45
Post-installation configuration 46
Configuring non-transparent proxy in the Usage Metering Collector 46
Chapter 4: Usage Metering Collector configuration 48
Usage Metering configuration checklist 48
Creating an initial user for Usage Metering Collector 51
Configuration settings 52
Configuring connectivity between Usage Metering and Avaya back-office systems 52
Configuring a name for the Usage Metering Collector 53

Configuring SMTP mail server to send email notifications..... 53
Alerts..... 54
Configuring session timeout and failed login attempt threshold..... 56
Enabling EASG login for remote access..... 57
Configuring security banner for the login page..... 58
User management..... 58
Creating a user..... 58
Forcing a user to change the password on the first login..... 59
Editing a user..... 59
Enabling or disabling a user account..... 59
Resetting the Usage Metering Collector password..... 60
Viewing the login history of a user..... 60
Deleting a user..... 61
Changing the Usage Metering Collector password..... 61
Usage Metering Collector password policy..... 61
Default password policy for Usage Metering Collector user accounts..... 61
Configuring custom password policy for Usage Metering Collector user accounts..... 62
Configuring a password reset policy for the Usage Metering Collector user accounts..... 64
Usage Metering Collector password reset policy parameters..... 65
Configuring an account lockout policy for Usage Metering Collector user accounts..... 66
Account lockout policy parameters..... 67
Setting the limit for concurrent login sessions for the Usage Metering Collector web interface..... 70
Enabling SNMP keep-alive trap messages from Usage Metering Collector..... 71
Usage Metering keep-alive parameters..... 72
Enabling or disabling hostname validation..... 72
Installing and configuring Advanced Intrusion Detection Environment utility..... 73
Chapter 5: Certificate management..... 75
SSL certificate..... 75
Generating a certificate signing request..... 75
Installing the CSR response..... 76
Generating a self-signed certificate..... 77
Installing a server certificate..... 77
CA SSL certificate..... 79
Retrieving certificate from a standalone Avaya WebLM..... 79
Installing an outbound certificate..... 80
Viewing installed certificates..... 80
Chapter 6: Avaya OneCloud™ Subscription system management in Usage Metering Collector..... 82
Avaya OneCloud™ Subscription system..... 82
Data source applications..... 83
Mandatory applications in an Avaya OneCloud™ Subscription system..... 85
Avaya OneCloud™ Subscription system management..... 86
WebLM management..... 86

Application management 92
Technical onboarding of applications to the Avaya Global Registration Tool 123
Managing the Avaya OneCloud™ Subscription system state 126
Migration of applications from perpetual licenses to subscription license 126
Prerequisites for migrating applications from perpetual licenses to subscription license 126
Migrating applications from perpetual licenses to subscription license 127
Application upgrade 128
Chapter 7: Usage Metering backup, restore, and geo-redundancy 130
Usage Metering server failure scenarios 130
Data collection failure and recovery 130
Usage Metering backup and restore 131
Usage Metering backup 131
Usage Metering restore 132
Restoring Usage Metering 132
Uninstalling Usage Metering Collector 134
Restoring Usage Metering Collector after uninstallation 135
Usage Metering in a geo-redundant environment 135
Verifying data collection on primary and secondary Usage Metering 136
Moving Usage Metering Collector between data centers 136
Preparing a cold standby server 137
Secondary data center recovery process 137
Moving service back to the primary data center 138
Testing the recovery process 138
Chapter 8: Upgrade Usage Metering Collector 139
Upgrading Usage Metering Collector 139
Chapter 9: Troubleshooting 140
No more mirrors to try error message is displayed during Usage Metering Collector installation. 140
Usage Metering SNMP MIB file location 141
Verifying Usage Metering Collector connectivity and operating system parameters 141
Viewing the recent logs and downloading the log files 142
Viewing the audit log of user activity in Usage Metering 143
Usage Metering does not display data when you log in by using the same window after two days 143
Usage Metering Collector cannot recognize a web proxy CA certificate 144
Usage Metering Collector did not refresh the subscription license 145
Usage Metering Collector cannot connect to Avaya Aura® Messaging 145
Alert management 146
Viewing Usage Metering alerts 146
Usage Metering alerts 146
Clearing a resolved alert 150
Application maintenance support 151
Chapter 10: Resources 152
Viewing the Avaya OneCloud™ Subscription online Help 152

Finding documents on the Avaya Support website 152
Avaya Documentation Center navigation 153
Support 154
Using the Avaya InSite Knowledge Base 154
Appendix A: Port assignment 155
Port assignments 155
Glossary 157

Chapter 1: Introduction

Purpose

This document provides information about how to:

- Migrate your on-premise applications that are licensed under perpetual licenses to subscription license.
- Manage WebLM in an Avaya OneCloud™ Subscription system.
- Manage Avaya Unified Communications (UC) and Contact Center (CC) applications in an Avaya OneCloud™ Subscription system.
- Perform Technical Onboarding of applications in the Avaya Global Registration Tool.
- Manage the Avaya OneCloud™ Subscription system state.
- Upgrade applications that are entitled by a subscription license.

This document also provides information about the following aspects of the Usage Metering Collector:

- Installation
- Upgrade
- Deployment
- Configuration
- Backup and restore
- Maintenance
- Troubleshooting

Change history

Release number	Issue number	Date	Summary
1.0	13	July 2023	Added the following information in the Verifying Usage Metering Collector connectivity and operating system parameters topic: • Command to verify the connectivity of Usage Metering Collector installed on RHEL 8.x.
	12	January 2023	Updated the following: • The document title from *Avaya OneCloud™ Subscription Reference* to *Avaya Subscription Reference*. • The Overview of Avaya OneCloud™ Subscription topic with information about rebranding of Avaya OneCloud™ Subscription to Avaya Subscription.
	11	November 2022	Removed the following information from the Installing Usage Metering Collector and Restoring Usage Metering topics: • Disable the postgresql module when installing the Usage Metering Collector on RHEL 8.x.
	10	March 2022	Added information about the following: • Installing and configuring the Advanced Intrusion Detection Environment (AIDE) utility for Usage Metering. • Configuring an account lockout policy for the Usage Metering Collector user accounts. • The password.max.changes.per.day and password.warning.days.before.expiration password policy parameters. • Installing Usage Metering on RHEL 8.x. Updated the following information: • Minimum configurable value of the password.max.age.days password policy parameter. • Description for the **Account lockout threshold (failed login attempts)** and **Delay after 3 failed login attempts (seconds)** fields. • Installing Usage Metering Collector. • Restoring Usage Metering.

Table continues…

Release number	Issue number	Date	Summary
	9	October 2021	Added information about enabling or disabling hostname validation for SSL connections.
	8	July 2021	Added information about the following: • Configuring a password reset policy. • Enabling keep-alive trap messages from the Usage Metering Collector. Updated the following information: • Resetting the Usage Metering Collector password. • `UM Alert 990` with information about the keep-alive trap messages.
	7	June 2021	Added information about the following: • SNMP v3 configuration. • Setting the limit for the number of concurrent login sessions to the Usage Metering Collector web interface.
	6	March 2021	Updated the following information: • Procedure for configuring connectivity between Usage Metering and Avaya back-office systems with information about noting down the Usage Metering Collector ID. • Usage Metering Collector starts collecting and submitting usage data every day at 3:20 a.m. local time. • Procedure for viewing and downloading the recent logs with information about logs older than 30 days are automatically deleted.

Table continues…

Release number	Issue number	Date	Summary
	5	January 2021	Updated the following information: • Procedure for configuring the non-transparent proxy details in the `bash_profile` file with information about configuring the user name and password of a proxy server that requires authentication. • Procedure for configuring the non-transparent proxy details in the Usage Metering Collector. • Operating system requirements section. • Prerequisites and process for adding Avaya Callback Assist Application Server section with information about the **CORE** and **ADDITIONAL** deployment type options for adding multiple Avaya Callback Assist Application Servers based on the deployment model. • Checklist for adding the on-premise applications that are entitled by the subscription license to an Avaya OneCloud™ Subscription system. • Usage Metering Collector installation, restore, and upgrade topics.

Table continues…

Release number	Issue number	Date	Summary
	4	December 2020	Added information about the following: • Default password policy for the Usage Metering Collector user accounts. • Configuring custom password policy for the Usage Metering Collector user accounts. • Checklist for installing Usage Metering Collector. • Clearing a resolved alert. • Creating a read-only user account for the Avaya Aura® Experience Portal local Postgres database. • Exporting the System Manager-signed root CA certificate from System Manager. • Exporting the SIP CA-signed Demo certificate from System Manager. • Verification of duplicate application IP address when adding applications of the same application type to one or more Avaya OneCloud™ Subscription systems that are configured on the same Usage Metering Collector. • Viewing the Avaya OneCloud™ Subscription online Help. • Minimum supported version numbers for SAL Gateway and SLA Mon™ in the list of supported applications by Avaya OneCloud™ Subscription. Updated the following information: • Hardware requirements for Usage Metering Collector containing up to 20 and more than 20 Avaya OneCloud™ Subscription systems. • Operating system requirements with information about the ability to install the following third-party antivirus software on the operating system where Usage Metering Collector is installed: CylancePROTECT version 2.1.1564 • Procedure for identifying the root CA certificate installed in Avaya Aura® Messaging and installing it in Usage Metering Collector. • Procedure for enabling SSL connection between Usage Metering and Avaya Callback Assist. • Procedure for enabling SSL connection to the CMS database.

Table continues…

Release number	Issue number	Date	Summary
			• Procedure for installing the root certificate used by Avaya IX™ Messaging for authentication in Usage Metering Collector.

Table continues…

Release number	Issue number	Date	Summary
	3	October 2020	Added information about the following: • SNMP MIB file location. • Prerequisites for adding Avaya Callback Assist as a data source application to an Avaya OneCloud™ Subscription system. • Prerequisites for sharing Avaya Aura® Experience Portal between multiple Avaya OneCloud™ Subscription systems. • Support for Avaya Aura® Experience Portal that uses external Microsoft SQL database. • New **Database IP** field when adding Avaya Aura® Experience Portal to an Avaya OneCloud™ Subscription system. • Troubleshooting for `No more mirrors to try` message shown during Usage Metering Collector installation. • Mandatory applications for the UC Attendant, UC Messaging Speech, UC Messaging Transcription, and Callback Assist service bundles. • Minimum supported version number for Avaya Workplace (for Mac / Windows). • Checklist for adding the on-premise applications that are entitled by the subscription license to an Avaya OneCloud™ Subscription system. Updated the following information: • The user account that you create as part of the prerequisites for adding Application Enablement Services must be created in the `susers` Linux group. • Caveat for installing a subscription license on a WebLM server that already hosts an activated perpetual license. • Changed the following product names: - Avaya IX™ Subscription to Avaya OneCloud™ Subscription - Equinox Mobility — IOS/ Android to Avaya Workplace (Mobility for IOS / Android) - Avaya Equinox® VDI to Avaya IX™ Workplace VDI

Table continues…

Release number	Issue number	Date	Summary
			- Avaya Equinox® Attendant to Avaya IX™ Workplace Attendant - Avaya Communicator for Microsoft Lync to Avaya Workplace Integration with Skype for Business
	2.2	August 2020	Added information about the following: • Enabling SSL connection between Experience Portal Postgres database and Usage Metering. Updated the following information: • Procedure for creating a CMS user with secure access permission to the CMS database. • Internet access requirements in System requirements to deploy Usage Metering on page 40. • Required URLs for Usage Metering Collector.
	2.1	August 2020	Added information about the following: • Installing multiple Avaya Call Management System (CMS) and Avaya IX™ Messaging applications that are part of the same Avaya OneCloud™ Subscription system requires separate WebLM servers. • Considerations for configuring Avaya OneCloud™ Subscription systems that are part of the same subscription offer in multiple Usage Metering Collectors.

Table continues…

Release number	Issue number	Date	Summary
	2	July 2020	Added information about the following: • Command to verify connectivity between Usage Metering and Avaya back-office systems. • Password reset support. • Disk partition encryption for Data Privacy. • Required URLs for Usage Metering Collector. • Avaya Aura® Session Manager and Avaya Aura® Experience Portal are non-shareable applications. • New alert number 606. • Prerequisites for adding the following data source applications to an Avaya OneCloud™ Subscription system: - Avaya Call Management System - Application Enablement Services - Avaya Aura® Messaging - Avaya IX™ Messaging - Avaya Aura® System Manager - Avaya Aura® Experience Portal Updated the following information: • Minimum supported version number for Avaya Aura® Application Enablement Services.
	1	May 2020	This is the first release of Avaya OneCloud™ Subscription.

Intended audience

This document is intended for Avaya Professional Services personnel, Avaya Business Partners, and Avaya customers who have placed a new order for Avaya UC and CC applications under an Avaya OneCloud™ Subscription offer or who want to migrate their existing on-premise applications from perpetual licenses to subscription license.

Chapter 2: Overview and architecture

Overview of Avaya OneCloud™ Subscription

Note:

Avaya OneCloud™ Subscription is rebranded to Avaya Subscription. Read all instances of Avaya OneCloud™ Subscription as Avaya Subscription in this document.

Avaya OneCloud™ Subscription allows enterprise customers to procure a fixed quantity of Avaya Unified Communications (UC) and Contact Center (CC) software applications. In the current release of Avaya OneCloud™ Subscription, fixed quantity refers to the quantity that is committed for a specific service as a part of your subscription contract. For example, you can order an Avaya contact center solution for a capacity of 1000 agents.

This fixed quantity is generally the nominal operating capacity requirement of your organization. With Avaya OneCloud™ Subscription, you can order an Avaya UC and CC software infrastructure dynamically, without placing software license or support orders.

Avaya OneCloud™ Subscription allows an overage, which is an additional capacity that you are entitled to over the Fixed Quantity Subscription, without any additional charges. For example, a Fixed Quantity Subscription may entitle a 20% overage. If you enter a contract for a Fixed Quantity Subscription for 1000 agents over 3 years, you can use an additional 20%, that is, use the capacity for up to 1200 agents without being charged additionally.

For information about the actual percentage of entitled overage, refer to your Avaya OneCloud™ Subscription Offer Definition document.

You can order a new Avaya OneCloud™ Subscription system or migrate your existing on-premise applications from perpetual licenses to a subscription license.

Avaya OneCloud™ Subscription is an "Application Use as a Service" solution that allows you to subscribe for a fixed quantity of Avaya UC and CC software (OPEX - subscription) instead of paying for the quantity of capacity of use of the software (CAPEX - perpetual). The billing is done on a recurring basis as per your subscription contract.

You can use Avaya OneCloud™ Subscription in both enterprise or partner-hosted deployment model, and cloud deployment model.

Avaya OneCloud™ Subscription uses Usage Metering to determine the service usage.

Avaya OneCloud™ Subscription uses other Avaya back-office systems that respond when existing infrastructure applications or application users may need to be scaled, or new applications are added to the existing infrastructure.

Overview of Usage Metering

Usage Metering is a component of a usage-based enterprise architecture.

The roles of Usage Metering are:

- Collect usage event records from the usage data sources.
- Integrate with Avaya assurance systems.
- Use processes for on-boarding to support existing Avaya business processes.

Usage Metering operationalizes Avaya post-paid offers that are historical and usage-based.

Usage Metering architecture supports reliable usage data collection offers.

Note:

Usage Metering collects certain personal data and sends it to Avaya for:

- Monitoring that the service usage adheres to the subscribed quantity.
- Generating usage reports that are required for billing purposes.

Examples of such personal data are email addresses, handles, extension numbers, mailbox numbers, agent IDs, and agent phone numbers.

Usage Metering uses data encryption to transmit and store this data in the Avaya back-office systems.

Usage Metering components

Deployment components

Location	Component	Purpose
Partner or customer data center	Usage Metering Collector	• Collects the service usage data from data sources. For example, it collects the number of logged-in agents and agent login and logout data from CMS. • Sends the service usage data to the Usage Metering Processor for further processing.
Avaya cloud	Usage Metering Processor	Calculates the service usage data and sends the data to the Avaya back-office systems for usage reporting and invoicing.
Partner or customer data center	SAL Concentrator	Receives Usage Metering alerts that the SAL gateway delivers. Provides an Avaya technician with remote access to Usage Metering by using the SAL gateway.
Partner or customer data center	SAL GW	Receives alerts that are generated by Usage Metering. Enables an Avaya technician to access Usage Metering.

Table continues…

Location	Component	Purpose
Partner or customer data center	SMTP Relay	Delivers Usage Metering notifications and alerts by using email (SMTP) to the Partner or customer.
Partner or customer data center	SNMP Trap Host	Receives Usage Metering alerts by using the SNMP Trap Host. This is an optional feature for the Partner or customer.
Partner or customer data center	Data source	Collects and stores raw usage data based on the use of the application by the Partner or customer. For example, CMS provides the number of agents logged in to the system.

You can use one of the following to deploy Usage Metering:

- Single data center
- Geo-redundant data center

  To prepare a cold standby setup, see Preparing a cold standby server on page 137.

You can setup a cold-standby Usage Metering in the secondary data center.

Networking Considerations

Usage Metering must have connectivity to the data sources to collect usage data.

In a geo-redundant deployment, Usage Metering must have connectivity to the data sources in the primary and secondary data centers.

Each meter requires a primary data source and an optional secondary data source.

If the system fails to collect usage data from a meter by using the primary data source, the system collects usage data from the corresponding meter by using the secondary data source.

If the primary and the secondary data source are not working, the system raises an alert and notifies the user.

For each meter, you must configure the following for the primary and optional secondary data source:

- IP or hostname
- Ports
- Credentials

Supported browsers

Usage Metering supports the latest versions of the following browsers:

- Mozilla Firefox
- Google Chrome

New in this release

There are no new features in the July 2023 update of Avaya Subscription Release 1.0.

Avaya OneCloud™ Subscription architecture

Avaya OneCloud™ Subscription allows you to dynamically use the subscribed Avaya UC and CC applications. After you install and configure the Avaya Usage Metering Collector, you can use the Usage Metering Collector to add or remove the subscribed UC and CC applications from the Avaya OneCloud™ Subscription system depending on your service bundle order.

A service bundle is a collection of services that are grouped. An example of a service is the Avaya Aura® Experience Portal IVR service. An example of a service bundle is Calling plus Voicemail.

Usage Metering Collector collects usage data on a daily basis from data source applications, such as Avaya Call Management System (CMS), that are part of your Avaya OneCloud™ Subscription system. Usage Metering Collector uploads the usage data to the Usage Metering Processor. The Usage Metering Processor calculates the service usage data and sends the data to the Avaya back-office systems for usage reporting and invoicing.

You must set the time zone for daily usage calculations. For more information, see Setting the time zone on page 44.

Avaya OneCloud™ Subscription system is a collection of Avaya UC and CC applications (Single or Geo-redundant data centers) connected to one or more WebLM servers for licensing.

For more information about Avaya OneCloud™ Subscription system and licensing, see Avaya OneCloud Subscription system on page 82 and License and software enablement on page 24.

Avaya OneCloud™ Subscription supports sharing of applications, such as Avaya Aura® Messaging or CMS, between two or more Avaya OneCloud™ Subscription systems.

For more information, see Application sharing between two or more Avaya OneCloud Subscription systems on page 23.

Avaya OneCloud™ Subscription uses:

- Usage Metering to manage the Avaya OneCloud™ Subscription system.
- SAL Gateway for remote maintenance support.

If you have configured a secondary data center for High Availability, you must also configure a secondary Usage Metering and a secondary SAL Gateway.

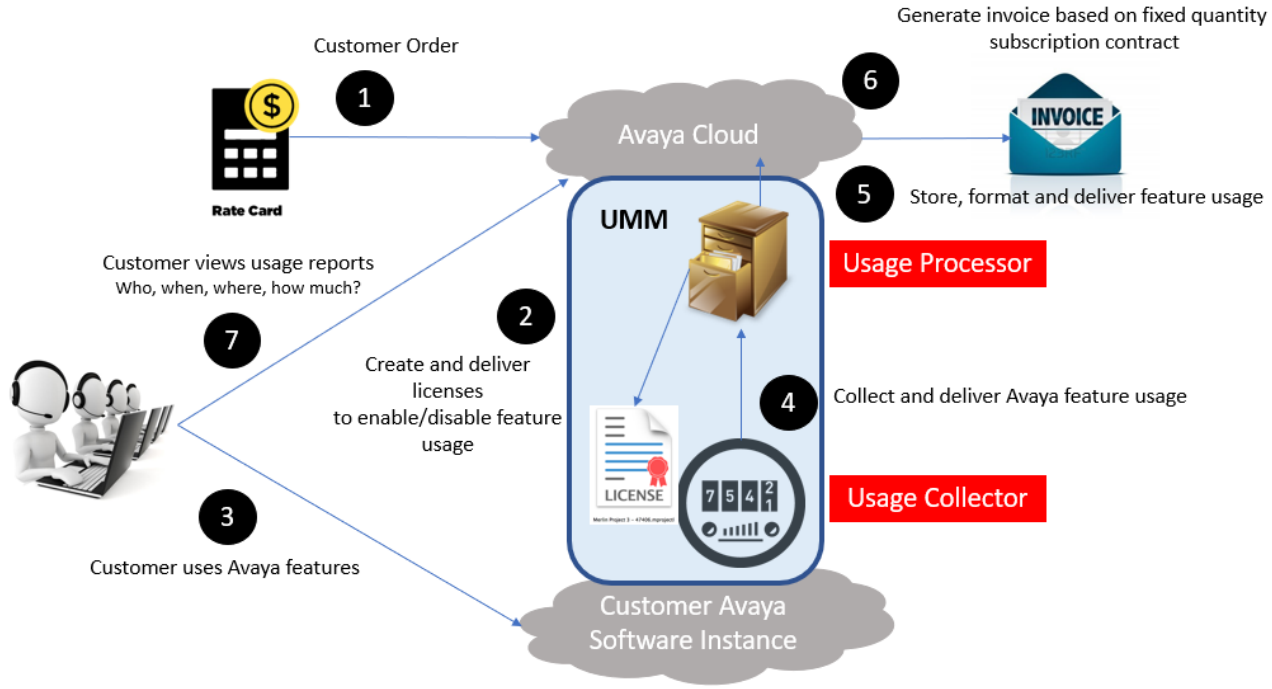
Depending on your requirement and service bundle order type, you can use different Avaya UC and CC applications in different Avaya OneCloud™ Subscription systems. For example, you can subscribe for two Avaya OneCloud™ Subscription systems for your organization, one for the call center and one for the back office. You can choose to use Call Recording in the Avaya OneCloud™ Subscription system for the call center, and remove it from the Avaya OneCloud™ Subscription system for the back office.

For more information, see Avaya OneCloud Subscription system deployment models on page 33.

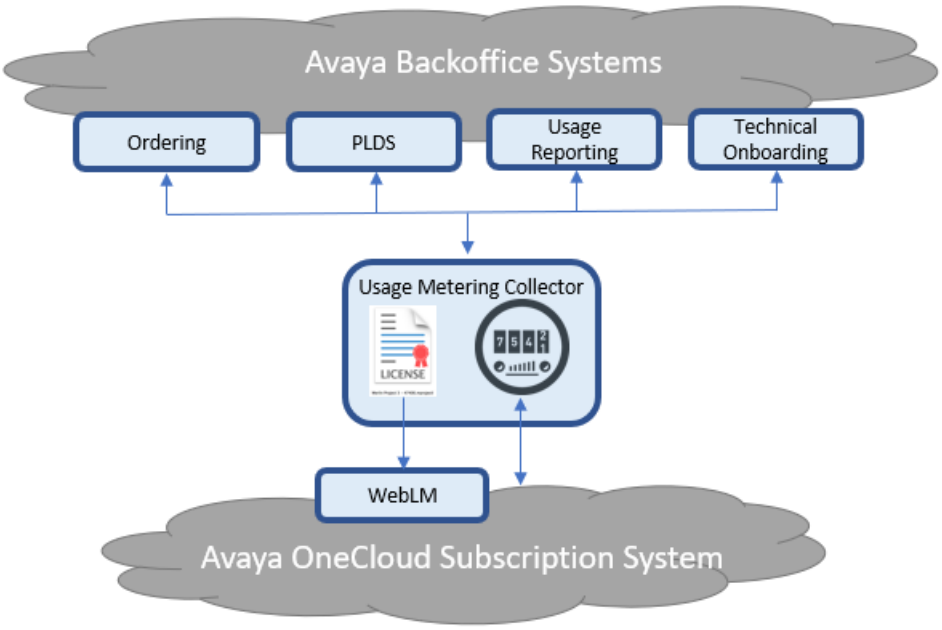
Avaya OneCloud™ Subscription system is a collection of Avaya UC and CC premise-deployed applications that are integrated with Avaya IT applications to enable an OpEX business model.

Architecture diagrams

The following is the architecture diagram of Usage Metering:



The following diagram depicts how an Avaya OneCloud™ Subscription system interacts with Usage Metering and other Avaya back-office systems:



Application sharing between two or more Avaya OneCloud™ Subscription systems

Avaya OneCloud™ Subscription supports sharing of applications, such as Avaya Aura® Messaging or CMS, between the Avaya OneCloud™ Subscription systems that are configured on the same Usage Metering Collector. For example, if you have subscribed for two Avaya OneCloud™ Subscription systems, one for the call center and one for the back office, you can share the same CMS between the two Avaya OneCloud™ Subscription systems, provided these two systems are configured on the same Usage Metering Collector. Shared applications are not independently charged.

Shared applications are applications, entitled by an Avaya OneCloud™ Subscription offer, that are "network-centric" in nature and can be used by multiple Avaya OneCloud™ Subscription systems.

Non-shareable applications

You cannot share the following applications between two or more Avaya OneCloud™ Subscription systems:

- Communication Manager.
- Session Manager.
- If the application that you want to share, for example, CMS, is entitled by the Avaya OneCloud™ Subscription offer, you can share this application only between Avaya OneCloud™ Subscription-entitled systems. You cannot share this application in a system that is non-Avaya OneCloud™ Subscription. For example, you cannot share a CMS that is licensed under a subscription license with a Communication Manager that is licensed under a perpetual license.

Related links

Sharing an application between multiple Avaya OneCloud Subscription systems on page 121

License and software enablement

Avaya OneCloud™ Subscription system is a collection of UC and CC applications (Single or Geo-redundant data centers) connected to one or more WebLM servers, depending on your deployment model, for licensing.

After you install and configure the Usage Metering Collector, you must add the WebLM server to your Avaya OneCloud™ Subscription system by using the Usage Metering Collector. After the Usage Metering Collector successfully registers to the WebLM server, Usage Metering automatically retrieves the subscription license for the subscribed applications from the Avaya back-office systems and installs it on the WebLM server.

Avaya OneCloud™ Subscription uses the subscription license to enable application entitlements and capacities.

A subscription license has an expiration period of 30 days. Usage Metering automatically refreshes the subscription license after every 20 days. If Usage Metering is unable to refresh the license after 20 days, it sends an alert. If the subscription license is not replaced within 30 days, then after 30 days, the applications run in a license error mode.

For more information, see Usage Metering Collector did not refresh the subscription license on page 145.

If you want to increase your fixed quantity subscription, you must place a change order request with Avaya. You need not perform any changes on the WebLM server for the subscription license.

If you add or remove an application from your Avaya OneCloud™ Subscription system, Usage Metering automatically updates the WebLM server with the new application request.

Note:

You can also use the **Synchronize Applications** option, which is available on the **WEBLMS** tab, to manually synchronize the updated application list with the WebLM server.

After a new application request is received, the WebLM server notifies the Usage Metering Collector for the license entitlement.

The Usage Metering Collector grants the subscription license entitlement if the Avaya OneCloud™ Subscription system status is in a good standing.

The following criteria determine in good standing status:

- Billing status is good (offer dependent).
- All on-premise Avaya UC and CC applications that are part of your Avaya OneCloud™ Subscription system order are configured in the Avaya OneCloud™ Subscription system in Usage Metering Collector, and usage data of the applications is collected.

- The on-premise applications that are added to the Avaya OneCloud™ Subscription system are of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version.

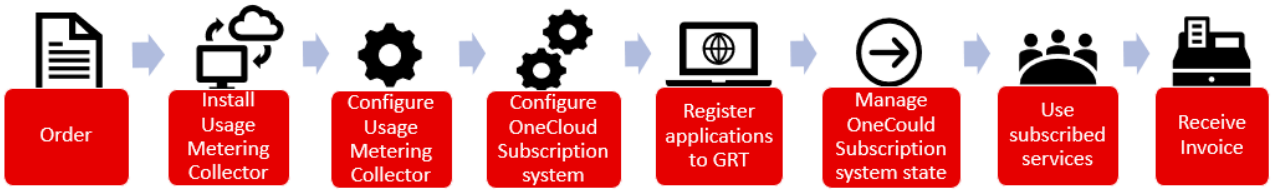
If the status is not in good standing, Avaya can disable the service by not renewing the subscription license.

Related links

WebLM management on page 86

Avaya OneCloud™ Subscription system process flow

The following diagram shows the process flow of an Avaya OneCloud™ Subscription system:



The following table provides information about the process flow of an Avaya OneCloud™ Subscription system:

No.	Task	Action / Description
1	Order	If you want to migrate your existing on-premise applications from perpetual licenses to subscription license, then before you place the Avaya OneCloud™ Subscription system order in the Avaya One Source ordering portal, ensure that the calculation of conversion credits from the existing perpetual licenses to subscription license is proper. This ensures correct Investment Protection Program (IPP) credit during migration of applications from perpetual licenses to subscription license. After your Avaya OneCloud™ Subscription system order is placed and processed in the Avaya One Source ordering portal, Avaya will send a notification email confirming your order fulfillment to your registered technical contact. After you receive the notification email, you must create a service request with Avaya to obtain your Access Key and Secret key. For more information, see Obtaining the Access key and Secret key on page 28. These keys are required to configure connectivity between the Usage Metering Collector and Avaya back-office systems. For more information, see Configuring connectivity between Usage Metering and Avaya back-office systems on page 52.
2	Install the Usage Metering Collector	For more information, see Checklist for installing Usage Metering Collector on page 38.
3	Configure the Usage Metering Collector	For more information, see Usage Metering configuration checklist on page 48. After you configure the connectivity between Usage Metering Collector and Avaya back-office systems, the Avaya OneCloud™ Subscription system that you ordered appears under your order ID in the Usage Metering Collector. For more information, see Configuring connectivity between Usage Metering and Avaya back-office systems on page 52. You can use the Usage Metering Collector to manage your Avaya OneCloud™ Subscription system.

Table continues…

No.	Task	Action / Description
4	Configure your Avaya OneCloud™ Subscription system	Configuring an Avaya OneCloud™ Subscription system includes configuring the WebLM and the subscribed on-premise Avaya UC and CC applications in the Avaya OneCloud™ Subscription system. Do the following: • Add WebLM to the Avaya OneCloud™ Subscription system. Use the Usage Metering Collector to add the WebLM server to the Avaya OneCloud™ Subscription system. After the Usage Metering Collector successfully registers to the WebLM server, Usage Metering automatically retrieves the subscription license from the Avaya back-office systems and installs it on the WebLM server. For more information, see Adding a WebLM server to an Avaya OneCloud Subscription system on page 89. • Install or migrate the on-premise Avaya UC and CC application: - If you are performing a new installation, install the on-premise application. - If you have opted to migrate the existing on-premise applications from perpetual licenses to subscription license, see Migrating applications from perpetual licenses to subscription license on page 127. **Note:** The on-premise application must be of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version. For more information, see Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30. • Add the subscribed on-premise Avaya UC and CC applications to the Avaya OneCloud™ Subscription system. Use the Usage Metering Collector to add the on-premise applications, including the mandatory applications, that are entitled by the subscription license to the Avaya OneCloud™ Subscription system. **Note:** These on-premise applications can run by using the subscription license after you add these applications to the Avaya OneCloud™ Subscription system. Before you add the applications, ensure that you read the instructions mentioned in the checklist for adding

Table continues…

No.	Task	Action / Description
		applications and perform the prerequisites for adding the applications. For more information, see Checklist for adding applications to an Avaya OneCloud Subscription system on page 92. For information about adding an application, see Adding an application to the Avaya OneCloud Subscription system on page 111.
5	Register the applications to the Avaya Global Registration Tool (GRT)	This allows Avaya to manage your Avaya OneCloud™ Subscription system renewals and provide you remote maintenance and troubleshooting support. For more information, see Technical onboarding of applications to the Avaya Global Registration Tool on page 123.
6	Manage your Avaya OneCloud™ Subscription system state	This allows Avaya to monitor your Avaya OneCloud™ Subscription system state. For more information, see Managing the Avaya OneCloud Subscription system state on page 126.
7	Use the subscribed services	Use the services that you have subscribed.
8	Receive invoice	An invoice is sent to you based on your fixed quantity subscription billing cycle.

Obtaining the Access key and Secret key

About this task

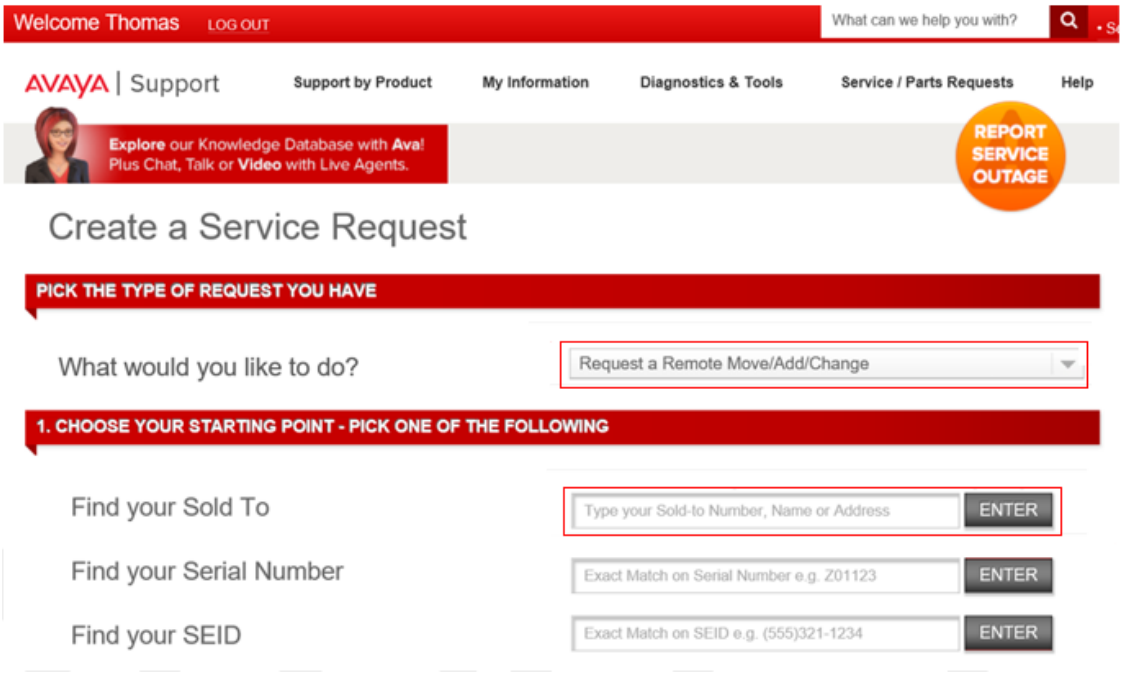
After your Avaya OneCloud™ Subscription system order is processed in the Avaya One Source ordering portal, Avaya sends a notification email confirming your order fulfillment to your registered technical contact. After you receive the notification email, you must create a service request with Avaya to obtain your Access key and Secret key.

These keys are required to configure connectivity between the Usage Metering Collector and Avaya back-office systems.

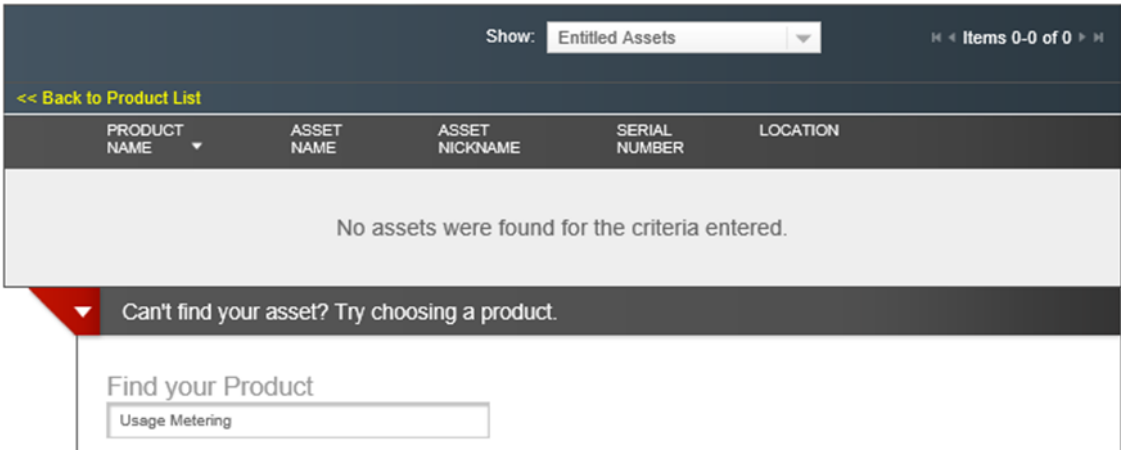
Procedure

1. Log on to https://support.avaya.com by using your Avaya credentials.
2. Under **Service/Parts Request**, click **Create Service Request**.
3. On the Create a Service Request page, do the following:
    a. In the **What would you like to do?** field, click **Request a Remote Move/Add/Change**.

b. In the **Find your Sold To** field, type the Sold To number where Usage Metering will be installed, and then click **ENTER**.



The system displays the list of products that are associated with the Sold To number, if any.



c. Click **Can’t find your asset? Try choosing a product**.

d. In the **Find your Product** field, type `Usage Metering`.

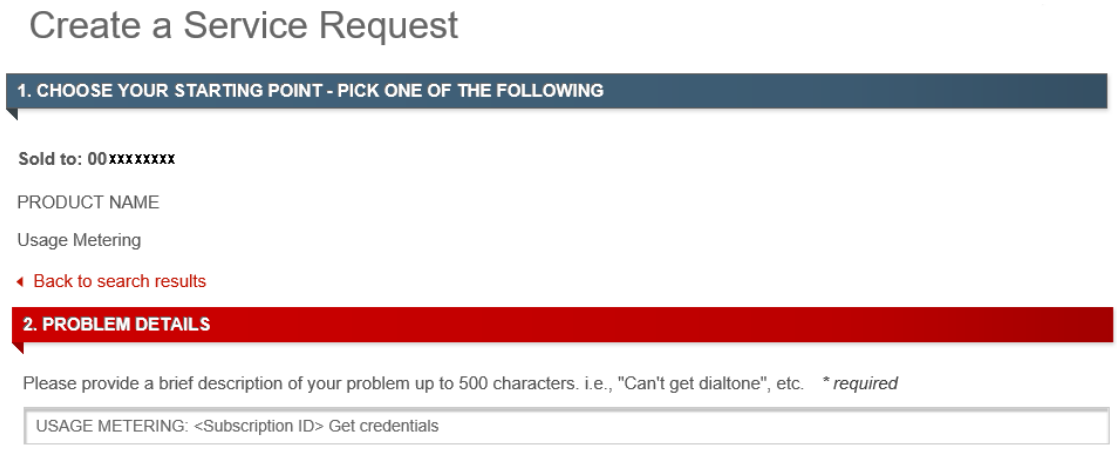
The system displays the Create a Service Request page.

4. Do the following:

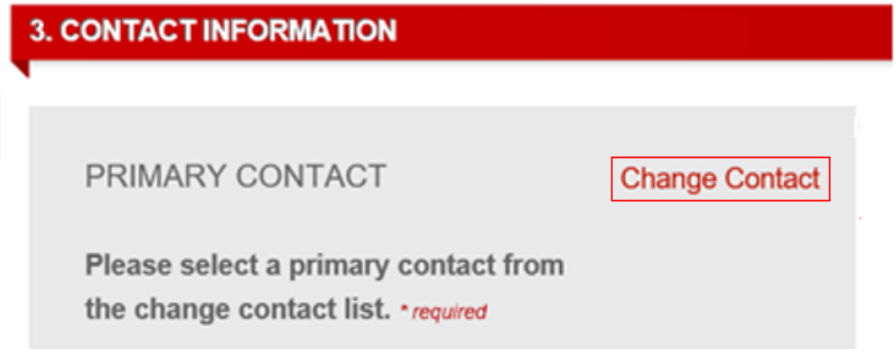
a. In the **PROBLEM DETAILS** area, provide the description in the following format:

`USAGE METERING: <Subscription ID>. Get Credentials`

```
Please provide <Subscription ID> with our credentials to
complete our Collector Configuration.
```



b. In the **Contact Information** area, specify the primary contact to whom Avaya must mail the Access key and Secret key.



5. Click **Submit**.

Result

Avaya processes your service request and sends an email containing the Access key and Secret key to your primary contact.

Related links

Configuring connectivity between Usage Metering and Avaya back-office systems on page 52

Avaya UC and CC applications supported by Avaya OneCloud™ Subscription

The following table provides the list of Avaya UC and CC applications, with their minimum version number, supported by Avaya OneCloud™ Subscription:

Avaya applications supported by Avaya OneCloud™ Subscription	Minimum version number supported by Avaya OneCloud™ Subscription
UC applications	
Avaya Aura® Communication Manager	8.0.1 Recommended 8.1.x
Avaya Aura® System Manager	8.1.2 (8.1.0 Feature Pack 2) + Hot Fix 3 or later For more information about the Hot Fix, see the Product Support Notice PSN005284u for System Manager Release 8.1.2 available at: https://support.avaya.com
Standalone Avaya WebLM	8.1.2
Avaya Aura® Session Manager	8.1.x
Avaya Aura® Presence Services	8.1.x
Avaya Aura® Messaging	7.1
Avaya IX™ Messaging (formerly known as Avaya Officelinx)	10.8
Avaya Workplace Integration with Skype for Business (formerly known as Avaya Communicator for Microsoft Lync)	6.4
Avaya Aura® Application Enablement Services (for Unified Desktop)	8.1.2.1 Super Patch 1 For more information, see the Product Support Notice PSN020489u-Avaya Aura® Application Enablement Services 8.1.2.1 Super Patches available at: https://support.avaya.com
Avaya Workplace (Mobility for IOS / Android)	3.6
Avaya Workplace (for Mac / Windows)	3.6
Avaya IX™ Workplace VDI (formerly known as Avaya Equinox® VDI)	3.0
Avaya Equinox® for Web	1.1
Avaya IX™ Workplace Attendant (formerly known as Avaya Equinox® Attendant)	5.2
Avaya one-X® Communicator	6.2.10
Avaya one-X® Client Enablement Services	6.2
Avaya Spaces	2.0
Avaya Equinox® Conferencing	9.1.x

Table continues…

Avaya applications supported by Avaya OneCloud™ Subscription	Minimum version number supported by Avaya OneCloud™ Subscription
Avaya Breeze® platform	3.6
Avaya Aura® Session Border Controller	8.0.1
Avaya Aura® Media Server	8.0
Call Park and Page Snap-in	1.0
Avaya Device Adapter Snap-in	8.0.1 for Communication Manager 8.0.1 8.1 for Communication Manager 8.1
Avaya Aura® Web Gateway	3.6
Avaya Aura® Device Services	8.0
CC applications	
Avaya Aura® Call Center Elite	8.0.1 (Recommended 8.1.x)
Avaya Call Management System	19
Avaya Agent for Desktop	1.6
Avaya one-X® Agent	2.5.12
Avaya Workspaces for Elite	3.7
Avaya Aura® Experience Portal (IVR excluding Speech) Currently, Avaya Aura® Experience Portal that uses local Postgres database, external Postgres database, or external Microsoft SQL database is supported.	7.2.3
Avaya Aura® Orchestration Designer	7.2.3
Avaya Dynamic Self Service	2.9.3
Customer Journey	3.7
CC Add-Ons	
Avaya Callback Assist	4.7.1
Avaya Aura® Application Enablement Services — DMCC Full / TSAPI Basic	8.1.2.1 Super Patch 1 For more information, see the Product Support Notice PSN020489u-Avaya Aura® Application Enablement Services 8.1.2.1 Super Patches available at: https://support.avaya.com
Avaya Diagnostic Server applications	
SAL Gateway	3.2
SLA Mon™	3.2

Related links

Adding an application to the Avaya OneCloud Subscription system on page 111

Order type and associated available features

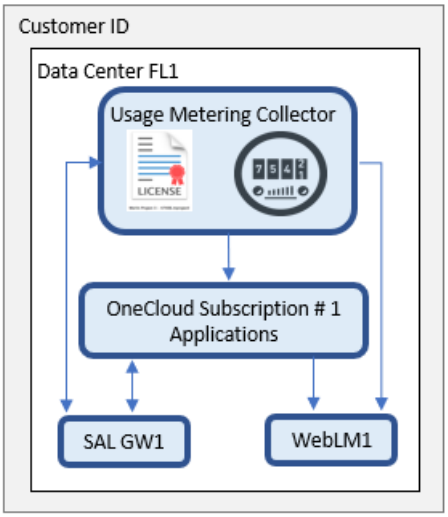
The UC and CC features that are available in an Avaya OneCloud™ Subscription system depend on the service bundle that you order, that is, Basic, Core, or Power.

For more information, refer to your Avaya OneCloud™ Subscription Offer Definition document.

Avaya OneCloud™ Subscription system deployment models

The following are the Avaya OneCloud™ Subscription system deployment models:

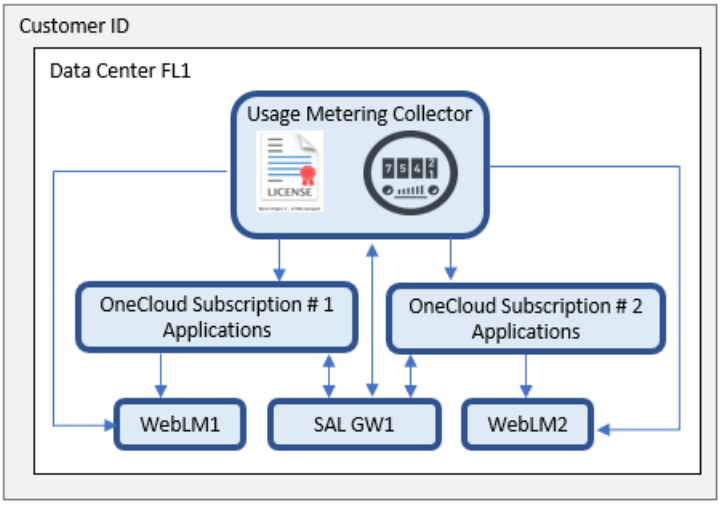
Single data center with one Avaya OneCloud™ Subscription system



In this deployment model:

- You can install a Usage Metering Collector in a data center and configure a single Avaya OneCloud™ Subscription system in the Usage Metering Collector. You can deploy the applications that are subscribed under this Avaya OneCloud™ Subscription system in the same data center.

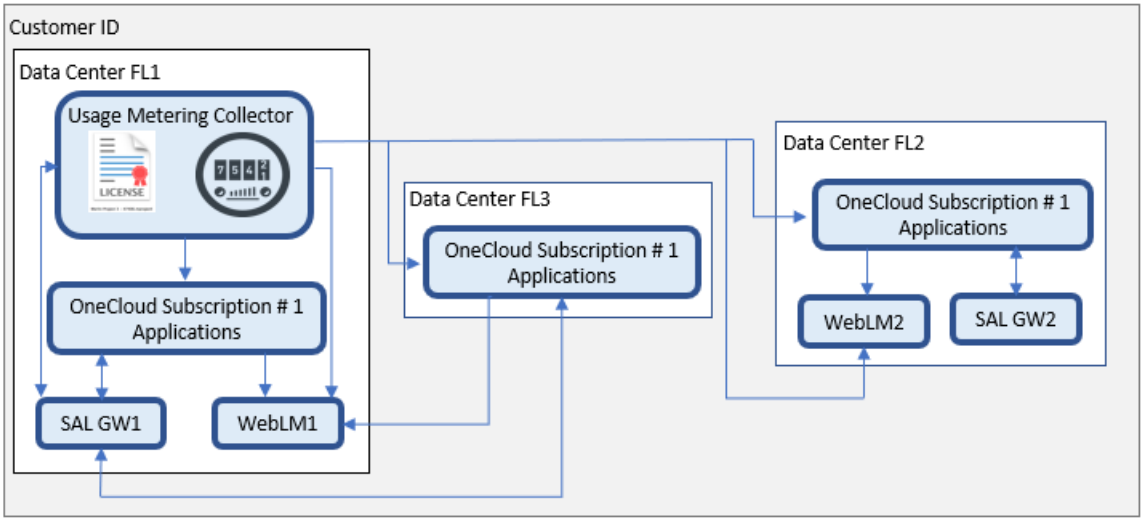
Single data center with multiple Avaya OneCloud™ Subscription systems



In this deployment model:

- You can install a Usage Metering Collector in a data center and configure multiple Avaya OneCloud™ Subscription systems in the Usage Metering Collector. You can deploy the applications that are subscribed under these Avaya OneCloud™ Subscription systems in the same data center.
- You must deploy a separate WebLM server and Communication Manager system — simplex or duplex — for each Avaya OneCloud™ Subscription system.
- You can share the same SAL GW among the Avaya OneCloud™ Subscription systems.

Single Avaya OneCloud™ Subscription system with multiple data centers



In this deployment model:

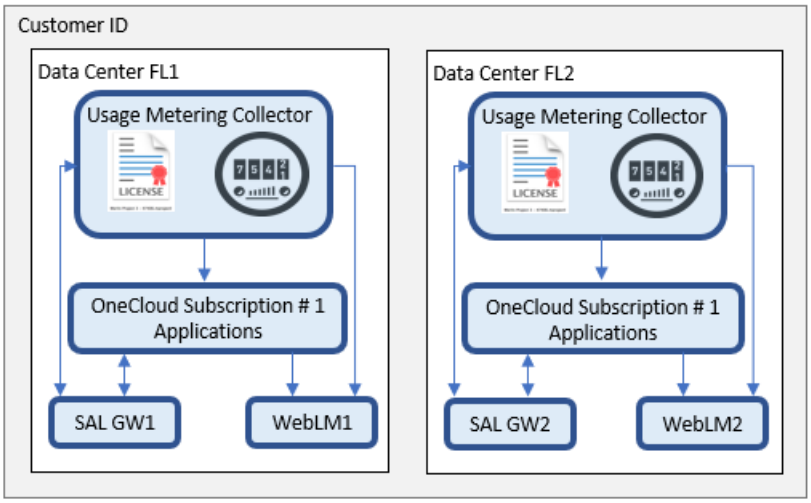
- You can install a Usage Metering Collector in one data center and configure an Avaya OneCloud™ Subscription system in the Usage Metering Collector. You can deploy the

applications that are subscribed under this Avaya OneCloud™ Subscription system in multiple data centers.

- You must deploy a separate WebLM server and SAL GW for each data center.

  However, some applications do not require license management. For example, licensing for the Communication Manager Survivable Core server is managed by the Communication Manager main server. Hence, if a data center has only those applications that do not require license management, you need not deploy a WebLM server in that data center.

Geo-Redundant data centers with single Avaya OneCloud™ Subscription system



In this deployment model:

- You cannot deploy a geo-redundant Usage Metering Collector because concurrently deploying two Usage Metering Collectors that contain the same Avaya OneCloud™ Subscription system causes duplicate usage calculation.

  In a geo-redundant environment, if the Usage Metering server fails in the primary data center or if a network outage is detected, you must perform a new installation of the Usage Metering server in the secondary data center. You must then restore the backup of the primary Usage Metering server on the secondary Usage Metering server by using the Usage Metering backup file.

  Note that the deployment of the applications that are subscribed under an Avaya OneCloud™ Subscription system in both primary and secondary data centers depends on the High Availability and geo-redundancy models that are supported for these applications.

- You must deploy a separate WebLM server and SAL GW for each data center.

  For more information, see Usage Metering in a geo-redundant environment on page 135.

Caveats

Consider the following caveats before choosing a deployment model for your data center:

- Currently, each Usage Metering Collector supports only one time zone.

  For more information, see Setting the time zone on page 44.

  Hence, ensure that you deploy each on-premise application, both primary and secondary applications, that is part of an Avaya OneCloud™ Subscription system by using the time zone

that is set for the Usage Metering Collector in which this Avaya OneCloud™ Subscription system is configured.

For more information, see Adding an application to the Avaya OneCloud Subscription system on page 111.

- Do not configure the same Avaya OneCloud™ Subscription system in multiple Usage Metering Collectors because it causes duplicate usage calculation.

  For more information, see Considerations for configuring Avaya OneCloud Subscription systems of the same subscription offer in multiple Usage Metering Collectors on page 36.

Considerations for configuring Avaya OneCloud™ Subscription systems of the same subscription offer in multiple Usage Metering Collectors

If you operate in multiple data centers that do not have connectivity between them, then consider the following to configure the Avaya OneCloud™ Subscription systems that are part of your subscription offer in these data centers and monitor the service usage:

- You must install and configure a new Usage Metering Collector in these data centers.

  Note:

  Ensure that you perform a new installation of the Usage Metering Collector in the data centers. Do not select the **Restore from backup** option when performing the installation.

  For more information, see Installing Usage Metering Collector on page 45.

- Use the same Access key and Secret key to configure connectivity for each of these Usage Metering Collectors.

  Usage Metering retrieves your Avaya OneCloud™ Subscription offer from the Avaya back-office system and populates it in the Usage Metering Collectors. You can identify the subscription offer by its offer ID. This offer ID contains the entire list of your subscribed Avaya OneCloud™ Subscription systems. You can identify the Avaya OneCloud™ Subscription systems by their subscription IDs.

  For more information, see Configuring connectivity between Usage Metering and Avaya back-office systems on page 52.

- On each Usage Metering Collector, configure the Avaya OneCloud™ Subscription systems that you want for the data center.

  For more information, see Avaya OneCloud™ Subscription system management.

  For more information about the deployment models, see Avaya OneCloud Subscription system deployment models on page 33.

Important:

Do not configure the same Avaya OneCloud™ Subscription system in more than one Usage Metering Collector. You can identify an Avaya OneCloud™ Subscription system by its subscription ID.

Configuring the same Avaya OneCloud™ Subscription system in more than one Usage Metering Collector causes duplicate usage calculation because multiple Usage Metering Collectors then perform usage data collection of the applications that are configured in the Avaya OneCloud™ Subscription system.

Avaya OneCloud™ Subscription service usage reports

Avaya Channel Partners can download the Avaya OneCloud™ Subscription service usage reports from the Avaya Channel Store.

Chapter 3: Usage Metering Collector installation

Checklist for installing Usage Metering Collector

Pre-installation checklist

No.	Task/Prerequisite	Related topic	Notes	✔
1	Prerequisite knowledge and application for installing and using Usage Metering Collector.	Prerequisite knowledge and application for installing and using Usage Metering Collector on page 39		
2	Ensure that the system requirements for installing Usage Metering Collector are met.	System requirements to deploy Usage Metering on page 40		
3	Ensure that your corporate firewall allows access to the URLs required for Usage Metering Collector.	Required URLs for Usage Metering Collector on page 42		
4	Perform disk partition encryption to comply with Data Privacy regulations.	Disk partition encryption for Data Privacy on page 42		
5	If your IT infrastructure uses a non-transparent proxy, configure the proxy details in the `bash_profile` file.	Configuring the non-transparent proxy details in the bash_profile file on page 43		
6	Set the time zone on the server where you want to install Usage Metering Collector.	Setting the time zone on page 44		

Installation checklist

No.	Task	Related topic	Notes	✔
1	Install Usage Metering Collector.	Installing Usage Metering Collector on page 45		

Post-installation checklist

No.	Task	Related topic	Notes	✔
1	If your IT infrastructure uses a non-transparent proxy, configure the non-transparent proxy in the Usage Metering Collector.	Configuring non-transparent proxy in the Usage Metering Collector on page 46		

Planning and pre-installation configuration

Prerequisite knowledge and application for installing and using Usage Metering Collector

Prerequisite knowledge

- Knowledge of Linux commands.
- If you want to install Usage Metering Collector on CentOS, knowledge of how to install CentOS by using the **Minimal Install** installation type option.
- If you want to install Usage Metering Collector on Red Hat Enterprise Linux (RHEL), knowledge of how to install RHEL by using the **Minimal Install** installation type option.

Prerequisite application

- An application to open an SSH session to the CentOS or RHEL server.

  For example, PuTTY.

After you install the Usage Metering Collector and configure connectivity between Usage Metering and Avaya back-office systems, your Avaya OneCloud™ Subscription system order that was placed in the Avaya One Source ordering portal appears under your offer ID in the Usage Metering Collector.

For more information, see Avaya OneCloud Subscription system on page 82.

System requirements to deploy Usage Metering

Requirement	Description
Operating system	Any of the following: • CentOS 7 64 bit x86 with update 3 or any later version of CentOS 7. • Red Hat Enterprise Linux (RHEL) 7 64 bit x86 with update 3 or any later version through RHEL 8.x. Points to consider: • CentOS 8.x is not supported. • Do not use a CentOS or RHEL Minimal ISO file to install CentOS or RHEL. • Do not use a CentOS or RHEL LiveCD ISO to install CentOS or RHEL. • Install CentOS or RHEL by using the **Minimal Install** installation type option. The **Minimal Install** installation type option is available on the Software Selection page of the CentOS or RHEL installation wizard. • Do not install any other software packages on the operating system. However, an exception is the following third-party antivirus software, which you can install on the operating system: CylancePROTECT version 2.1.1564 • Do not install Tomcat on the operating system. • Installation of Usage Metering Collector on RHEL requires a Red Hat subscription. Without a subscription, the installation can fail. If the installation fails, the following message is displayed notifying you to buy a Red Hat subscription. `This system was not registered with an entitlement server. You can use subscription manager to register.` • The Yum installation installs the dependent RPMs. • Usage Metering installs all the required packages.

Table continues…

Requirement	Description
	Usage Metering supports virtualized and bare metal environments.
Hardware specifications	For Usage Metering Collector containing up to 20 Avaya OneCloud™ Subscription systems: • 8 GB of RAM • 2 CPU cores such as 2.6GHz Intel Xeon E5 (Sandy Bridge), 2.5 GHz Intel Xeon E5 v2 (Ivy Bridge), or 2.3 GHz Intel Xeon E5 v3 (Haswell) • 100–GB hard disk For Usage Metering Collector containing more than 20 Avaya OneCloud™ Subscription systems: • 16 GB of RAM • 4 CPU cores such as 2.6GHz Intel Xeon E5 (Sandy Bridge), 2.5 GHz Intel Xeon E5 v2 (Ivy Bridge), or 2.3 GHz Intel Xeon E5 v3 (Haswell) • 100–GB hard disk
Network specifications	Access to the Avaya OneCloud™ Subscription components and applications. Usage Metering must have connectivity to the following: • SAL Gateway (SAL GW) • SNMP Trap Host. SAL Gateway must have connectivity to Usage Metering.
Internet access	The SAL Gateway must have access to the public internet. Additionally: • Installation of the Usage Metering Collector on CentOS requires unrestricted HTTP and HTTPS access to the public internet, including a Domain Name System (DNS) • Installation of the Usage Metering Collector on RHEL requires the following: - Access to the Red Hat Yum repository. For more information, see the Red Hat documentation. - Restricted HTTPS access to the public internet.

Table continues…

Requirement	Description
Time and Time zone	Time: • The system starts collecting and submitting usage data every day at 3:20 a.m. local time. • Configure NTP to ensure the time remains correct. Time zone: • Set the time zone according to your locale. • The time zone you set on the system determines the start and stop of each billing day. • CentOS and RHEL use the tz database of time zones.

You need an email (SMTP) account for Usage Metering to send an email. For example, SendGrid.

Required URLs for Usage Metering Collector

Usage Metering Collector uses the following URLs to communicate with the Avaya back-office systems.

Ensure that your corporate firewall allows access to the following URLs:

- https://apigateway.eu-central-1.amazonaws.com
- https://a4yz7gmcu2.execute-api.eu-central-1.amazonaws.com
- https://s3.eu-central-1.amazonaws.com
- https://processor-prod-venususagedatas3bucket-199ibo6k84brm.s3.eu-central-1.amazonaws.com
- https://iam.amazonaws.com
- https://yum.avaya.com
- https://rfde692u8f.execute-api.eu-central-1.amazonaws.com

Additionally, ensure the following if you are planning to install the Usage Metering Collector on RHEL:

- Your corporate firewall allows access to Red Hat Subscription Manager:

  https://cdn.redhat.com

  For more information, see https://access.redhat.com/solutions/65300.

Disk partition encryption for Data Privacy

The Usage Metering Collector installation creates the following directories:

- `/opt/Avaya/usage-metering/`

- `/var/lib/pgsql/`

Note:

To comply with Data Privacy regulations, Avaya recommends you to do the following before installing the Usage Metering Collector:

- Encrypt the disk partition that will contain the `/opt/Avaya/usage-metering/` and `/var/lib/pgsql/` directories.

Important:

Ensure that you remember the encryption passphrase. If you make a note of the encryption passphrase, ensure that you store it at a secure location.

If you forget the encryption passphrase, you cannot access the files and data located on the encrypted disk partition. If you forget the encryption passphrase, you must re-deploy the operating system, perform a new installation of the Usage Metering Collector, and restore the Usage Metering data by using the Usage Metering backup file.

Related links

Usage Metering backup and restore on page 131

Configuring the non-transparent proxy details in the bash_profile file

About this task

If your IT infrastructure uses a non-transparent proxy, then before you install the Usage Metering Collector, you must configure the non-transparent proxy details in the `bash_profile` file.

Depending on the protocol used, you can use the *http_proxy* or *https_proxy* environment variables of Linux to configure the non-transparent proxy details in the `bash_profile` file.

After you install the Usage Metering Collector, you must configure these proxy details in the Usage Metering Collector. This allows Usage Metering Collector to access the cloud services by using the proxy server.

If your proxy server requires authentication, configure the user name and password of the proxy server in the `bash_profile` file.

Procedure

1. On the CLI command prompt of the server on which you will install Usage Metering Collector, run the following command to edit the `bash_profile` file:

   `vi ~/.bash_profile`

2. To configure an HTTP proxy, do any of the following:
   - If the HTTP proxy server does not require authentication, run the following command:

     `export http_proxy=http://<proxy IP address>:<proxy port number>`
   - If the HTTP proxy server requires authentication, run the following command:

```
export http_proxy=http://<proxy user name>:<proxy
password>@<proxy IP address>:<proxy port number>
```

Where,

<*proxy IP address*> is the IP address of the HTTP proxy server.

<*proxy port number*> is the port number of the HTTP proxy server.

<*proxy user name*> is the user name to access the HTTP proxy server.

<*proxy password*> is the password to access the HTTP proxy server.

3. To configure an HTTPS proxy, do any of the following:
   - If the HTTPS proxy server does not require authentication, run the following command:

     ```
     export https_proxy=http://<proxy IP address>:<proxy port number>
     ```

   - If the HTTPS proxy server requires authentication, run the following command:

     ```
     export https_proxy=http://<proxy user name>:<proxy
     password>@<proxy IP address>:<proxy port number>
     ```

     Where,

     <proxy IP address> is the IP address of the HTTPS proxy server.

     <proxy port number> is the port number of the HTTPS proxy server.

     <proxy user name> is the user name to access the HTTPS proxy server.

     <proxy password> is the password to access the HTTPS proxy server.

4. Run the following command for the changes in the `bash_profile` file to take effect at run time, without restarting the system:

   ```
   source ~/.bash_profile
   ```

Next steps

- After you perform the pre-installation configuration, install the Usage Metering Collector.
- Configure these non-transparent proxy details in the Usage Metering Collector.

Related links

Configuring non-transparent proxy in the Usage Metering Collector on page 46

Setting the time zone

About this task

Currently:

- Usage Metering calculates the daily usage data based on the operating system time zone that you set for the Usage Metering Collector server.
- Each Usage Metering Collector supports only one time zone.

Use this procedure to set the operating system time zone for the Usage Metering Collector server.

You must set the time zone before installing Usage Metering. If you set or change the time zone after installing Usage Metering, you must restart the Usage Metering server.

Before you begin

- To view the current time zone settings, run the following command:

  `timedatectl`

- To view a list of time zones, run the following command:

  `timedatectl list-timezones`

Procedure

1. In an SSH client, run the following command:

   `timedatectl set-timezone` *<your time zone>*

   For example, to configure the time zone for New York, run the following command:

   `timedatectl set-timezone` *America/New_York*

2. (Optional) To restart the Usage Metering server, run the following command:

   `um-restart`

   The change in the time zone that you set takes effect.

Related links

Avaya OneCloud Subscription system deployment models on page 33

Installing Usage Metering Collector

About this task

Use this procedure to install Usage Metering Collector on CentOS 7.x, RHEL 7.x, or RHEL 8.x server.

If your IT infrastructure uses a proxy server, you have configured the proxy details in the `bash_profile` file, and you are using root credentials, then run the commands in this procedure without using **`sudo`**. If you run the commands by using **`sudo`**, Usage Metering Collector installation tries to connect to the cloud services without using the proxy server.

Procedure

1. Open an SSH session to the CentOS or RHEL server on which you want to install the Usage Metering Collector.
2. To add the Usage Metering Yum repository to your Yum configuration, do one of the following:

   - If you are installing Usage Metering Collector on CentOS 7.x or RHEL 7.x, run the following command in your SSH session:

     ```
     sudo curl -o /etc/yum.repos.d/avaya-um.repo \
     ```

```
https://yum.avaya.com/um-repo/avaya-um.repo
```

Ensure that there is a space before the backslash (\) and no space after the backslash (\) on the first line.

If you manually type this command, do not type a space after the "\" on the first line. You can type the entire command on one line.

- If you are installing Usage Metering Collector on RHEL 8.x, run the following command in your SSH session:

```
sudo curl -o /etc/yum.repos.d/avaya-um-rhel8.repo https://
yum.avaya.com/um-repo-rhel8/avaya-um-rhel8.repo
```

If the preceding commands fail, see Usage Metering Collector cannot recognize a web proxy CA certificate on page 144.

3. Run the following command to install Usage Metering Collector and all required dependencies:

```
sudo yum -y install avaya-usage-metering
```

The Usage Metering software installation can update the kernel or other core operating system libraries of your server.

4. Run the following command to declare a stage name for the Usage Metering deployment and replicate it in the Avaya back-office systems:

```
echo "stage=<stage name>" | sudo tee -a /opt/Avaya/usage-metering/
um.properties
```

5. Run the following command to restart Usage Metering:

```
um-restart
```

Related links

System requirements to deploy Usage Metering on page 40

Post-installation configuration

Configuring non-transparent proxy in the Usage Metering Collector

About this task

If your IT infrastructure uses a non-transparent proxy, then after you install the Usage Metering Collector, you must configure the non-transparent proxy in the Usage Metering Collector. Use the proxy server details that you configured in the `bash_profile` file.

This allows Usage Metering Collector to access the cloud services by using the proxy server.

If your proxy server requires authentication, configure the user name and password of the proxy server in the Usage Metering Collector.

Use the **um-set-proxy.sh** script to configure the non-transparent proxy details in the Usage Metering Collector.

Before you begin

The proxy details that you specify when running the **um-set-proxy.sh** script are stored in the `um.properties` file. Hence, back up the `um.properties` file before performing this procedure. In case the `um.properties` file becomes corrupted, you can replace the corrupted file with the backup file.

Procedure

1. At the Usage Metering Collector server CLI command prompt, run the following command:

   ./um-set-proxy.sh

2. Do the following to configure the proxy server IP address and port number in the Usage Metering Collector:

   a. At the **Please enter proxy IP address** prompt, type the proxy server IP address that is configured in the `bash_profile` file and press `Enter`.

   b. At the **Please enter proxy port number** prompt, type the proxy server port number that is configured in the `bash_profile` file and press `Enter`.

3. If the proxy server requires authentication, do the following to configure the user name and password of the proxy server:

   a. At the **Please enter proxy username (Press ENTER if none)** prompt, type the proxy server user name that is configured in the `bash_profile` file and press `Enter`.

   If the proxy server does not require authentication, press `Enter` without specifying the user name.

   b. At the **Please enter proxy password (Press ENTER if none)** prompt, type the proxy server password that is configured in the `bash_profile` file and press `Enter`.

   The password that you specify is stored in an encrypted format in the `um.properties` file.

   If the proxy server does not require authentication, press `Enter` without specifying the password.

4. Run the following command to restart the Usage Metering Collector server:

   um-restart

   The configured proxy details take effect after the Usage Metering Collector server is restarted.

Related links

Configuring the non-transparent proxy details in the bash_profile file on page 43

Chapter 4: Usage Metering Collector configuration

Usage Metering configuration checklist

Use this checklist to configure Usage Metering.

Mandatory configuration

No.	Task	Description	Notes	✔
1	Create the initial Usage Metering user	Before logging on to the Usage Metering Collector interface for the first time, ensure that you create an initial user. For more information, see Creating an initial user for Usage Metering Collector on page 51.		
2	Configure users	To configure Usage Metering users. For more information, see User management on page 58.		
3	Configure the SMTP server	To enable the Usage Metering Collector to send email notifications. For more information, see Configuring SMTP mail server to send email notifications on page 53.		

Table continues…

No.	Task	Description	Notes	✔
4	Configure connectivity between Usage Metering and Avaya back-office systems	To connect the Usage Metering Collector with the Avaya back-office systems. After the connectivity is established, Usage Metering retrieves your Avaya OneCloud™ Subscription offer from the Avaya back-office systems and displays it on the **Offers** tab of the Usage Metering Collector web interface. For more information, see Configuring connectivity between Usage Metering and Avaya back-office systems on page 52.		
5	Configure the SNMP server	To enable the Usage Metering Collector to send alerts. For more information, see Configuring alerts on page 54.		
6	Enable EASG login	To allow Avaya Services personnel to access your system remotely and provide remote maintenance and troubleshooting support. For more information, see Enabling EASG login for remote access on page 57.		

Optional configuration

No.	Task	Description	Notes	✔
1	Configure certificates	Install and manage certificates for Usage Metering. For more information, see Certificate management.		
2	Configure a name for the Usage Metering Collector	To specify a name for the Usage Metering Collector that helps you easily identify the Usage Metering Collector. For more information, see Configuring a name for the Usage Metering Collector on page 53.		

Table continues…

No.	Task	Description	Notes	✔
3	Configure the syslog server	To enable the Usage Metering Collector to send logs. For more information, see Configuring alerts on page 54.		
4	Configure session time out and failed login attempt threshold	To configure session time out and number of permissible failed login attempts for a user. For more information, see Configuring session timeout and failed login attempt threshold on page 56.		
5	Configure security banner for the login page	To configure the text that appears on the login page of the Usage Metering Collector. For more information, see Configuring security banner for the login page on page 58.		
6	Configure custom password policy	To configure a custom password policy for the Usage Metering Collector user accounts. For more information, see Configuring custom password policy for Usage Metering Collector user accounts on page 62. For information about the default password policy, see Default password policy for Usage Metering Collector user accounts on page 61.		
7	Configure password reset policy	To configure a password reset policy for the Usage Metering Collector user accounts. For more information, see Configuring a password reset policy for the Usage Metering Collector user accounts on page 64.		
8	Configure account lockout policy	To configure an account lockout policy for the Usage Metering Collector user accounts. For more information, see Configuring an account lockout policy for Usage Metering Collector user accounts on page 66.		

Table continues…

No.	Task	Description	Notes	✔
9	Configure number of concurrent login sessions allowed	To set the limit for the number of concurrent login sessions to the Usage Metering Collector web interface. For more information, see Setting the limit for concurrent login sessions for the Usage Metering Collector web interface on page 70.		
10	Enable keep-alive trap messages	To enable the keep-alive trap messages from the Usage Metering Collector. For more information, see Enabling SNMP keep-alive trap messages from Usage Metering Collector on page 71.		
11	Configure hostname validation	To enable or disable hostname validation for SSL connections. By default, hostname validation is enabled. For more information, see Enabling or disabling hostname validation on page 72.		
12	Install and configure Advanced Intrusion Detection Environment (AIDE) utility for Usage Metering	To protect the Usage Metering files from unauthorized changes. For more information, see Installing and configuring Advanced Intrusion Detection Environment utility on page 73.		

To verify that the Usage Metering Collector is properly configured and running, on the **OVERVIEW** tab of the Usage Metering Collector Home page, verify that the **Status** field displays **Running**.

Creating an initial user for Usage Metering Collector

About this task

Use this procedure to create a user profile to log on to the Usage Metering Collector interface for the first time.

Procedure

1. In a web browser, type the IP address or the fully qualified domain name (FQDN) of the CentOS or RHEL server on which Usage Metering Collector is installed.

2. Select the **I accept the terms and conditions in the license agreement** check box and click **ACCEPT**.
3. On the **Initial User Creation** page, type the relevant information in the following fields:
   - **Email**
   - **Password**
   - **Confirm Password**
   - **First name**
   - **Last name**
4. Click **CREATE**.
5. In the **Initial User Created** dialog box, click **OK**.
6. In the **Email** and **Password** fields, type your credentials and click **LOGIN**.

Configuration settings

Configuring connectivity between Usage Metering and Avaya back-office systems

About this task

Use the Access key and Secret key that you have received from Avaya to configure connectivity between Usage Metering and Avaya back-office systems.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click  , and then click **CONFIGURATION**.
3. In the left navigation pane, click **AWS**.
4. In the **AWS Access Key** field, type the Access key.
5. In the **AWS Secret Key** field, type the Secret key.

Result

- The Avaya back-office system does the following:
  - Auto-generates a unique ID for the customer and displays it in the **Usage Metering ID** field. You cannot modify the Usage Metering ID.
  - Auto-generates a name for the Usage Metering Collector and displays it in the **Collector Name** field. You can modify the name of the Usage Metering Collector.
  - Auto-generates a unique Collector ID for the Usage Metering Collector and displays it in the **Collector ID** field. You cannot modify the Collector ID.

- Usage Metering uses the Access key and Secret key to connect to the Avaya back-office systems, and link the Usage Metering Collector ID and name to the Usage Metering ID.
- Usage Metering retrieves your Avaya OneCloud™ Subscription offer and displays it on the **Offers** tab.

Next steps

Note down the Usage Metering Collector ID displayed in the **Collector ID** field.

Identifying a Usage Metering Collector by its Collector ID is useful when you want to restore the Usage Metering Collector, especially when you have multiple Usage Metering Collectors installed. This is because you need to specify the Collector ID of the Usage Metering Collector when performing the restore procedure.

Related links

Obtaining the Access key and Secret key on page 28
Avaya OneCloud Subscription system on page 82
Configuring a name for the Usage Metering Collector on page 53

Configuring a name for the Usage Metering Collector

About this task

Avaya recommends you to configure a unique name for the Usage Metering Collector so that the Usage Metering Collector is easily identifiable.

Before you begin

Ensure that you configure connectivity between Usage Metering and Avaya back-office systems.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click , and then click **CONFIGURATION**.
3. In the left navigation pane, click **AWS**.
4. In the **Collector Name** field, type a unique name for the Usage Metering Collector and click anywhere on the page outside of the **Collector Name** field.

Result

The system saves the configured name of the Usage Metering Collector.

Related links

Configuring connectivity between Usage Metering and Avaya back-office systems on page 52

Configuring SMTP mail server to send email notifications

About this task

You can configure the SMTP mail server details and email addresses of users to whom Usage Metering must send SMTP (email) notifications.

To send email notifications, use an SMTP account such as SendGrid.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click  , and then click **CONFIGURATION**.
3. In the left navigation pane, click **GENERAL**.
4. In the **SMTP (Mail) Server** field, type the name of the SMTP server.

   For example, if you use SendGrid, type `smtp.sendgrid.net`.
5. In the **Port** field, type the port number of the SMTP server.
6. In the **SMTP (Mail) User ID** field, type the user ID of your SMTP account.
7. In the **Password** field, type the password of your SMTP account.
8. In the **From Email Address** field, type the email address provided by your organization for the sender.

   This email address is shown in the `From` field when the users receive an automatic email notification from Usage Metering.
9. In the **Operator Emails (separate with commas)** field, type the email addresses of the users to whom Usage Metering must send email notifications and alerts.

   Use a comma as a separator to specify multiple email addresses.

   The **Collector URI (typically the FQDN of the server)** field shows the URI of the Usage Metering Collector. You can retain this field to the default value.
10. Enable the **Require TLS for sending emails** option to use the TLS protocol when sending email notifications.
11. Enable the **Validate SMTP server SSL certificate** option to validate the SMTP server SSL certificate.

Alerts

You can configure alerts so that Usage Metering can send the alert notifications to Avaya and to the email addresses that you specify. Usage Metering sends alert notifications when any significant event occurs in the system, for example, when you change an Avaya OneCloud™ Subscription system state from **Testing** to **Go Live**.

Configuring alerts allows Avaya to monitor the system, which is useful when providing remote maintenance and troubleshooting support.

Configuring alerts

About this task

Usage Metering sends alerts by using both Simple Network Management Protocol (SNMP) and email.

Usage Metering supports SNMP versions v2 and v3.

Before you begin

If you want to use Syslog to store the event and log messages, set up your syslog server.

For SNMP traps, set up your SNMP trap receiver.

You must configure the SAL Gateway as one of the SNMP trap receivers so that Avaya also receives the SNMP traps.

You can also configure an additional SNMP trap receiver where you want to receive the SNMP traps from the Usage Metering Collector.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click  , and then click **CONFIGURATION**.
3. In the left navigation pane, click **ALERTS**.
4. In the **Avaya Diagnostics Server (SAL Gateway)** field, type the IP address or FQDN of the SAL Gateway where Usage Metering Collector must send the SNMP traps.
5. If you are using an additional SNMP trap receiver, in the **SNMP Trap Send Address** field, type the IP address of the SNMP trap receiver.
6. In the **SNMP trap Version** field, select the SNMP version. That is, v2 or v3.
7. Do the following if you have selected SNMP v2:

   In the **SNMP Trap Community** field, type the appropriate community name for the SNMP trap.

   The default community name is **public**.
8. Do the following if you have selected SNMP v3:
   a. In the **SNMP trap Security Name** field, type the security name that Usage Metering Collector must use when generating the SNMP traps.

      The security name you specify in this field must match the security name that is configured in the SAL Gateway and the other SNMP trap receiver you are using.
   b. In the **SNMP Trap Security Level** field, do one of the following:

      - Click **noAuthNoPriv** if Usage Metering must not use authentication and encryption when communicating with the SNMP trap receivers.
      - Click **authNoPriv** if Usage Metering must use authentication, but no encryption when communicating with the SNMP trap receivers.
      - Click **authPriv** if Usage Metering must use both authentication and encryption when communicating with the SNMP trap receivers.

      The security level you select in this field must match the security level configured in the SAL Gateway and the other SNMP trap receiver you are using.
   c. Do the following if you have selected the **authNoPriv** or **authPriv** security level:
      a. In the **SNMP Trap Auth Protocol** field, click the authentication protocol that Usage Metering must use to authenticate with the SNMP trap receivers.

b. In the **SNMP Trap Auth Passphrase** field, type the password that Usage Metering must use to authenticate with the SNMP trap receivers.

   The password must be at least 8 characters in length.

The SNMP v3 authentication protocol and password you specify in these fields must match the SNMP v3 authentication protocol and password configured in the SAL Gateway and the other SNMP trap receiver you are using.

d. Do the following if you have selected the **authPriv** security level:

   a. In the **SNMP Trap Priv Protocol** field, click the privacy protocol that Usage Metering must use for encryption when communicating with the SNMP trap receivers.

   b. In the **SNMP Trap Priv Passphrase** field, type the privacy password that Usage Metering must use for encryption when communicating with the SNMP trap receivers.

      The password must be at least 8 characters in length.

   The SNMP v3 privacy protocol and password you specify in these fields must match the SNMP v3 privacy protocol and password configured in the SAL Gateway and the other SNMP trap receiver you are using.

9. In the **Syslog Server** field, type the IP address of your syslog server.
10. In the **Syslog Port** field, type the port number of your syslog server.
11. Enable the **Send emails (operator email list) on alerts** option to send the alerts by email to the email addresses you have configured when configuring the SMTP mail server.
12. Click **TEST ALERT** to generate and send a test alert from the Usage Metering Collector to the configured email addresses, syslog server, and SNMP trap receivers.

Related links

Usage Metering SNMP MIB file location on page 141
Configuring SMTP mail server to send email notifications on page 53

Configuring session timeout and failed login attempt threshold

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click  , and then click **CONFIGURATION**.
3. In the left navigation pane, click **GENERAL**.
4. In the **Idle session timeout (minutes)** field, type the duration (in minutes) for which a user can remain inactive in Usage Metering.

   After the number of minutes of inactivity is reached, Usage Metering automatically logs out the user.

5. In the **Account lockout threshold (failed login attempts)** field, type the maximum number of consecutive failed login attempts due to invalid credentials to be permitted to a user.

   After the maximum number of failed login attempts is reached, Usage Metering locks the user account.

   Set the value to 0 if you do not want to lock the user accounts because of consecutive failed login attempts.

   To set the number of minutes after which a locked user account must be automatically unlocked, use the **unlock.timeout.minutes** account lockout policy parameter.

6. In the **Delay after 3 failed login attempts (seconds)** field, type the number of seconds for which the last login attempt, of the total login attempts configured in the failed.logins.to.delay account lockout policy parameter, must be processed.

   Use the **Delay after 3 failed login attempts (seconds)** option along with the failed.logins.to.delay parameter to delay the last login attempt of a user if the previous login attempts fail consecutively because of invalid credentials.

   If a user provides valid credentials during the last login attempt, the delay is not applied to the login attempt.

Related links

Enabling or disabling a user account on page 59

Enabling EASG login for remote access

About this task

Avaya uses Enhanced Access Security Gateway (EASG) to:

- Remotely and securely access customer systems.
- Provide remote maintenance and troubleshooting support.

Turning on EASG login allows Avaya Services personnel to access your system remotely.

Note:

Avaya Services personnel can access Usage Metering by using the command line interface only.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click , and then click **CONFIGURATION**.
3. In the left navigation pane, click **GENERAL**.
4. Enable the **Allow Avaya Services Login (EASG)** option.

Configuring security banner for the login page

About this task

The text that you configure in the security banner appears on the login page of Usage Metering Collector.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click  , and then click **CONFIGURATION**.
3. In the left navigation pane, click **SECURITY BANNER**.
4. Enable the **Display the Security Banner** option.
5. In the **Security Banner Text** area, type the text for the Usage Metering Collector login page.

User management

Note:

Any user that you create in the Usage Metering Collector has administrative privileges by default.

You can:

- Add a new user.
- Edit the email address, first name, and last name of a user.
- Force a user to change the password on first login.
- Enable or disable a user.
- Delete a user.
- View the login history of a user.
- Reset or change the Usage Metering Collector password.

Creating a user

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click **USERS**.
3. Click **Create User** .

4. In the Create User dialog box, do the following:
    a. In the **email address** field, type the email address of the user.
    b. In the **password** field, type a password that the user can use to access the Usage Metering Collector.
    c. In the **retype password** field, retype the password.
    d. In the **first name** field, type the first name of the user.
    e. In the **last name** field, type the last name of the user.
    f. Click **CREATE**.

Forcing a user to change the password on the first login

About this task

Use this procedure to force a user to change the Usage Metering Collector password on the first login.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click , and then click **CONFIGURATION**.
3. In the left navigation pane, click **GENERAL**.
4. Enable the **Force password change on first login** option to force a user to change the Usage Metering Collector password on the first login.

Editing a user

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click **USERS**.
3. Click **Edit User** corresponding to the user that you want to edit.
4. In the Edit User dialog box, do the required changes, and then click **EDIT**.

Enabling or disabling a user account

About this task

Use this procedure to allow or prevent a user from accessing the Usage Metering Collector.

After you enable a user account that was disabled or locked due to failed login attempts, the user can use the last password to access the Usage Metering Collector.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click **USERS**.

3. Click **Edit User Security** corresponding to the user account that you want to enable or disable.
4. In the Edit User Security <email ID of the user> dialog box, do one of the following:
   - To enable the user account, enable the **User Enabled** option.
   - To disable the user account, disable the **User Enabled** option.
5. Click **OK**.

Related links

Configuring session timeout and failed login attempt threshold on page 56

Resetting the Usage Metering Collector password

About this task

Use this procedure to reset your Usage Metering Collector password if you forget the password.

Procedure

1. If an SMTP mail server and mail ID is configured in the Usage Metering Collector, do the following:
   a. Click **Forgot your password?** on the Usage Metering Collector login page.
   b. On the Reset Password page, in the **Email Address** field, type the email ID of your Usage Metering Collector user account for which you want to reset the password.
   c. Click **Continue**.

      Usage Metering sends an email message containing a password reset URL to the email ID you specified. Use the URL to reset your password.
2. If an SMTP mail server is not configured in the Usage Metering Collector, create a service request with Avaya for a password reset at: https://support.avaya.com.

Related links

Configuring a password reset policy for the Usage Metering Collector user accounts on page 64
Configuring SMTP mail server to send email notifications on page 53

Viewing the login history of a user

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click **USERS**.

   Usage Metering Collector displays the list of users.
3. Click the user name.

Result

Usage Metering Collector displays the login history of the user.

Deleting a user

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click **USERS**.
3. Click **Delete User** corresponding to the user that you want to delete.
4. In the Delete User dialog box, click **DELETE**.

Changing the Usage Metering Collector password

About this task

Use this procedure to change your Usage Metering Collector password.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click , and then click **CHANGE PASSWORD**.
3. On the Change Password page, in the **Current Password** field, type your current password.
4. In the **New Password** field, type a new password.
5. In the **Confirm New Password** field, retype the new password.
6. Click **SAVE**.

Usage Metering Collector password policy

Default password policy for Usage Metering Collector user accounts

This topic contains information about the default password policy and password character requirements for Usage Metering Collector user accounts.

Default character requirements for password

By default, the Usage Metering Collector password:

- Must be a minimum of 14 characters in length.
- Can be a maximum of 20 characters in length.
- Can contain a maximum of two consecutive repeated characters, that is, letters, numbers, or special characters. For example, AA.
- Can contain a maximum of four consecutive characters of the same character class. For example, four consecutive uppercase letters, such as ABEF.

- Must not contain spaces.
- Must not contain the login name of the user account.

Default password policy

- The password is valid for 90 days.
- The password must not be the same as the previous 10 passwords.
- The number of times a user can change the password per day is one.

For information about configuring a custom password policy, see Configuring custom password policy for Usage Metering Collector user accounts on page 62.

Configuring custom password policy for Usage Metering Collector user accounts

About this task

Use this procedure to configure a custom password policy for the Usage Metering Collector user accounts.

The new password policy takes effect for a user account when the user logs on to the Usage Metering Collector for the first time after the password policy is changed.

Before you begin

Back up the `um.properties` file before performing this procedure. In case the `um.properties` file becomes corrupted, you can replace the corrupted file with the backup file.

Procedure

1. At the Usage Metering Collector server CLI command prompt, run the following command to edit the `um.properties` file:

   `vi /opt/Avaya/usage-metering/um.properties`

2. Add the password policy parameter that you want in the following format to the `um.properties` file:

   <password policy parameter name>=<value>

   To configure multiple password policy parameters, add each parameter on a separate line.

   For information about the configurable password policy parameters and their associated values, see Usage Metering Collector password policy parameters on page 63.

Example

To set the minimum length of the password to 8 characters, add the password.min.length parameter in the following format to the `um.properties` file:

```
password.min.length=8
```

Related links

Default password policy for Usage Metering Collector user accounts on page 61

Usage Metering Collector password policy parameters

To configure a custom password policy for the Usage Metering Collector user accounts, you can add the following parameters to the `um.properties` file and set a value for these parameters.

For information about how to add these parameters to the `um.properties` file, see Configuring custom password policy for Usage Metering Collector user accounts on page 62.

Note:

Back up the `um.properties` file before performing any changes in the file. In case the `um.properties` file becomes corrupted, you can replace the corrupted file with the backup file.

Parameter name	Description	Default value	Minimum configurable value	Maximum configurable value
password.min.length	Type the minimum length of the password.	14 characters	8 characters	N/A
password.min.uppercase	Type the minimum number of uppercase letters the password must contain.	0	0	N/A
password.min.lowercase	Type the minimum number of lowercase letters the password must contain.	0	0	N/A
password.min.number	Type the minimum number of numeric digits the password must contain.	0	0	N/A
password.min.special	Type the minimum number of special characters the password must contain.	0	0	N/A
password.max.length	Type the maximum length of the password.	20 characters	N/A	20 characters
password.max.uppercase	Type the maximum number of uppercase letters the password can contain.	20	N/A	20
password.max.lowercase	Type the maximum number of lowercase letters the password can contain.	20	N/A	20
password.max.number	Type the maximum number of numeric digits the password can contain.	20	N/A	20
password.max.special	Type the maximum number of special characters the password can contain.	20	N/A	20

Table continues…

Parameter name	Description	Default value	Minimum configurable value	Maximum configurable value
password.history.size	Type the number of previous passwords that cannot be repeated.	10	0	24
password.max.age.days	Type the number of days for which a password must remain valid. After the validity period elapses, the password expires. The user must configure a new password on or before the password expiry date to operate the user account. If you set the value to 0, the passwords do not expire. This parameter is not applicable to the oldest user account that exists in Usage Metering Collector.	90	0	365
password.max.changes.per.day	Type the maximum number of times a user can change the password per day.	1	1	N/A
password.warning.days.before.expiration	Type how many days ahead of the password expiry day, a password expiry notification must be sent to a user.	10	1	Must be less than password.max.age.days value

Configuring a password reset policy for the Usage Metering Collector user accounts

About this task

Use this procedure to configure a password reset policy for the Usage Metering Collector user accounts.

The password reset policy is used when a user clicks the **Forgot your password?** option on the Usage Metering Collector login page to reset the password.

Before you begin

Back up the `um.properties` file before performing this procedure. In case the `um.properties` file becomes corrupted, you can replace the corrupted file with the backup file.

Procedure

1. At the Usage Metering Collector server CLI command prompt, run the following command to edit the `um.properties` file:

   `vi /opt/Avaya/usage-metering/um.properties`

2. Add the password reset policy parameters that you want in the following format to the `um.properties` file:

   <password reset policy parameter name>=<value>

   Add each password reset policy parameter on a separate line.

   For information about the configurable password reset policy parameters and their associated values, see Usage Metering Collector password reset policy parameters on page 65.

Example

To set a validity period of 48 hours for the password reset URL sent to the user when the user clicks **Forgot your password?**, add the reset.password.expiry.minutes parameter in the following format to the `um.properties` file:

```
reset.password.expiry.minutes=2880
```

Related links

Resetting the Usage Metering Collector password on page 60

Usage Metering Collector password reset policy parameters

To configure a password reset policy for the Usage Metering Collector user accounts, add the following parameters to the `um.properties` file and set a value for these parameters.

For information about adding these parameters to the `um.properties` file, see Configuring a password reset policy for the Usage Metering Collector user accounts on page 64.

Note:

Back up the `um.properties` file before performing any changes in the file. In case the `um.properties` file becomes corrupted, you can replace the corrupted file with the backup file.

Parameter name	Description	Default value	Minimum configurable value	Maximum configurable value
reset.password.expiry.minutes	Type the number of minutes for which the password reset URL must remain valid after Usage Metering sends the URL to the user. Usage Metering sends the password reset URL to the user after the user clicks **Forgot your password?** on the Usage Metering Collector login page.	1440	30	10080
reset.password.token.max.invalidAttempts	Type the maximum number of consecutive failed password reset attempts to be allowed to a user. After a user attempts the maximum number of consecutive failed password reset attempts, Usage Metering blocks any new password reset attempt by the user for the number of minutes you configure in the reset.password.token.invalidAttemptsLock.minutes parameter.	3	1	15
reset.password.token.invalidAttemptsLock.minutes	Type the number of minutes for which Usage Metering must block a new password reset attempt by a user who has attempted the maximum number of consecutive failed password reset attempts.	1	1	1440

Configuring an account lockout policy for Usage Metering Collector user accounts

About this task

You can configure an account lockout policy to determine the duration a user account must be locked due to invalid login attempts or account inactivity. A strong account lockout policy helps protect your Usage Metering Collector user accounts from password-guessing attacks.

Any changes to the account lockout policy are applied to a user account when the user logs on to the Usage Metering Collector for the first time after the policy is changed.

Before you begin

Back up the `um.properties` file before performing this procedure. If the `um.properties` file is corrupted, you can replace the corrupted file with the backup file.

Procedure

1. At the Usage Metering Collector server CLI command prompt, run the following command to edit the `um.properties` file:

   `vi /opt/Avaya/usage-metering/um.properties`

2. Set the values for the account lockout policy parameters as required in the `um.properties` file in the following format:

   <name of account lockout policy parameter>=<value>

   For information about the account lockout policy parameters and their associated values, see Account lockout policy parameters on page 67.

Example

To unlock a user account that is locked due to consecutive failed login attempts after 60 minutes, set the unlock.timeout.minutes parameter in the `um.properties` file in the following format:

```
unlock.timeout.minutes=60
```

Related links

Account lockout policy parameters on page 67

Account lockout policy parameters

You can set values for the following parameters in the `um.properties` file to configure an account lockout policy for the Usage Metering Collector user accounts.

For more information about configuring an account lockout policy, see Configuring an account lockout policy for Usage Metering Collector user accounts on page 66.

Note:

Back up the `um.properties` file before performing any changes in the file. If the `um.properties` file is corrupted, you can replace the corrupted file with the backup file.

Parameter name	Description	Default value	Minimum configurable value	Maximum configurable value
failed.logins.to.delay	Type the number of consecutive failed login attempts for applying the login processing delay configured in **Delay after 3 failed login attempts (seconds)**. The login processing delay is applied to the last login attempt of the total login attempts specified in this parameter. For example, if the value of this parameter is set to 4 and the first three consecutive login attempts by a user fail, then the fourth login attempt is processed for the number of seconds configured in **Delay after 3 failed login attempts (seconds)**. Thus, delaying the last login attempt. However, if a user provides valid credentials during the last login attempt, the delay is not applied to the login attempt. For information about setting the login processing delay, see Configuring session timeout and failed login attempt threshold on page 56.	3	0	N/A

Table continues…

Parameter name	Description	Default value	Minimum configurable value	Maximum configurable value
unlock.timeout.minutes	Type the number of minutes after which a locked user account must be automatically unlocked. This parameter applies to user accounts that are locked because of consecutive failed login attempts as set in **Account lockout threshold (failed login attempts)**. Set the value to 0 if you do not want to unlock a user account automatically. However, you can manually unlock the user account. For information about manually unlocking a user account, see Enabling or disabling a user account on page 59. For information about setting the failed login attempt threshold, see Configuring session timeout and failed login attempt threshold on page 56.	10	0	N/A
lock.account.days	Type the number of days of inactivity, that is, zero logins done by using a user account, after which the user account must be locked. The counter to count the number of days specified in this parameter starts from the password expiry day. Set the value to 0 if you do not want to lock the user accounts because of inactivity. This parameter does not apply to the oldest user account in Usage Metering Collector.	10	0	N/A

Related links

Configuring an account lockout policy for Usage Metering Collector user accounts on page 66

Setting the limit for concurrent login sessions for the Usage Metering Collector web interface

About this task

You can use any one of the following parameters to limit the number of concurrent login sessions to the Usage Metering Collector web interface:

Parameter name	Description	Default value	Minimum configurable value	Maximum configurable value
maximum.concurrenct.session	Parameter to limit the total number of concurrent login sessions to the Usage Metering Collector web interface.	100	1	150
maximum.concurrenct.session.per.user	Parameter to limit the number of concurrent login sessions per user to the Usage Metering Collector web interface.	5	1	50

The concurrent number of login sessions value you set takes effect for a user account when the user logs on to the Usage Metering Collector after you set the value.

Before you begin

Back up the `um.properties` file before performing this procedure. In case the `um.properties` file becomes corrupted, you can replace the corrupted file with the backup file.

Procedure

1. At the Usage Metering Collector server CLI command prompt, run the following command to edit the `um.properties` file:

   `vi /opt/Avaya/usage-metering/um.properties`

2. Do one of the following:
   - To set the limit for the total number of concurrent login sessions, add the following parameter to the `um.properties` file:

     maximum.concurrenct.session=<*Total number of concurrent login sessions to be allowed*>
   - To set the limit for the number of concurrent login sessions per user, add the following parameter to the `um.properties` file:

     maximum.concurrenct.session.per.user=<*Number of concurrent login sessions to be allowed per user*>

Example

To limit the number of concurrent login sessions per user to 4, add the maximum.concurrenct.session.per.user parameter in the following format to the `um.properties` file:

```
maximum.concurrenct.session.per.user=4
```

Enabling SNMP keep-alive trap messages from Usage Metering Collector

About this task

You can configure the keep-alive parameters to send the SNMP keep-alive trap messages at regular intervals from the Usage Metering Collector.

When the keep-alive parameters are enabled, Usage Metering Collector sends `UM Alert 990: Test Alert`, which is a keep-alive trap message, to the SNMP trap receiver configured in the **SNMP Trap Send Address** field in the Usage Metering Collector.

The keep-alive trap messages are generated for the SNMP version, that is, v2 or v3, configured in the Usage Metering Collector. For more information, see Configuring alerts on page 54.

Usage Metering Collector sends the keep-alive trap messages to the SNMP trap receiver as per the configured interval and also every time the Usage Metering Collector starts.

You can use the keep-alive trap messages to monitor the status of the Usage Metering Collector at regular intervals.

By default, the keep-alive trap messages are disabled.

For information about the configurable keep-alive parameters and their associated values, see Usage Metering keep-alive parameters on page 72.

Before you begin

- Ensure that an SNMP trap receiver is configured in the **SNMP Trap Send Address** field in the Usage Metering Collector.
- Back up the `um.properties` file before performing this procedure. In case the `um.properties` file becomes corrupted, you can replace the corrupted file with the backup file.

Procedure

1. At the Usage Metering Collector server CLI command prompt, run the following command to edit the `um.properties` file:

   `vi /opt/Avaya/usage-metering/um.properties`

2. Add the keep-alive parameters in the following format to the `um.properties` file:

   <keep-alive parameter name>=<value>

   Add each parameter on a separate line.

Example

To enable the keep-alive trap messages, add the keep.alive.snmp.enabled parameter in the following format to the `um.properties` file:

```
keep.alive.snmp.enabled=true
```

Next steps

Restart the Usage Metering Collector to apply the keep-alive parameter configuration.

Usage Metering keep-alive parameters

You can configure the following keep-alive parameters in the `um.properties` file to send the keep-alive trap messages at regular intervals from the Usage Metering Collector to the SNMP trap receiver.

For information about configuring the keep-alive parameters, see Enabling SNMP keep-alive trap messages from Usage Metering Collector on page 71.

Note:

Back up the `um.properties` file before performing any changes in the file. In case the `um.properties` file becomes corrupted, you can replace the corrupted file with the backup file.

Parameter name	Description	Default value	Minimum configurable value	Maximum configurable value
keep.alive.snmp.enabled	Parameter to enable or disable the SNMP keep-alive trap messages from the Usage Metering Collector. Valid values are `true` and `false`.	false	Not applicable	Not applicable
keep.alive.snmp.interval.minutes	Parameter to configure the interval, in minutes, after which the Usage Metering Collector must send a keep-alive trap message to the SNMP trap receiver.	1440	1	10080

Enabling or disabling hostname validation

About this task

Hostname validation is performed when establishing an SSL connection between Usage Metering and other applications, such as CMS, to validate the hostname of the server where the application is hosted.

When hostname validation is enabled, the hostname of the application server configured in Usage Metering must match the hostname present in the Subject Alternative Name (SAN) or Common Name (CN) field of the certificate installed in Usage Metering for authenticating with the application server. Otherwise, the SSL connection fails.

By default, hostname validation is enabled in Usage Metering.

You can also disable hostname validation in Usage Metering to allow SSL connection without performing hostname validation.

Before you begin

Back up the `um.properties` file before performing this procedure. In case the `um.properties` file becomes corrupted, you can replace the corrupted file with the backup file.

Procedure

1. At the Usage Metering Collector server CLI command prompt, run the following command to edit the `um.properties` file:

   `vi /opt/Avaya/usage-metering/um.properties`

2. To disable hostname validation, in the `um.properties` file, set the ssl.hostname.validation parameter to `false`.
3. To enable hostname validation, set the ssl.hostname.validation parameter to `true`.

Installing and configuring Advanced Intrusion Detection Environment utility

About this task

You can use the Advanced Intrusion Detection Environment (AIDE) utility to protect the Usage Metering files from unauthorized changes and cyber attacks.

AIDE creates a database of files based on the files and directories you specify in the `/etc/aide.conf` file, and uses the database to ensure file integrity and detect system intrusions.

AIDE validates the integrity of a file to determine whether it is altered after its creation, curation, archiving, or any other qualifying event.

Procedure

1. To install AIDE, at the Usage Metering Collector server CLI command prompt, run the following command:

   `yum install aide`

2. **(Optional)** To view the version number of the installed AIDE utility, run the following command:

   `aide -v`

3. To edit the `/etc/aide.conf` file, run the following command:

   `vi /etc/aide.conf`

4. Add the following to the `/etc/aide.conf` file:

   ```
   add
   # Just do md5 and sha256 hashes
   LSPP = R+sha256
   /opt/apache-tomcat/usage-metering/ LSPP
   /opt/Avaya/usage-metering/bin/ LSPP
   ```

5. To initialize the AIDE database, run the following command:

   `aide --init`

   The preceding command creates an initial `/var/lib/aide/aide.db.new.gz` database.

6. Because AIDE performs checks on the `/var/lib/aide/aide.db.gz` database, rename the database to `/var/lib/aide/aide.db.gz` by running the following command:

   `mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz`

7. To manually check the AIDE database for any updates, run the following command:

   `aide --check`

8. If there are any changes to the already selected files or addition of new file definitions in the configuration file, manually update the AIDE database by running the following command:

   `aide --update`

   The preceding command creates the `/var/lib/aide/aide.db.new.gz` database.

9. To start using the updated database for integrity checks, rename the AIDE database to `/var/lib/aide/aide.db.gz` by running the following command:

   `mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz`

Chapter 5: Certificate management

SSL certificate

Generating a certificate signing request

About this task

Use this procedure to generate a certificate signing request (CSR) file by using the Usage Metering Collector. Install the CA server certificate file on the same Usage Metering server.

Note:

When you have a pending CSR request, the Usage Metering Collector interface displays an option to install the CSR response.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click , and then click **CERTIFICATES**.
3. In the left navigation pane, click **GENERATE CSR/SELF-SIGNED CERT**.
4. In the **commonName (typically the FQDN of the server)** field, type the FQDN that you want to secure with the certificate. For example, www.avaya.com
5. In the **orgUnitName** field, type the name of the department or unit that is generating the certificate signing request.
6. In the **orgName** field, type the legal name of your organization.
7. In the **city** field, type the name of the city where your organization is legally incorporated.
8. In the **stateorProv** field, type the name of the state or province where your organization is legally incorporated.
9. In the **countryCode** field, type the two-letter country code where your organization is legally incorporated. For example, US
10. Click **GENERATE CSR**.
11. In the **Certificate Signing Request (CSR) for Usage Metering** dialog box, copy all the encrypted text.
12. Save the copied CSR text.

    Save the CSR text in the `.pem` file format. A CSR file is a private key.

13. Send your CSR to the CA.

Next steps

Install the CSR response. For more information, see Installing the CSR response on page 76.

Installing the CSR response

About this task

Use this procedure to install a signed CA server certificate file on the Usage Metering server.

A CSR response is a CA server certificate file generated by the CA.

When a Certificate Signing Request (CSR) that you generate is in a pending state, Usage Metering Collector displays an option to install the CSR response.

Uploading a certificate chain file is optional. Contact your CA to check whether you need to upload a certificate chain file.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click , and then click **CERTIFICATES**.
3. In the left navigation pane, click **INSTALL CSR RESPONSE**.
4. To install the CA server certificate, do any of the following:
   - To install the CA server certificate by copying the certificate text, click **from text** and do the following:
     a. Open the CA server certificate file and copy the text from the file.
     b. In the **Signed Certificate** field, paste the copied text.
   - To install the CA server certificate by uploading the CA server certificate file, click **from file** and do the following:
     a. Click **UPLOAD** next to **Signed Certificate**.
     b. Browse to the location of the CA server certificate file and select the file.
5. To install the certificate chain file, do any of the following:
   - To install the certificate chain file by copying the certificate text, click **from text** and do the following:
     a. Open the certificate chain file and copy the text from the file.
     b. In the **Certificate chain (optional)** field, paste the copied text.
   - To install the certificate chain file by uploading the certificate chain file, click **from file** and do the following:
     a. Click **UPLOAD** next to **Certificate chain (optional)**.
     b. Browse to the location of the certificate chain file and select the file.
6. Click **INSTALL**.

The system replaces the default SSL certificate for the HTTPS interface of the web user interface with the new certificate.

7. Refresh your browser to reload the Usage Metering user interface.
8. Click **INSTALLED CERTIFICATES** to view the CA server certificate file in the list of installed certificates.

Result

The browser does not display an invalid certificate warning when you log on to the Usage Metering Collector web interface.

The system identifies your Usage Metering web connection as a secure connection.

The Usage Metering server can validate whether there is no man-in-the-middle attack proxy.

Generating a self-signed certificate

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click  , and then click **CERTIFICATES**.
3. In the left navigation pane, click **GENERATE CSR/SELF-SIGNED CERT**.
4. In the **commonName (typically the FQDN of the server)** field, type the FQDN that you want to secure with the certificate.

   For example, www.avaya.com
5. In the **orgUnitName** field, type the name of the department or unit that is generating the certificate signing request.
6. In the **orgName** field, type the legal name of your organization.
7. In the **city** field, type the name of the city where your organization is legally incorporated.
8. In the **stateorProv** field, type the name of the state or province where your organization is legally incorporated.
9. In the **countryCode** field, type the two-letter country code where your organization is legally incorporated.

   For example, US
10. Click **GENERATE SELF-SIGNED CERT**.

Installing a server certificate

About this task

Use this procedure to install a signed CA server certificate on the Usage Metering server.

A CA server generates a signed CA certificate.

The signed CA certificate is generated independently on a CA server, where you get the private key along with the signed CA certificate.

A server certificate is an SSL certificate that a CA generates.

Uploading a certificate chain file is optional. Contact your CA to check whether you need to upload a certificate chain file. The CA provides the certificate chain file.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click , and then click **CERTIFICATES**.
3. In the left navigation pane, click **INSTALL SERVER CERTIFICATE**.
4. To install the CA server certificate, do any of the following:
   - To install the CA server certificate by copying the certificate text, click **from text** and do the following:
     a. Open the CA server certificate file and copy the text from the file.
     b. In the **Signed Certificate** field, paste the copied text.
   - To install the CA server certificate by uploading the CA server certificate file, click **from file** and do the following:
     a. Click **UPLOAD** next to **Signed Certificate**.
     b. Browse to the location of the CA server certificate file and select the file.
5. To install the private key file, do any of the following:
   - To install the private key file by copying the private key text, click **from text** and do the following:
     a. Open the private key file that you receive from the CA and copy the text from the file.

        You can use a console to generate the private key file.
     b. In the **Private key** field, paste the copied text.
   - To install the private key file by uploading the private key file, click **from file** and do the following:
     a. Click **UPLOAD** next to **Private Key**.
     b. Browse to the location of the file and select the file.
6. To install the certificate chain file, do any of the following:
   - To install the certificate chain file by copying the certificate text, click **from text** and do the following:
     a. Open the certificate chain file and copy the text from the file.
     b. In the **Certificate chain (optional)** field, paste the copied text.
   - To install the certificate chain file by uploading the certificate chain file, click **from file** and do the following:
     a. Click **UPLOAD** next to **Certificate chain (optional)**.

b. Browse to the location of the certificate chain file and select the file.

7. Click **INSTALL**.

   The system replaces the SSL certificate for the HTTPS interface of the web user interface.

8. Refresh your browser to reload the Usage Metering Collector interface.
9. Click **INSTALLED CERTIFICATES** to view the CA server certificate file in the list of installed certificates.

Result

The browser does not display an invalid certificate warning when you log on to the Usage Metering Collector web interface.

The system identifies your Usage Metering web connection as a secure connection.

The Usage Metering server can validate whether there is no man-in-the-middle attack proxy.

CA SSL certificate

Retrieving certificate from a standalone Avaya WebLM

About this task

Use this procedure to retrieve the certificate from a standalone Avaya WebLM by using the Firefox browser.

Note:

Ensure that the version number of Firefox is 76.0.1 or later.

Procedure

1. On the web browser, type the URL of the standalone Avaya WebLM:

   `https://<Fully Qualified Domain Name>:<PortNumber>/WebLM`

2. On the address bar, click the **Lock** icon.
3. Click the **Show connection details** icon.
4. Click **More Information**.
5. Click **View certificates**.

   The certificate details are displayed in a new browser.

6. Click **Download**, and then click **PEM (cert)**.
7. Save the certificate to your local computer.

Next steps

Install the certificate in Usage Metering.

For more information, see Installing an outbound certificate on page 80.

Installing an outbound certificate

About this task

Use this procedure to do the following:

- Enable Usage Metering to trust a certificate authority (CA) such as an internal CA provided by your IT department.
- Add an outbound certificate of the server to which the Usage Metering server connects.
- Establish an outbound SSL connection from the Usage Metering server to other servers such as an SMTP server.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click  , and then click **CERTIFICATES**.
3. In the left navigation pane, click **INSTALL OUTBOUND CERTIFICATES**.
4. If you select the **from text** option, do the following:
   a. In the **Certificate alias** field, type a name for the certificate.
   b. Open the outbound certificate file and copy the text from the file.
   c. In the **Signed Certificate** field, paste the copied text.
5. If you select the **from file** option, do the following:
   a. In the **Certificate alias** field, type a name for the certificate.
   b. Click **UPLOAD** next to the **Signed Certificate** field.
   c. Browse to the location of the file and select the file.
6. Click **INSTALL**.

Viewing installed certificates

About this task

Use this procedure to view the certificates that are installed in Usage Metering.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click  , and then click **CERTIFICATES**.
3. In the left navigation pane, click **INSTALLED CERTIFICATES**.
4. Click **Alias** to sort the certificates by name.

5. Click **Show Details**  to view the certificate details.

Chapter 6: Avaya OneCloud™ Subscription system management in Usage Metering Collector

Avaya OneCloud™ Subscription system

Avaya OneCloud™ Subscription system is a group of Avaya UC and CC applications aligned to one active instance of Communication Manager — simplex or duplex.

After you configure the connectivity between Usage Metering and Avaya back-office systems, your Avaya OneCloud™ Subscription system order that was placed in the Avaya One Source ordering portal appears under your offer ID in the Usage Metering Collector.

For more information, see Configuring connectivity between Usage Metering and Avaya back-office systems on page 52.

You can click the offer ID to view your subscribed Avaya OneCloud™ Subscription systems within the offer. Each Avaya OneCloud™ Subscription system has a subscription ID assigned to it, and is associated with the service bundle that you ordered for this Avaya OneCloud™ Subscription system.

Any new Avaya OneCloud™ Subscription system order received by the Usage Metering Collector appears in an **ORDERED** state. The Usage Metering Collector verifies the order and automatically updates the state to **INSTALLING**.

Use the Usage Metering Collector to configure the Avaya OneCloud™ Subscription system:

- Add the WebLM server to your Avaya OneCloud™ Subscription system.

  After the Usage Metering Collector successfully registers to the WebLM server, Usage Metering automatically retrieves the subscription license for the subscribed applications from the Avaya back-office systems and installs it on the WebLM server.

  For more information, see Adding a WebLM server to an Avaya OneCloud Subscription system on page 89.

  For information about managing the WebLM servers for licenses, see WebLM management on page 86.
- Add the on-premise Avaya UC and CC applications that are entitled by the subscription license to your Avaya OneCloud™ Subscription system.

The applications that you can add to an Avaya OneCloud™ Subscription system depend on the service bundle that you ordered for the Avaya OneCloud™ Subscription system.

These on-premise applications can run by using the subscription license only after you add these applications to the Avaya OneCloud™ Subscription system.

For more information, see Adding an application to the Avaya OneCloud Subscription system on page 111.

Some applications, such as Avaya Call Management System, are called data source applications in Avaya OneCloud™ Subscription because Usage Metering collects usage data from these applications.

For more information, see Data source applications on page 83.

Depending on the service bundle that you order, some applications are mandatory in your Avaya OneCloud™ Subscription system. You must add the mandatory applications to your Avaya OneCloud™ Subscription system.

For more information, see Mandatory applications in an Avaya OneCloud Subscription system on page 85.

You can also share applications between two or more Avaya OneCloud™ Subscription systems.

For more information, see Application sharing between two or more Avaya OneCloud Subscription systems on page 23.

You can modify or remove applications and WebLMs from your Avaya OneCloud™ Subscription system.

An Avaya OneCloud™ Subscription system can contain only those applications that are entitled by a subscription license.

Important:

Do not configure the same Avaya OneCloud™ Subscription system in multiple Usage Metering Collectors because it causes duplicate usage calculation.

For more information, see Considerations for configuring Avaya OneCloud Subscription systems of the same subscription offer in multiple Usage Metering Collectors on page 36.

For information about the Avaya OneCloud™ Subscription system process flow, see Avaya OneCloud Subscription system process flow on page 25.

Data source applications

Usage Metering collects usage data from the following applications of your Avaya OneCloud™ Subscription system for usage reporting:

- Avaya Aura® Application Enablement Services

- Avaya Aura® Experience Portal

  Currently, Avaya OneCloud™ Subscription supports Avaya Aura® Experience Portal that uses the local Postgres database, external Postgres database, or external Microsoft SQL database.
- Avaya Aura® Messaging
- Avaya Aura® System Manager
- Avaya Callback Assist
- Avaya Call Management System
- Avaya IX™ Messaging

Because usage data is collected from these applications, these applications act as data sources in Avaya OneCloud™ Subscription.

The data source applications that you can add to your Avaya OneCloud™ Subscription system depend on the service bundle that you order for the Avaya OneCloud™ Subscription system.

Note:

Before you add a data source application to your Avaya OneCloud™ Subscription system, you must perform the prerequisites for adding the data source application.

For example, prerequisites for adding certain data source application can involve the following:

- Installing certificates.
- Creating a new user account in the data source application. You need to use the access credentials of the new user account when adding the data source application to your Avaya OneCloud™ Subscription system. Usage Metering Collector uses these credentials to connect to the data source application for collecting usage data.

For information about the prerequisites for adding data source applications to your Avaya OneCloud™ Subscription system, see:

- Prerequisites and process for adding Application Enablement Services on page 94
- Prerequisites and process for adding Experience Portal Manager on page 95
- Prerequisites and process for adding Avaya Aura Messaging on page 99
- Prerequisites and process for adding System Manager on page 102
- Prerequisites and process for adding Avaya Callback Assist Application Server on page 104
- Prerequisites and process for adding Avaya Call Management System on page 106
- Prerequisites and process for adding Avaya IX Messaging on page 109

Mandatory applications in an Avaya OneCloud™ Subscription system

Depending on the service bundle that you order, some applications are mandatory in your Avaya OneCloud™ Subscription system. A service bundle is a collection of services that are grouped. An example of a service is the Avaya Aura® Experience Portal IVR service. An example of a service bundle is Calling plus Voicemail.

Note:

You must add the mandatory applications to your Avaya OneCloud™ Subscription system.

The following table provides the list of mandatory applications for each service bundle type:

Service bundle	Mandatory applications
Basic UC	• Avaya Aura® Communication Manager • Avaya Aura® System Manager
Core UC	• Avaya Aura® Communication Manager • Avaya Aura® System Manager
Power UC	• Avaya Aura® Communication Manager • Avaya Aura® System Manager
Basic Voice CC	• Avaya Aura® Communication Manager • Avaya Aura® System Manager • Avaya Call Management System (CMS)
IVR CC (without Basic UC, Core UC, or Power UC)	• Avaya Aura® Experience Portal
UC Add-Ons	
UC Attendant	• Avaya IX™ Workplace Attendant
UC Messaging Speech	• Avaya IX™ Messaging
UC Messaging Transcription	• Avaya IX™ Messaging
CC Add-Ons	
Computer Telephony Integration (CTI)	• Avaya Aura® Application Enablement Services
Callback Assist	• Avaya Callback Assist

Related links

Adding an application to the Avaya OneCloud Subscription system on page 111

Avaya OneCloud™ Subscription system management

WebLM management

Avaya OneCloud™ Subscription system is a collection of UC and CC applications (Single or Geo-redundant data centers) connected to one or more WebLM servers, depending on your deployment model, for licensing.

Note:

You must add the WebLM server to your Avaya OneCloud™ Subscription system by using the Usage Metering Collector.

After the Usage Metering Collector successfully registers to the WebLM server, Usage Metering automatically retrieves the subscription license for the subscribed applications from the Avaya back-office system and installs it on the WebLM server.

Supported WebLM servers

Avaya OneCloud™ Subscription currently supports the following WebLM servers:

- Standalone Avaya WebLM.
- WebLM that is provided by Avaya Aura® System Manager.

Caveats

- You cannot share a WebLM server between two or more Avaya OneCloud™ Subscription systems.
- Installing multiple Avaya Call Management System (CMS) and Avaya IX™ Messaging applications that are part of the same Avaya OneCloud™ Subscription system requires separate WebLM servers.

  For example, if the subscription license of your Avaya OneCloud™ Subscription system contains entitlements for two CMS applications and you want to install both the CMS applications, you must configure two separate WebLM servers. You must then add these WebLM servers to your Avaya OneCloud™ Subscription system, and register the Usage Metering Collector to these WebLM servers. After successful registration, Usage Metering automatically installs the subscription license for the Avaya OneCloud™ Subscription system on these WebLM servers. You must use the subscription license from one of these WebLM servers to install one CMS. To install the second CMS, you must use the subscription license that is installed on the other WebLM server.
- The WebLM server that you add to your Avaya OneCloud™ Subscription system for installing the subscription license must not already host an activated perpetual license.

  However, if you want to install the subscription license on a WebLM server that already hosts an activated perpetual license, create a service request with Avaya at: https://support.avaya.com

Related links

License and software enablement on page 24

Prerequisites for adding a System Manager-provided WebLM to an Avaya OneCloud™ Subscription system

If you are using a WebLM server that is provided by System Manager, then you must perform the following prerequisites before adding the WebLM server to the Avaya OneCloud™ Subscription system:

No.	Prerequisite	Related topic
1	Install the System Manager certificate in Usage Metering Collector.	Installing the System Manager certificate in Usage Metering Collector on page 87
2	Create a new administrative user account in System Manager.	Create a new administrative user account in System Manager on page 88

Installing the System Manager certificate in Usage Metering Collector

Procedure

1. Do one of the following:
   - If you have performed a new installation of System Manager Release 8.1.x, export the System Manager-signed root CA certificate from System Manager.

     For more information, see Exporting the System Manager-signed root CA certificate from System Manager on page 88.
   - If System Manager has been upgraded from Release 7.0.x and earlier, do one of the following:
     - If System Manager uses the System Manager root CA certificate, export the System Manager-signed root CA certificate from System Manager.

       For more information, see Exporting the System Manager-signed root CA certificate from System Manager on page 88.
     - If System Manager uses the SIP CA Demo certificate, export the SIP CA-signed Demo certificate from System Manager.

       For more information, see Exporting the SIP CA-signed Demo certificate from System Manager on page 88.

       Note:

       Because the SIP CA Demo certificate is not NIST compliant, Avaya recommends you to replace the SIP CA Demo certificate with the System Manager root CA certificate in System Manager. You must then export the System Manager-signed root CA certificate from System Manager and install it in the Usage Metering Collector.

       For information about replacing the certificate in System Manager, see the *Certificate Management for Avaya Aura® System Manager* guide.
2. Install the certificate that you exported from System Manager in the Usage Metering Collector.

   For more information, see Installing an outbound certificate on page 80.

Exporting the System Manager-signed root CA certificate from System Manager

About this task

For any recent updates in this procedure, see the *Administering Avaya Aura® System Manager* guide.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.
4. Click **Download PEM file** corresponding to the **tmdefaultca** section to download the System Manager-signed root CA certificate.

Exporting the SIP CA-signed Demo certificate from System Manager

About this task

For any recent updates in this procedure, see the *Certificate Management for Avaya Aura® System Manager* guide.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Select the primary or secondary System Manager instance.
4. Click **More Actions** > **Manage Identity Certificates**.
5. Select the **webIm** service in the list.
6. Click **Export** to export the SIP CA-signed Demo certificate.

Create a new administrative user account in System Manager

Do the following by using the System Manager web console:

- Create a new administrative user in System Manager and assign the System Administrator role to the user.

  For more information, see “Adding an administrative user” in the *Administering Avaya Aura® System Manager* guide.

Note:

You must use the access credentials of this administrative user when adding the System Manager-provided WebLM to your Avaya OneCloud™ Subscription system.

Do not use these access credentials to perform any other operations in System Manager.

Adding a WebLM server to an Avaya OneCloud™ Subscription system

Before you begin

- For information about the WebLM server that you can use in an Avaya OneCloud™ Subscription system to install the subscription license, see WebLM management on page 86.
- If you are migrating the on-premise applications from perpetual licenses to subscription license, delete the perpetual licenses, license entitlements of which are transferred to Avaya OneCloud™ Subscription, from your WebLM server.

  For more information, see Migrating applications from perpetual licenses to subscription license on page 127.

  Important:

  Do not delete the perpetual licenses, license entitlements of which are not transferred to Avaya OneCloud™ Subscription.
- Before adding a System Manager-provided WebLM to the Avaya OneCloud™ Subscription system, ensure that you perform the prerequisites.

  For more information, see Prerequisites for adding a System Manager-provided WebLM to an Avaya OneCloud Subscription system on page 87.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.
3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.
4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system in which you want to add the WebLM server.
5. On the **WEBLMS** tab, click **Add WebLM**.
6. In the Add WebLM dialog box, in the **WebLM Name** field, type a name for the WebLM server.
7. In the **Primary Host** field, type the FQDN of the WebLM server.
8. In the **Failover Host** field, type the FQDN of the fail-over WebLM server.
9. In the **Port** field, type the port number to access the WebLM server.
10. In the **WebLM Username** field, type the user name to access the WebLM server.
11. In the **WebLM Password** field, type the password to access the WebLM server.
12. Click **SAVE** to add the WebLM server to the Avaya OneCloud™ Subscription system and register the Usage Metering Collector to the WebLM server.

Result

After the Usage Metering Collector successfully registers to the WebLM server:

- The **WEBLMS** tab displays the host ID of the WebLM server and changes the **Status** to **Registered**.
- Usage Metering automatically retrieves the subscription license from the Avaya back-office system and installs it on the WebLM server. After the license is successfully installed, the **Subscription License Status** on the **WEBLMS** tab changes to **Installed**.

Editing a WebLM server

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.
3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.
4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system.
5. On the **WEBLMS** tab, click **Edit WebLM** corresponding to the WebLM server that you want to edit.
6. In the Edit WebLM dialog box, do the required modifications.
7. Do any one of the following:
   - Click **SAVE**.

     Usage Metering saves the changes.
   - Click **REGISTER**.

     Usage Metering saves the changes, registers with the WebLM server by using the updated details, retrieves the subscription license for the subscribed applications from the Avaya back-office system, and installs it on the WebLM server.

     The **REGISTER** option is available only when you edit an unregistered WebLM server.
   - Click **UNREGISTER**.

     Usage Metering removes the subscription license from the WebLM server and unregisters with the WebLM server.

     The **UNREGISTER** option is available only when you edit a registered WebLM server.

     For more information, see Unregistering and re-registering a WebLM server on page 90.

Unregistering and re-registering a WebLM server

About this task

Use this procedure to unregister and re-register a WebLM server.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.
3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.
4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system.
5. On the **WEBLMS** tab, click **Edit WebLM** corresponding to the WebLM server that you want to unregister.
6. In the Edit WebLM dialog box, click **UNREGISTER**.

   Usage Metering removes the subscription license from the WebLM server and unregisters with the WebLM server.

   The **UNREGISTER** option is available only when you edit a registered WebLM server.
7. To re-register with the WebLM server, in the Edit WebLM dialog box, click **REGISTER**.

   Usage Metering re-registers with the WebLM server, retrieves the subscription license for the subscribed applications from the Avaya back-office system, and installs it on the WebLM server.

Deleting a WebLM server

About this task

Use this procedure to delete a WebLM server from an Avaya OneCloud™ Subscription system.

Caution:

Do not delete an active WebLM server. If you delete an active WebLM server, the applications that use the subscription license that is installed on the WebLM server run in a license error mode. This causes your Avaya OneCloud™ Subscription system to stop after the permitted grace number of days.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.
3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.
4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system.

5. On the **WEBLMS** tab, click **Delete** corresponding to the WebLM server that you want to delete.
6. In the Delete WebLM dialog box, click **OK** to delete the WebLM server from the Avaya OneCloud™ Subscription system.

Application management

You can add, edit, share, and delete the subscribed Avaya UC and CC applications from your Avaya OneCloud™ Subscription system.

After the subscription license is installed on the WebLM server, you must add the on-premise applications that are entitled by the subscription license to your Avaya OneCloud™ Subscription system.

The applications that you can add to each Avaya OneCloud™ Subscription system depend on the service bundle that you have ordered for the Avaya OneCloud™ Subscription system.

Note:

The on-premise applications that are entitled by the subscription license can run by using the subscription license only after you add the applications to the Avaya OneCloud™ Subscription system.

Some applications, such as Avaya Call Management System, are called data source applications in Avaya OneCloud™ Subscription because Usage Metering collects usage data from these applications.

Depending on the service bundle that you order, some applications are mandatory in your Avaya OneCloud™ Subscription system. You must add the mandatory applications to your Avaya OneCloud™ Subscription system.

For more information, see Checklist for adding applications to an Avaya OneCloud Subscription system on page 92.

You can also share applications between two or more Avaya OneCloud™ Subscription systems.

For more information, see Application sharing between two or more Avaya OneCloud Subscription systems on page 23.

Related links

WebLM management on page 86

Checklist for adding applications to an Avaya OneCloud™ Subscription system

Ensure that you adhere to the following checklist for adding your on-premise applications that are entitled by the subscription license to the Avaya OneCloud™ Subscription system.

The applications that you can add to each Avaya OneCloud™ Subscription system depend on the service bundle that you have ordered for the Avaya OneCloud™ Subscription system.

No.	Item	Related topic	Notes	✔
1	The on-premise application must be of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version. If the on-premise application is of an earlier version than the minimum supported version, then before adding the application to the Avaya OneCloud™ Subscription system, upgrade the on-premise application to at least the minimum supported version.	Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30		
2	Before adding a data source application to your Avaya OneCloud™ Subscription system, ensure that you perform the prerequisites for adding the data source application to your Avaya OneCloud™ Subscription system.	• Data source applications on page 83 • Prerequisites and process for adding Application Enablement Services on page 94 • Prerequisites and process for adding Experience Portal Manager on page 95 • Prerequisites and process for adding Avaya Aura Messaging on page 99 • Prerequisites and process for adding System Manager on page 102 • Prerequisites and process for adding Avaya Callback Assist Application Server on page 104 • Prerequisites and process for adding Avaya Call Management System on page 106 • Prerequisites and process for adding Avaya IX Messaging on page 109		

Table continues…

No.	Item	Related topic	Notes	✔
3	Add all on-premise applications that are entitled by the subscription license to your Avaya OneCloud™ Subscription system. The on-premise applications that are entitled by the subscription license can run by using the subscription license only after you add the applications to the Avaya OneCloud™ Subscription system.	Adding an application to the Avaya OneCloud Subscription system on page 111		
4	Depending on your service bundle order type, add the mandatory applications to your Avaya OneCloud™ Subscription system.	Mandatory applications in an Avaya OneCloud Subscription system on page 85		

Related links

Adding an application to the Avaya OneCloud Subscription system on page 111

Prerequisites and process for adding Application Enablement Services

The following table provides step-by-step information about the prerequisites and process for adding Application Enablement Services that is entitled by the subscription license to your Avaya OneCloud™ Subscription system:

Step	Task	Related topic
Perform the following prerequisites before adding Application Enablement Services to the Avaya OneCloud™ Subscription system:		
1	Ensure that the on-premise installed Application Enablement Services is of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version. If the on-premise Application Enablement Services is of an earlier version than the minimum supported version, upgrade it to at least the minimum supported version.	Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30
2	Create a new user account in Application Enablement Services.	Create a new user account in Application Enablement Services on page 95
Add Application Enablement Services:		

Table continues…

Step	Task	Related topic
3	Add Application Enablement Services to the Avaya OneCloud™ Subscription system.	• Adding an application to the Avaya OneCloud Subscription system on page 111 • Create Application page field descriptions on page 112

Create a new user account in Application Enablement Services

Do the following by using the Application Enablement Services – Management Console:

- Create a new user account in the `susers` Linux group.

  When creating a new user account, ensure the following:

  - In the **Default Login Group** field, type `susers`.
  - Select the **Allow Linux Shell Access** check box.
  - In the **Maximum number of days a password may be used (PASS_MAX_DAYS)** field, type the number of days after which the password for this user account must expire.

    Avaya recommends you to set this value to the maximum number of days, which is `99999` days.

    If you set this value to fewer number of days and if you do not change the password on time and the password expires, Usage Metering cannot connect to Application Enablement Services.

  For more information, see “Adding a local Linux account for an administrator” in the *Administering Avaya Aura® Application Enablement Services* guide.

Note:

You must use the access credentials of this user when adding Application Enablement Services to your Avaya OneCloud™ Subscription system in the Usage Metering Collector. Usage Metering Collector uses these access credentials to connect to Application Enablement Services.

Do not use these access credentials to perform any other operations in Application Enablement Services.

Prerequisites and process for adding Experience Portal Manager

Usage Metering collects usage data from the Experience Portal database.

Note:

Currently:

- Avaya OneCloud™ Subscription supports Experience Portal that uses any of the following databases only:
  - Experience Portal local Postgres database

- External Postgres database
- External Microsoft SQL database

- Avaya OneCloud™ Subscription supports SSL connection for the Experience Portal local Postgres and external Postgres databases only.

The following table provides step-by-step information about the prerequisites and process for adding Experience Portal Manager (EPM) (also known as Voice Portal EPM) that is entitled by the subscription license to your Avaya OneCloud™ Subscription system:

Step	Task	Related topic
Perform the following prerequisites before adding EPM to the Avaya OneCloud™ Subscription system:		
1	Ensure that the on-premise installed Experience Portal is of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version. If the on-premise Experience Portal is of an earlier version than the minimum supported version, upgrade it to at least the minimum supported version.	Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30
2	Create a new read-only user account for the Experience Portal database.*	Create a read-only user account for the Experience Portal database on page 96
3	If you want to enable SSL connection between Experience Portal local or external Postgres database and Usage Metering, perform the prerequisites for enabling SSL connection.*	Enabling SSL connection between Experience Portal Postgres database and Usage Metering on page 97
Add EPM:		
4	Add EPM to the Avaya OneCloud™ Subscription system.	• Adding an application to the Avaya OneCloud Subscription system on page 111 • Create Application page field descriptions on page 112

* You need not perform these prerequisites for adding an auxiliary EPM to the Avaya OneCloud™ Subscription system.

Create a read-only user account for the Experience Portal database

Do one of the following:

- If Experience Portal uses the local Postgres database, then on the EPM server, create a new read-only (report) user account for the local Postgres database.

  For more information, see Creating a read-only user account for Experience Portal local Postgres database on page 97.

- If Experience Portal uses an external Postgres database or Microsoft SQL database, create a new read-only user account for the external Postgres database or Microsoft SQL database.

For more information, see the *Administering Avaya Aura® Experience Portal* guide.

Note:

You must use the access credentials of this user account when adding the EPM to your Avaya OneCloud™ Subscription system in the Usage Metering Collector. Usage Metering Collector uses these access credentials to connect to the Experience Portal database.

Do not use these access credentials to perform any other operations in Experience Portal.

Creating a read-only user account for Experience Portal local Postgres database

About this task

Use this procedure to create a read-only (report) user account for the Experience Portal local Postgres database.

For more information about this procedure, see “Configuring the PostgreSQL database user accounts” in the *Administering Avaya Aura® Experience Portal* guide.

Procedure

1. Log in to the primary Experience Portal Manager CLI.
2. Run the following command to switch to the root user:

   su - root
3. Run the following command:

   cd /opt/Avaya/ExperiencePortal/Support/Security-Tools
4. Run the following command to create a read-only (report) user account for the Experience Portal local Postgres database:

   ./SetDbPassword.sh add_report_r -u <user name>

   Where, <*user name*> is a user name for the new read-only user account.
5. At the `Please enter the password` prompt, type a password for the read-only (report) user account and press `Enter`.
6. After the user account is successfully created, the system shows the following message indicating the list of services to be restarted:

   ```
   The following services will be restarted automatically:
   - postgresql
   ```
7. Press `Y` to restart the service.

Enabling SSL connection between Experience Portal Postgres database and Usage Metering

About this task

Perform this procedure if you want to enable SSL connection between any of the following:

- An Experience Portal local Postgres database and Usage Metering.
- An Experience Portal external Postgres database and Usage Metering.

Procedure

1. Connect to the Postgres server by using PuTTY.
2. Run the following command and note down the output of the command:

   hostname

3. Do the following to make the Postgres server a root certificate authority:
   a. Replace **<root.yourdomain.com>** in the following command with the output of the **hostname** command and run the following command to generate a root certificate signing request (CSR) and a public/private key file (`root.key`):

   ```
   openssl req -new -nodes -text -out root.csr \
     -keyout root.key -subj "/CN=<root.yourdomain.com>"
   ```

   b. Run the following command to remove read, write, and execute permissions from the `root.key` file for all users except the file owner:

   chmod og-rwx root.key

   c. Run the following command to generate a CA-signed root certificate by using the `root.key` and `openssl.cnf` files:

   ```
   openssl x509 -req -in root.csr -text -days 3650 \
     -extfile /etc/ssl/openssl.cnf -extensions v3_ca \
     -signkey root.key -out root.crt
   ```

   The preceding command generates the `root.crt` file, which is a CA-signed root certificate file.

   d. If the command in the preceding step displays an error mentioning that the `openssl.cnf` file is not found, run the following command to find the file on the server:

   find / -name "<filename>"

   Replace the file location in the command in the preceding step with the correct file location and run the command.

4. Do the following to generate a server certificate that is signed by this root CA:
   a. Replace **<dbhost.yourdomain.com>** in the following command with the output of the **hostname** command and run the following command to generate a server certificate CSR and a public/private key file (`server.key`) for this CSR:

   ```
   openssl req -new -nodes -text -out server.csr \
     -keyout server.key -subj "/CN=<dbhost.yourdomain.com>"
   ```

   b. Run the following command to remove read, write, and execute permissions from the `server.key` file for all users except the file owner:

   chmod og-rwx server.key

c. Run the following command to generate a server certificate that is signed by this root CA:

```
openssl x509 -req -in server.csr -text -days 365 \
  -CA root.crt -CAkey root.key -CAcreateserial \
  -out server.crt
```

You can specify the number of days for certificate validity in the preceding command based on your corporate policy.

The preceding command generates the `server.crt` file that is signed by this root CA.

5. Copy the `server.crt` and `server.key` files to the `var/lib/pgsql/data/` folder on the Postgres server.
6. Run the following commands to allow the Postgres server access to the `server.crt` and `server.key` files:

`chown postgres:postgres server.crt`

`chown postgres:postgres server.key`

7. Do the following to enable SSL connection:
   a. Run the following command to edit the `postgresql.conf` file:

`vi postgresql.conf`

   b. Set the following parameters in the `postgresql.conf` file:

- ssl = `on`
- ssl_crt_file = `'server.crt'`
- ssl_key_file = `'server.key'`

   c. Save the `postgresql.conf` file.
   d. To apply the changes, restart the Postgres service by running the following command:

`sudo service postgresql restart`

8. Copy the `server.crt` file to the Usage Metering Collector server.
9. Install the `server.crt` file in the Usage Metering Collector.

   For more information, see Installing an outbound certificate on page 80.

Next steps

After you perform this procedure, you must select the **SSL** check box when adding Experience Portal Manager to your Avaya OneCloud™ Subscription system to enable the SSL connection.

Prerequisites and process for adding Avaya Aura® Messaging

The following table provides step-by-step information about the prerequisites and process for adding Avaya Aura® Messaging that is entitled by the subscription license to your Avaya OneCloud™ Subscription system:

Step	Task	Related topic
Perform the following prerequisites before adding Avaya Aura® Messaging to the Avaya OneCloud™ Subscription system:		
1	Ensure that the on-premise installed Avaya Aura® Messaging is of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version. If the on-premise Avaya Aura® Messaging is of an earlier version than the minimum supported version, upgrade it to at least the minimum supported version.	Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30
2	Add the Usage Metering Collector as a trusted server in Avaya Aura® Messaging.	Add Usage Metering Collector as a trusted server in Avaya Aura Messaging on page 100
3	Enable LDAP SSL port in Avaya Aura® Messaging.	Enabling LDAP SSL port in Avaya Aura Messaging on page 101
4	Identify the root CA certificate installed in Avaya Aura® Messaging and install it in the Usage Metering Collector.	Identifying the root CA certificate installed in Avaya Aura Messaging and installing it in Usage Metering Collector on page 101
Add Avaya Aura® Messaging:		
5	Add Avaya Aura® Messaging to the Avaya OneCloud™ Subscription system.	• Adding an application to the Avaya OneCloud Subscription system on page 111 • Create Application page field descriptions on page 112

Add Usage Metering Collector as a trusted server in Avaya Aura® Messaging

Use the Avaya Aura® Messaging - System Management Interface to add the Usage Metering Collector as a trusted server in Avaya Aura® Messaging.

Ensure the following when adding the Usage Metering Collector as a trusted server:

- In the **Trusted Server Name** field, type a unique name for the Usage Metering Collector.
- In the **Machine Name/IP Address** field, type the IP address of the Usage Metering Collector.
- In the **LDAP Access Allowed** field, click **yes**.
- In the **Password** and **Confirm Password** fields, type a password to access the Avaya Aura® Messaging server.
- In the **Service Name** field, type a descriptive name that indicates the use of this trusted server. For example, `collector LDAP`.
- In the **LDAP Connection Security** field, click **Must use SSL**.

For more information about adding a trusted server in Avaya Aura® Messaging, see “Adding a trusted server” in the *Administering Avaya Aura® Messaging* guide.

Note:

You must use this trusted server name and password when adding Avaya Aura® Messaging to your Avaya OneCloud™ Subscription system in the Usage Metering Collector. Usage Metering Collector uses these credentials to connect to Avaya Aura® Messaging.

Do not use these credentials to perform any other operations in Avaya Aura® Messaging.

Enabling LDAP SSL port in Avaya Aura® Messaging

Procedure

1. Log on to the Avaya Aura® Messaging - System Management Interface.
2. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Administration**.
3. In the **SYSTEM TCP/IP PORTS** area, set the **LDAP SSL Port** field to **Enabled** and specify the LDAP SSL port number.

   Note:

   You must use this LDAP SSL port number when adding Avaya Aura® Messaging to your Avaya OneCloud™ Subscription system.

   The default port is 636.

Identifying the root CA certificate installed in Avaya Aura® Messaging and installing it in Usage Metering Collector

About this task

For any recent updates on certificate management in Avaya Aura® Messaging, see the *Administering Avaya Aura® Messaging* guide.

Procedure

1. Log on to the Avaya Aura® Messaging - System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Do the following to view the CA and Common Name (CN) of the Avaya Aura® Messaging server:
   a. In the left navigation pane, click **Security** > **Server/Application Certificates**.

      The system displays the list of installed server and application certificates.

   b. Identify the Avaya Aura® Messaging server identity certificate installed in the Messaging repository.

      The Messaging repository is represented by the letter **M** under **Installed In**.

   c. Note down the CA, displayed under **Issued By**, that signed this identity certificate.

   d. Note down the Avaya Aura® Messaging server CN displayed under **Issued To**.

4. Do the following to copy the root certificate of the CA you identified in Step 3:
   a. In the left navigation pane, click **Security** > **Trusted Certificates**.

      The system displays the list of installed trusted certificates.
   b. Select the root certificate of the CA that you identified in Step 3.

      Ensure that you select the root certificate that is installed in the Messaging repository of the Avaya Aura® Messaging server.
   c. Click **Display** to view the certificate.
   d. Copy the certificate text from `BEGIN CERTIFICATE` through `END CERTIFICATE`.
5. Install the copied certificate in the Usage Metering Collector by using the **from text** option.

   For more information, see Installing an outbound certificate on page 80.
6. Ensure that the DNS server has an Avaya Aura® Messaging server FQDN to IP address mapping entry.

   If the DNS server does not contain the mapping, add a mapping entry in the following format to the `/etc/hosts` file located on the Usage Metering Collector server:

   `<IP address of Avaya Aura® Messaging server> <FQDN of the Avaya Aura® Messaging server>`

   For example, `10.100.10.100 aam.pu.ava.com`

   Ensure that the Avaya Aura® Messaging server FQDN mentioned in the DNS server or `/etc/hosts` file matches the CN present in the Avaya Aura® Messaging server identity certificate that you noted in Step 3.

Prerequisites and process for adding System Manager

Usage Metering collects usage data from the System Manager Postgres database.

The following table provides step-by-step information about the prerequisites and process for adding System Manager that is entitled by the subscription license to your Avaya OneCloud™ Subscription system:

Step	Task	Related topic
Perform the following prerequisites before adding System Manager to the Avaya OneCloud™ Subscription system:		
1	Ensure that the on-premise installed System Manager is of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version. If the on-premise System Manager is of an earlier version than the minimum supported version, upgrade it to at least the minimum supported version.	Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30

Table continues…

Step	Task	Related topic
2	Install the System Manager CA certificate in the Usage Metering Collector.	Installing the System Manager CA certificate in Usage Metering Collector on page 103
3	Create a Postgres user and enable SSL connection between Usage Metering and System Manager Postgres database.	Creating a Postgres user and enabling SSL connection between Usage Metering and System Manager Postgres database on page 103
Add System Manager:		
4	Add System Manager to the Avaya OneCloud™ Subscription system.	• Adding an application to the Avaya OneCloud Subscription system on page 111 • Create Application page field descriptions on page 112

Installing the System Manager CA certificate in Usage Metering Collector

About this task

Skip this procedure if you have already installed the root certificate of this System Manager in Usage Metering Collector when performing the prerequisites for adding the System Manager-provided WebLM to your Avaya OneCloud™ Subscription system.

For more information, see Prerequisites for adding a System Manager-provided WebLM to an Avaya OneCloud Subscription system on page 87.

Procedure

1. Export the System Manager-signed CA certificate from System Manager.

   For more information, see Exporting the System Manager-signed root CA certificate from System Manager on page 88.

2. Install the System Manager-signed CA certificate in the Usage Metering Collector.

   For more information, see Installing an outbound certificate on page 80.

Creating a Postgres user and enabling SSL connection between Usage Metering and System Manager Postgres database

About this task

Usage Metering uses SSL connection to retrieve usage data from the System Manager Postgres database. You can use the `smgrmeterchanges.sh` script to enable the SSL connection.

The `smgrmeterchanges.sh` script does the following:

- Opens port 5432. Usage Metering uses this port to connect to the System Manager Postgres database.
- Enables SSL connection between Usage Metering and the System Manager Postgres database.

Note:

You must create a new read-only user for the System Manager Postgres database. You must use the access credentials of this user when adding System Manager to the Avaya OneCloud™ Subscription system in the Usage Metering Collector. Usage Metering Collector uses these access credentials to connect to the System Manager Postgres database.

Do not use these access credentials to perform any other operations in System Manager.

Procedure

1. On the server where the Usage Metering Collector is installed, navigate to the `/opt/Avaya/usage-metering/bin/` location and download the following file:

   `smgrmeterchanges.sh`

2. Copy the `smgrmeterchanges.sh` file to any directory on the System Manager server.
3. Run the following command as a root user at the System Manager CLI command prompt:

   `sh smgrmeterchanges.sh <collector_IPAddress> <postgres_user> <postgres_password>`

   Where:

   - <*collector_IPAddress*> is the IP address of the Usage Metering Collector server.
   - <*postgres_user*> is a user name for the new read-only user for the Postgres database.
   - <*postgres_password*> is a password for the new read-only user for the Postgres database.

Prerequisites and process for adding Avaya Callback Assist Application Server

Depending on the deployment model of Avaya Callback Assist, your on-premise Avaya Callback Assist can include more than one Avaya Callback Assist Application Servers.

For example, if Avaya Callback Assist is deployed for High Availability, there can be more than one Avaya Callback Assist Application Servers installed.

In such scenario, you can add more than one Avaya Callback Assist Application Servers to the Avaya OneCloud™ Subscription system.

However, ensure that you add only one Avaya Callback Assist Application Server as the main server by selecting the **CORE** option in the **Deployment Type** field. You can add the remaining Avaya Callback Assist Application Servers by selecting the **ADDITIONAL** option in the **Deployment Type** field. The **Deployment Type** field is available on the Create Application page for adding an application to the Avaya OneCloud™ Subscription system.

The following table provides step-by-step information about the prerequisites and process for adding Avaya Callback Assist Application Server that is entitled by the subscription license to your Avaya OneCloud™ Subscription system:

Step	Task	Related topic
Perform the following prerequisites before adding Avaya Callback Assist Application Server to the Avaya OneCloud™ Subscription system:		
1	Ensure that the on-premise installed Avaya Callback Assist is of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version. If the on-premise Avaya Callback Assist is of an earlier version than the minimum supported version, upgrade it to at least the minimum supported version.	Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30
2	Install the following certificates in Avaya Callback Assist: • Root CA-signed certificate that is installed on the WebLM server for authentication. This is the WebLM server on which the subscription license containing entitlement for Avaya Callback Assist is installed. • Root CA-signed certificate that is installed on Experience Portal Manager (EPM) for authentication. This is the EPM that is integrated with Avaya Callback Assist.	Refer to the respective product documentation.
3	If Avaya Aura® Orchestration Designer that is integrated with Avaya Callback Assist is entitled by the subscription license, ensure that you add Avaya Aura® Orchestration Designer to the Avaya OneCloud™ Subscription system.	• Adding an application to the Avaya OneCloud Subscription system on page 111 • Create Application page field descriptions on page 112
4	If you want to enable SSL connection between Usage Metering and Avaya Callback Assist, perform the prerequisites for enabling SSL connection.	Enabling SSL connection between Usage Metering and Avaya Callback Assist on page 105
Add the Avaya Callback Assist Application Server:		
5	Add the Avaya Callback Assist Application Server to the Avaya OneCloud™ Subscription system.	• Adding an application to the Avaya OneCloud Subscription system on page 111 • Create Application page field descriptions on page 112

Enabling SSL connection between Usage Metering and Avaya Callback Assist

About this task

Perform this procedure only if you want to enable SSL connection between Usage Metering and Avaya Callback Assist.

You can skip Step 2 if you have already installed the root certificate of this CA in the Usage Metering Collector when performing the prerequisites for adding other data source application or System Manager-provided WebLM to any Avaya OneCloud™ Subscription system configured on the same Usage Metering Collector.

Procedure

1. Configure the Avaya Callback Assist server to communicate on SSL.

   For more information, see the *Installing and configuring Avaya Callback Assist* and *Avaya Callback Assist Security and TLS Configuration* guides.

   Because implementation of SSL/TLS is redesigned from Avaya Callback Assist Release 5.0, refer to Avaya Callback Assist documentation for the Avaya Callback Assist version that you are using.

2. Do the following only if you want to enable SSL connection between Avaya Callback Assist Release 5.0 or later and Usage Metering.

   a. Do one of the following:

      - If System Manager is the CA for Avaya Callback Assist, export the System Manager-signed root certificate from System Manager.

        For more information, see Exporting the System Manager-signed root CA certificate from System Manager on page 88.

      - If Avaya Callback Assist uses a third-party CA, retrieve the root certificate of the third-party CA from the third-party CA.

   b. Install this root certificate in the Usage Metering Collector.

      For more information, see Installing an outbound certificate on page 80

Next steps

After you perform this procedure, you must select the **SSL** check box when adding Avaya Callback Assist Application Server to your Avaya OneCloud™ Subscription system to enable the SSL connection.

Prerequisites and process for adding Avaya Call Management System

Usage Metering Collector collects usage data from the Avaya Call Management System (CMS) database.

The following table provides step-by-step information about the prerequisites and process for adding CMS that is entitled by the subscription license to your Avaya OneCloud™ Subscription system:

Step	Task	Related topic
Perform the following prerequisites before adding CMS to the Avaya OneCloud™ Subscription system:		
1	Ensure that the on-premise installed CMS is of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version. If the on-premise CMS is of an earlier version than the minimum supported version, upgrade it to at least the minimum supported version.	Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30

Table continues…

Step	Task	Related topic
2	Create a new user account in CMS with secure access permission to the CMS database.	Creating a new user account in CMS with secure access permission to the CMS database on page 107
3	If you want to enable SSL connection between the CMS database and Usage Metering, perform the prerequisite for enabling SSL connection.	Enabling SSL secure connection to the CMS database on page 108
Add CMS:		
4	Add CMS to the Avaya OneCloud™ Subscription system.	• Adding an application to the Avaya OneCloud Subscription system on page 111 • Create Application page field descriptions on page 112

Creating a new user account in CMS with secure access permission to the CMS database

About this task

The access credentials that you use to add CMS to your Avaya OneCloud™ Subscription system must have secure access permission to the CMS database.

You must create a new user in CMS and grant the user secure access permission to the CMS database.

Note:

You must use the access credentials of this user when adding CMS to your Avaya OneCloud™ Subscription system in the Usage Metering Collector. Usage Metering Collector uses these access credentials to connect to the CMS database.

Do not use these access credentials to perform any other operations in CMS.

Procedure

1. Log in to Avaya Call Management System CLI by using root credentials.
2. Run the following command to create a new Linux user in CMS:

   useradd <user_name>

   Where, <*user_name*> is a user name for the new user.
3. Run the following command and set a password for the new user:

   passwd <user_name>

   Where, <*user_name*> is the user name of the new user.
4. Run the following DB-Access utility command for the CMS database:

   dbaccess cms
5. Press **Enter** and select the **Query-language** option.
6. Press **Enter** and select the **New** option.

7. Do the following to grant the user secure access permission to the CMS database:
   a. Run the following command:

      `grant dba to <user_name>`

      Where, <*user_name*> is the user name of the new user.
   b. Press **Esc**.
   c. Press **Enter** and select the **Run** option.

      The system shows the `Permission granted` message.
8. Press the Left Arrow key or Right Arrow key to quit the DB-Access utility.

Enabling SSL secure connection to the CMS database

About this task

Perform this procedure if you want to enable SSL secure connection to the CMS database.

Note:

CMS supports secure connection to the CMS database from Release 19.1 and later.

You can skip installing the root certificate of System Manager or third-party CA if you have already installed this root certificate in the Usage Metering Collector when performing the prerequisites for adding other data source application or System Manager-provided WebLM to any Avaya OneCloud™ Subscription system configured on the same Usage Metering Collector.

Procedure

1. In Avaya Call Management System, enable Informix network encryption by using either a CMS self-signed certificate or a CA-signed certificate.

   For more information, see “Enabling Informix network encryption” in the *Using ODBC and JDBC with Avaya Call Management System* guide.
2. Do one of the following:
   - If System Manager is the CA for Avaya Call Management System, export the System Manager-signed root certificate from System Manager.

     For more information, see Exporting the System Manager-signed root CA certificate from System Manager on page 88.
   - If Avaya Call Management System uses a third-party CA, retrieve the root certificate of the third-party CA from the third-party CA.
   - If Avaya Call Management System uses a self-signed certificate, retrieve the self-signed certificate from Avaya Call Management System.

     The self-signed certificate file `<HOSTNAME>_cms_net_encrypt.pem` is located in the `/opt/informix/ssl` directory on the CMS server.

     For more information, see the *Using ODBC and JDBC with Avaya Call Management System* guide.

3. Install this certificate in the Usage Metering Collector.

   For more information, see Installing an outbound certificate on page 80.

Next steps

After you perform this prerequisite, you must select the **SSL** check box when adding CMS to your Avaya OneCloud™ Subscription system to enable the SSL connection.

Prerequisites and process for adding Avaya IX™ Messaging

The following table provides step-by-step information about the prerequisites and process for adding Avaya IX™ Messaging (formerly known as Avaya Officelinx) that is entitled by the subscription license to your Avaya OneCloud™ Subscription system:

Step	Task	Related topic
Perform the following prerequisites before adding Avaya IX™ Messaging to the Avaya OneCloud™ Subscription system:		
1	Ensure that the on-premise installed Avaya IX™ Messaging is of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version. If the on-premise Avaya IX™ Messaging is of an earlier version than the minimum supported version, upgrade it to at least the minimum supported version.	Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30
2	Create a new administrative user account in Avaya IX™ Messaging.	Create a new administrative user account in Avaya IX Messaging on page 109
3	Install the root certificate that is used by Avaya IX™ Messaging for authentication in the Usage Metering Collector.	Installing the root certificate used by Avaya IX Messaging for authentication in Usage Metering Collector on page 110
Add Avaya IX™ Messaging:		
4	Add Avaya IX™ Messaging to the Avaya OneCloud™ Subscription system.	• Adding an application to the Avaya OneCloud Subscription system on page 111 • Create Application page field descriptions on page 112

Create a new administrative user account in Avaya IX™ Messaging

Do the following by using the Avaya IX™ Messaging web interface:

- Create a new administrative user in Avaya IX™ Messaging.

  When creating the administrative user, ensure the following:

  - In the **Related Company** field, click **All**.

- Select the following check boxes to grant the user permission to perform these administrative tasks:
  - **Edit System Configuration**
  - **Edit PBX**
  - **Add Edit Companies, Feature Groups, Remote Site, Routing Tables, Voice Menus, Customize TUI**
  - **Add Range of Mailboxes**
  - **Log Management**
  - **Backup Management**
  - **Report Management**

For information about creating an administrative user in Avaya IX™ Messaging, see “Edit/Add User” in the *Avaya IX™ Messaging Server Configuration Guide*.

Note:

You must use the access credentials of this administrative user when adding Avaya IX™ Messaging to your Avaya OneCloud™ Subscription system in the Usage Metering Collector. Usage Metering Collector uses these access credentials to connect to Avaya IX™ Messaging.

Do not use these access credentials to perform any other operations in Avaya IX™ Messaging.

Installing the root certificate used by Avaya IX™ Messaging for authentication in Usage Metering Collector

About this task

You can skip Steps 1 and 2 if you have already installed the root certificate of this CA in the Usage Metering Collector when performing the prerequisites for adding other data source application or System Manager-provided WebLM to any Avaya OneCloud™ Subscription system configured on the same Usage Metering Collector.

Procedure

1. Do one of the following:
   - If System Manager is the CA for Avaya IX™ Messaging, export the System Manager-signed root certificate from System Manager.

     For more information, see Exporting the System Manager-signed root CA certificate from System Manager on page 88.
   - If Avaya IX™ Messaging uses a third-party CA, retrieve the root certificate of the third-party CA from the third-party CA.
2. Install this root certificate in the Usage Metering Collector.

   For more information, see Installing an outbound certificate on page 80.

3. Do the following to view the Avaya IX™ Messaging server Common Name (CN) displayed in the Avaya IX™ Messaging server identity certificate:
   a. On a web browser, type the URL of Avaya IX™ Messaging.
   b. On the address bar, click the Lock icon.
   c. Click **Certificate**.
   d. In the Certificate dialog box, on the **General** tab, note down the Avaya IX™ Messaging server CN displayed in the **Issued to** field.
4. Ensure that the DNS server has an Avaya IX™ Messaging server FQDN to IP address mapping entry.

   If the DNS server does not contain the mapping, add a mapping entry in the following format to the `/etc/hosts` file located on the Usage Metering Collector server:

   `<IP address of Avaya IX Messaging™ server> <FQDN of the Avaya IX Messaging™ server>`

   For example, `10.100.10.100 am.pu.ava.com`

   Ensure that the Avaya IX™ Messaging server FQDN mentioned in the DNS server or `/etc/hosts` file matches the CN present in the Avaya IX™ Messaging server identity certificate that you noted in Step 3.

Adding an application to the Avaya OneCloud™ Subscription system

About this task

Use this procedure to add the on-premise Avaya UC or CC application that is entitled by the subscription license to your Avaya OneCloud™ Subscription system.

The applications that you can add to the Avaya OneCloud™ Subscription system depend on the service bundle that you have ordered for the Avaya OneCloud™ Subscription system.

Note:

The on-premise Avaya UC or CC application that is entitled by a subscription license can run by using the subscription license only after you add the application to the Avaya OneCloud™ Subscription system.

Before you begin

Before you add an application or a data source application to your Avaya OneCloud™ Subscription system, ensure that you read the instructions mentioned in the checklist for adding applications and perform the prerequisites for adding applications and data source applications.

For more information, see Checklist for adding applications to an Avaya OneCloud Subscription system on page 92.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.

3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.

4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system in which you want to add an application.

5. On the **APPLICATIONS** tab, click **Add Application**.

   Usage Metering displays the **Create Application** dialog box.

6. In the **Create Application** dialog box, configure the application information.

   For more information, see Create Application page field descriptions on page 112.

7. To configure a geo-redundant application, enable **With Secondary**, and configure the information of the secondary application that resides in the secondary data center.

8. Click **SUBMIT**.

Create Application page field descriptions

Note:

Before you add an application or a data source application to your Avaya OneCloud™ Subscription system, ensure that you read the instructions mentioned in the checklist for adding applications and perform the prerequisites for adding applications and data source applications.

For example, prerequisites for adding certain data source application can involve the following:

- Installing certificates.
- Creating a new user account in the data source application. You need to use the access credentials of the new user account when adding the data source application to your Avaya OneCloud™ Subscription system. Usage Metering Collector uses these credentials to connect to the data source application for collecting usage data.

For more information, see Checklist for adding applications to an Avaya OneCloud Subscription system on page 92.

Common fields on the Create Application page

Field name	Description
Application Type	Click the application that you want to add to the Avaya OneCloud™ Subscription system. The applications that are displayed in the **Application Type** field depend on the service bundle that you have ordered for this Avaya OneCloud™ Subscription system.
Application Description	Type a description for the application.

Table continues…

Field name	Description
Primary IP	Type the IP address of the primary application. **Note:** If you are adding a Session Manager, type the Management Interface IP address of the Session Manager. If you are adding applications of the same application type to one or more Avaya OneCloud™ Subscription systems that are configured on the same Usage Metering Collector, ensure that the IP address that you specify is different for each such application. Otherwise, Usage Metering Collector shows an error message. An example of applications of the same application type is two or more CMS. Usage Metering Collector performs this verification on the IP addresses that you specify in both **Primary IP** and **Secondary IP** fields when you are adding these applications. However, if you want to share an application, for example, a CMS, between two or more Avaya OneCloud™ Subscription systems, see Application sharing between two or more Avaya OneCloud Subscription systems on page 23.
Version	Click the version number of the application. Ensure that the application is of either the minimum version that is supported by Avaya OneCloud™ Subscription or of a later version. For more information, see Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30.
Deployment Type	Click the deployment type of the application.
FL/Sold-To	Type the Functional Location number (FL) or Sold To number (ST) of your location.
SAL Gateway SEID	Type the Solution Element ID (SEID) of the SAL gateway.

If you are adding a data source application to your Avaya OneCloud™ Subscription system, Usage Metering displays additional data source application-specific fields.

For information about the data source application-specific fields, refer to the data source application-specific sections in this topic.

Application Enablement Services-specific fields

The following additional fields are available when you are adding Application Enablement Services to your Avaya OneCloud™ Subscription system.

Ensure that you have performed the prerequisites before adding Application Enablement Services to your Avaya OneCloud™ Subscription system.

For more information, see Prerequisites and process for adding Application Enablement Services on page 94.

Field name	Description
Hostname	Type the FQDN of the Application Enablement Services server.
Port	Type the SSH port number to access Application Enablement Services. If you do not specify a port number, Usage Metering uses the default SSH port number 22 to access Application Enablement Services.
Username	Type the user name of the user account that you created in the `susers` Linux group in Application Enablement Services. For more information, see Create a new user account in Application Enablement Services on page 95.
Password	Type the password of the user account.
TEST	Click to verify if Usage Metering successfully connects to the Application Enablement Services server.

Experience Portal Manager-specific fields

The following additional fields are available when you are adding Avaya Aura® Experience Portal - Experience Portal Manager (EPM) (also known as Voice Portal EPM) to the Avaya OneCloud™ Subscription system.

These fields are not available when you are adding an auxiliary EPM to your Avaya OneCloud™ Subscription system.

Ensure that you have performed the prerequisites before adding EPM to your Avaya OneCloud™ Subscription system.

For more information, see Prerequisites and process for adding Experience Portal Manager on page 95.

Field name	Description
Database IP	Type the IP address of the Experience Portal database server that Usage Metering must connect to for collecting usage data.
Port	Type the port number to access the Experience Portal database. If you do not specify a port number, Usage Metering uses the default port number 1433 to access the Experience Portal database.
Username	Do one of the following: • If Experience Portal uses the local Postgres database, type the user name of the read-only (report) user that you created for the local Postgres database. For more information, see Creating a read-only user account for Experience Portal local Postgres database on page 97. • If Experience Portal uses an external database, that is, an external Postgres or Microsoft SQL database, type the user name of the read-only user that you created for the external database. For more information, see Create a read-only user account for the Experience Portal database on page 96.

Table continues…

Field name	Description
Password	Type the password to access the Experience Portal database.
Socket Timeout	Type the time, in seconds, till which Usage Metering must attempt to connect to the Experience Portal database. If you do not specify a time-out period, Usage Metering uses the default time-out period, which is 120 seconds.
Database Name	Type the name of the Experience Portal database. If Experience Portal uses the local Postgres database, type `VoicePortal`.
SSL	Select the **SSL** check box if you want to use SSL secure connection to connect to the Experience Portal Postgres database. Ensure that you have performed the prerequisite for enabling SSL connection to the Experience Portal Postgres database. For more information, see Enabling SSL connection between Experience Portal Postgres database and Usage Metering on page 97. Currently, Avaya OneCloud™ Subscription supports SSL connection only for the Experience Portal local Postgres and external Postgres databases. Do not select this check box if Experience Portal uses a Microsoft SQL database. **Note:** If you enable SSL for the primary EPM, Avaya recommends you to enable SSL for the secondary EPM.
TEST	Click to verify if Usage Metering successfully connects to the Experience Portal database.

Avaya Aura® Messaging-specific fields

The following additional fields are available when you are adding Avaya Aura® Messaging to your Avaya OneCloud™ Subscription system.

Ensure that you have performed the prerequisites before adding Avaya Aura® Messaging to your Avaya OneCloud™ Subscription system.

For more information, see Prerequisites and process for adding Avaya Aura Messaging on page 99.

Field name	Description
Hostname	Type the FQDN of the Avaya Aura® Messaging server. Ensure that the FQDN matches the following: • Avaya Aura® Messaging server CN present in the identity certificate of the Avaya Aura® Messaging server. • Avaya Aura® Messaging server FQDN to IP address mapping entry that is present in the DNS server or `/etc/hosts` file. For more information, see Identifying the root CA certificate installed in Avaya Aura Messaging and installing it in Usage Metering Collector on page 101.
Port	Type the LDAP SSL port number that you specified in Avaya Aura® Messaging. For more information, see Enabling LDAP SSL port in Avaya Aura Messaging on page 101 and Add Usage Metering Collector as a trusted server in Avaya Aura Messaging on page 100. If you do not specify a port number, Usage Metering uses the default port number 636 to access Avaya Aura® Messaging.
Username	Type the trusted server name that you specified for the Usage Metering Collector when adding it as a trusted server in Avaya Aura® Messaging. For more information, see Add Usage Metering Collector as a trusted server in Avaya Aura Messaging on page 100.
Password	Type the password that you specified when adding the Usage Metering Collector as a trusted server in Avaya Aura® Messaging.
TEST	Click to verify if Usage Metering successfully connects to the Avaya Aura® Messaging server.

Avaya Aura® System Manager-specific fields

The following additional fields are available when you are adding System Manager to your Avaya OneCloud™ Subscription system.

Ensure that you have performed the prerequisites before adding System Manager to your Avaya OneCloud™ Subscription system.

For more information, see Prerequisites and process for adding System Manager on page 102.

Field name	Description
Port	Type `5432`. Ensure that you have performed the prerequisite that opens port 5432 and enables SSL connection. Usage Metering Collector uses port 5432 to access the System Manager Postgres Server. For more information, see Creating a Postgres user and enabling SSL connection between Usage Metering and System Manager Postgres database on page 103.
User name	Type the user name of the read-only user that you created for the Postgres database. For more information, see Creating a Postgres user and enabling SSL connection between Usage Metering and System Manager Postgres database on page 103.
Password	Type the password of the read-only user that you created for the Postgres database.
Database Name	Type `avmgmt`, which is the name of the System Manager Postgres database.
Socket Timeout	Type the time, in seconds, till which Usage Metering must attempt to connect to the Postgres database. If you do not specify a time-out period, Usage Metering uses the default time-out period, which is 120 seconds.
TEST	Click to verify if Usage Metering successfully connects to the System Manager Postgres database.

Avaya Callback Assist Application Server-specific fields

The following additional fields are available when you are adding Avaya Callback Assist Application Server to your Avaya OneCloud™ Subscription system.

Ensure that you have performed the prerequisites before adding Avaya Callback Assist Application Server to your Avaya OneCloud™ Subscription system.

For more information, see Prerequisites and process for adding Avaya Callback Assist Application Server on page 104.

Field name	Description
Hostname	Type the FQDN or IP address of the Avaya Callback Assist Application Server.
Port	Type the port number to access Kafka broker in Avaya Callback Assist. If you do not specify a port number, Usage Metering uses the following default ports: • Port 9092 to connect to Kafka broker by using unsecure connection. • Port 9093 to connect to Kafka broker by using SSL.

Table continues…

Field name	Description
User name	Type the user name of Kafka broker that is configured in Avaya Callback Assist. If you do not specify the user name, Usage Metering uses the default user name that is displayed in this field. The **User name** field is unavailable if you are adding Avaya Callback Assist version 4.7.x to your Avaya OneCloud™ Subscription system.
Password	Type the password of Kafka broker that is configured in Avaya Callback Assist. If you do not specify the password, Usage Metering uses the default password that is displayed in an encrypted format in this field. The **Password** field is unavailable if you are adding Avaya Callback Assist version 4.7.x to your Avaya OneCloud™ Subscription system.
Kafka Topic Name	Retain the default value, that is, `callback-requests`, in this field. This is the name of the Avaya Callback Assist Kafka topic from which Usage Metering collects usage data.
SSL	Select the **SSL** check box if you want to use SSL secure connection to connect to Avaya Callback Assist Kafka broker. Ensure that you have performed the prerequisites for enabling SSL connection between Usage Metering and Avaya Callback Assist. For more information, see Enabling SSL connection between Usage Metering and Avaya Callback Assist on page 105. **Note:** If you enable SSL for the primary Avaya Callback Assist Application Server, Avaya recommends you to enable SSL for the secondary Avaya Callback Assist Application Server.
TEST	Click to verify if Usage Metering successfully connects to Avaya Callback Assist Kafka broker.

Avaya Call Management System-specific fields

The following additional fields are available when you are adding Avaya Call Management System to your Avaya OneCloud™ Subscription system.

Ensure that you have performed the prerequisites before adding Avaya Call Management System (CMS) to your Avaya OneCloud™ Subscription system.

For more information, see Prerequisites and process for adding Avaya Call Management System on page 106.

Field name	Description
Port	Type the port number to access Avaya Call Management System. If you do not specify a port number, Usage Metering uses the default port number 50001 to access Avaya Call Management System.
User name	Type the user name, with secure access permissions to the CMS database, that you created in CMS. For more information, see Creating a new user account in CMS with secure access permission to the CMS database on page 107.
Password	Type the password to access the CMS database.
Socket Timeout	Type the time, in seconds, till which Usage Metering must attempt to connect to the CMS database. If you do not specify a time-out period, Usage Metering uses the default time-out period, which is 120 seconds.
SSL	Select the **SSL** check box if you want to use SSL secure connection to connect to the CMS database. Ensure that you have performed the prerequisite for enabling SSL connection to the CMS database. For more information, see Enabling SSL secure connection to the CMS database on page 108. **Note:** If you enable SSL for the primary CMS, Avaya recommends you to enable SSL for the secondary CMS.
TEST	Click to verify if Usage Metering successfully connects to Avaya Call Management System.

Avaya IX™ Messaging-specific fields

The following additional fields are available when you are adding Avaya IX™ Messaging (Office Linx) to your Avaya OneCloud™ Subscription system.

Ensure that you have performed the prerequisites before adding Avaya IX™ Messaging to your Avaya OneCloud™ Subscription system.

For more information, see Prerequisites and process for adding Avaya IX Messaging on page 109.

Field name	Description
Hostname	Type the FQDN of the Avaya IX™ Messaging server. Ensure that the FQDN matches the following: • Avaya IX™ Messaging server CN present in identity certificate of the Avaya IX™ Messaging server. • Avaya IX™ Messaging server FQDN to IP address mapping entry that is present in the DNS server or `/etc/hosts` file. For more information, see Installing the root certificate used by Avaya IX Messaging for authentication in Usage Metering Collector on page 110.
Username	Type the user name of the administrative user that you created in Avaya IX™ Messaging. For more information, see Create a new administrative user account in Avaya IX Messaging on page 109.
Password	Type the password of the administrative user that you created in Avaya IX™ Messaging.
Port	Type the port number to access Avaya IX™ Messaging. If you do not specify a port number, Usage Metering uses the default port number 443 to access Avaya IX™ Messaging.
Auth Type	Click **OL_JWT**. Usage Metering uses JSON Web Token to authenticate with and connect to Avaya IX™ Messaging.
TEST	Click to verify if Usage Metering successfully connects to Avaya IX™ Messaging.

Related links

Adding an application to the Avaya OneCloud Subscription system on page 111

Prerequisites for sharing Experience Portal between multiple Avaya OneCloud™ Subscription systems

You can share Experience Portal between multiple Avaya OneCloud™ Subscription systems that are configured on the same Usage Metering Collector.

However, before sharing an Experience Portal between multiple Avaya OneCloud™ Subscription systems, you must use the Organization feature in Experience Portal to create a separate organization for each Avaya OneCloud™ Subscription system in which you want to share the Experience Portal.

When creating the organization in Experience Portal, you must specify the subscription ID of your Avaya OneCloud™ Subscription system as the organization name. You must then share the Experience Portal only between these Avaya OneCloud™ Subscription systems in the Usage Metering Collector.

Configuring a separate organization for each Avaya OneCloud™ Subscription system that shares the Experience Portal allows Usage Metering to collect and segment usage data for each of these Avaya OneCloud™ Subscription systems.

Note:

You need not perform these prerequisites if you are using Experience Portal as a dedicated (non-shared) application in your Avaya OneCloud™ Subscription system.

Do the following in Experience Portal Manager (EPM):

1. Enable organizational level access in Experience Portal.
2. Create an organization for each Avaya OneCloud™ Subscription system in which you want to share this Experience Portal.

   Ensure that you specify the subscription ID of your Avaya OneCloud™ Subscription system as the organization name when creating the organization.

   For more information about enabling organization level access and creating an organization in EPM, see the *Administering Avaya Aura® Experience Portal* guide.

Related links

Sharing an application between multiple Avaya OneCloud Subscription systems on page 121

Sharing an application between multiple Avaya OneCloud™ Subscription systems

About this task

You can share an application only between Avaya OneCloud™ Subscription systems that are configured on the same Usage Metering Collector.

Before you begin

- Ensure that you have added the application in any one of the Avaya OneCloud™ Subscription systems between which you want to share the application. Use this procedure in the remaining Avaya OneCloud™ Subscription systems to share the application.

  For information about adding an application, see Adding an application to the Avaya OneCloud Subscription system on page 111.
- If you want to share Experience Portal between multiple Avaya OneCloud™ Subscription systems, ensure that you perform the prerequisites before sharing Experience Portal.

  For more information, see Prerequisites for sharing Experience Portal between multiple Avaya OneCloud Subscription systems on page 120.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.
3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.
4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system in which you want to share an application.
5. On the **APPLICATIONS** tab, click **Link Application**.

6. In the Link Application dialog box, in the **Application Type** field, click the application that you want share in the Avaya OneCloud™ Subscription system.
7. In the **Application** field, click the IP address of the application.
8. Click **LINK**.

Result

If you have shared this application in any other Avaya OneCloud™ Subscription system, the subscription ID of the Avaya OneCloud™ Subscription system is displayed under **Other Linked Systems** on the **APPLICATIONS** tab.

Related links

Application sharing between two or more Avaya OneCloud Subscription systems on page 23

Editing an application

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.
3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.
4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system in which you want to edit an application.
5. On the **APPLICATIONS** tab, click **Edit Application** corresponding to the application that you want to edit.
6. In the Edit Application dialog box, do the required modifications.

   For more information, see Create Application page field descriptions on page 112.
7. In the **State** field, click the option to indicate whether the application is in an active or paused state.

   Information in this field is used by Avaya to monitor the application status.
8. Click **SUBMIT**.

Deleting an application

About this task

Use this procedure to delete an application from an Avaya OneCloud™ Subscription system.

Caution:

Do not delete a mandatory application or any application that is used by your Avaya OneCloud™ Subscription system. If you delete such an application, WebLM will not grant the required license and the application will run in a license error mode. This causes your Avaya OneCloud™ Subscription system to stop after the permitted grace number of days.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.
3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.
4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system from which you want to delete an application.
5. On the **APPLICATIONS** tab, click **Delete** corresponding to the application that you want to delete.
6. In the Delete Application dialog box, click **OK** to delete the application.

Related links

Mandatory applications in an Avaya OneCloud Subscription system on page 85

Downloading the list of applications within an Avaya OneCloud™ Subscription system

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.
3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.
4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system.
5. Click **Export to CSV** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system.

   Usage Metering generates a .csv file that contains the list of applications and information about the applications that are configured in the Avaya OneCloud™ Subscription system.
6. Open the .csv file to view the list of applications.

   The .csv file opens in an Excel format.

Technical onboarding of applications to the Avaya Global Registration Tool

After you configure the WebLM and applications in your Avaya OneCloud™ Subscription system, you must perform a technical onboarding of your applications to the Avaya Global Registration

Tool (GRT). Technical onboarding involves configuring the SAL Gateway for each application to ensure remote connectivity of the application.

Technical onboarding of applications allows Avaya to manage your Avaya OneCloud™ Subscription system renewals.

Perform a technical onboarding of applications to do any of the following:

- Create SEIDS and Alarm IDs for applications.
- Test connectivity and alarming for applications.
- Modify the existing registered applications.
- Re-test connectivity and alarming.

The SAL Gateway allows Avaya Services personnel to:

- Monitor application alarms.
- Automatically open and close support tickets and notify you.
- Remotely access your applications and prioritize alarms.
- Provide remote maintenance and troubleshooting support.

Process to perform technical onboarding of applications to Avaya Global Registration Tool

Before you begin

Ensure that you have configured the required WebLM and applications in your Avaya OneCloud™ Subscription system.

Procedure

1. Steps to be performed by Avaya customers:
   a. Download the Excel file containing the list of applications that are configured in your Avaya OneCloud™ Subscription system.

      For more information, see Downloading the list of applications within an Avaya OneCloud Subscription system on page 123.

   b. Email the Excel file to Avaya at: recordsupport@avaya.com
2. Avaya will add the following additional columns to the Worksheet sheet and email the updated Excel file to the Avaya Business Partner or Avaya Professional Services personnel who is providing implementation and deployment support to the customer:
   - **AddIB**: Set to **True** if the application can be onboarded.
   - **Onboard**: Set to **True** if the application can be onboarded.
   - **IBNumber**: The Installed Base number of the application.
   - **SEID**: N/A

3. Steps to be performed by Avaya Business Partner or Avaya Professional Services personnel:
   a. Go to: https://support.avaya.com
   b. Click **Diagnostics & Tools** > **Global Registration Tool**.
   c. Use the information in the Excel file to onboard each application to the Avaya GRT and generate an SEID for the application.

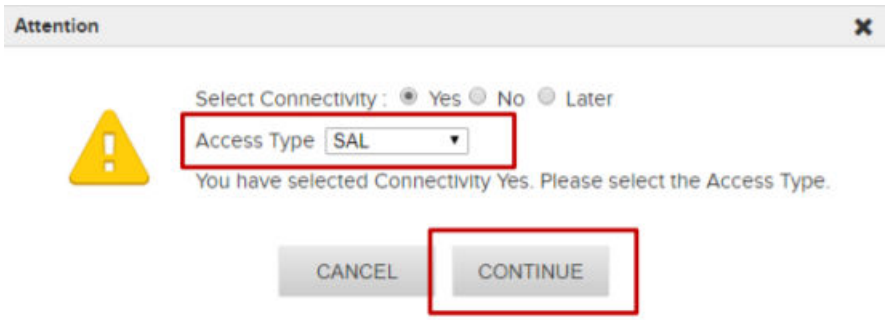
      Note:

      Perform a technical onboarding of only those applications for which the **AddIB** and **Onboard** columns are set to **True**, and the Installed Base number is provided in the Excel file.

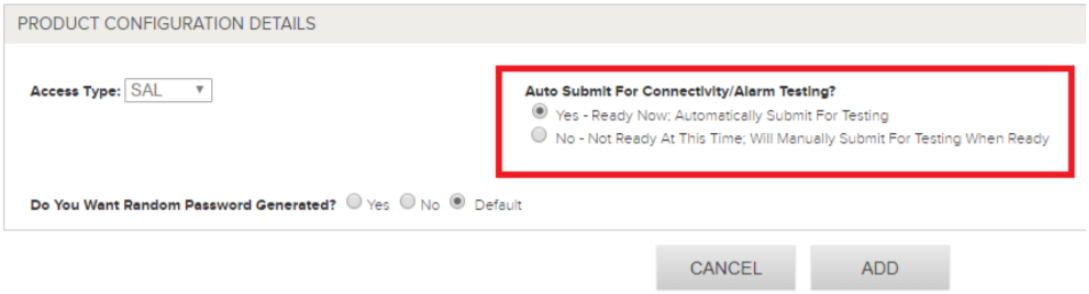
      When performing the technical onboarding, you must:

      - Click **Yes** in the **Select Connectivity** field and configure the SAL GW details.

        This allows Avaya to remotely monitor the Avaya OneCloud™ Subscription system of the customer and provide remote maintenance and troubleshooting support.



      - In **Auto Submit For Connectivity/Alarm Testing**, click **Yes - Ready Now; Automatically Submit For Testing** to automatically initiate connectivity and alarm testing after the technical onboarding of the application is completed.



      The documentation to perform technical onboarding of applications to the Avaya GRT is available on the Avaya Support site at: https://support.avaya.com

   d. Update the **SEID** column in the Worksheet with the SIED of the application that is generated by the GRT and email the Excel file to Avaya at: recordsupport@avaya.com

Managing the Avaya OneCloud™ Subscription system state

Before you begin

Ensure that you have configured the required Avaya UC and CC applications and WebLMs for the Avaya OneCloud™ Subscription system, and the system in an **Installing** state.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. Click **OFFERS**.
3. Click **Show Details** corresponding to the offer ID.

   Usage Metering displays the Avaya OneCloud™ Subscription systems within the offer ID.
4. Click **Show Details** corresponding to the subscription ID of the Avaya OneCloud™ Subscription system, state of which you want to change.
5. Click **COMPLETE INSTALLATION**.

   The **STATE** changes to **TESTING**.
6. Test the Avaya OneCloud™ Subscription system.
7. After you test the Avaya OneCloud™ Subscription system, click **GO LIVE**.

Migration of applications from perpetual licenses to subscription license

Prerequisites for migrating applications from perpetual licenses to subscription license

If you want to migrate an Avaya UC or CC application that is currently licensed under a perpetual license to a subscription license, ensure that the perpetually-licensed (on-premise) application is of either the minimum version supported by Avaya OneCloud™ Subscription or of a later version.

If the perpetually-licensed (on-premise) application is of an earlier version than the minimum supported version by Avaya OneCloud™ Subscription, then before adding the application to the Avaya OneCloud™ Subscription system, upgrade the application to at least the minimum supported version. For more information, see Migrating applications from perpetual licenses to subscription license on page 127.

For information about the minimum supported version numbers of Avaya UC and CC applications by Avaya OneCloud™ Subscription, see Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30.

Migrating applications from perpetual licenses to subscription license

Before you begin

Before you perform this procedure, ensure that you delete the perpetual licenses, license entitlements of which are transferred to Avaya OneCloud™ Subscription, from your WebLM server.

For information about managing the WebLM servers for licenses, see WebLM management on page 86.

Procedure

1. Place your Avaya OneCloud™ Subscription system order with Avaya.
2. Obtain your Access key and Secret key.

   For more information, see Obtaining the Access key and Secret key on page 28.
3. Install and configure the Usage Metering Collector.
4. Use the Usage Metering Collector to add WebLM to your Avaya OneCloud™ Subscription system.

   For more information, see Adding a WebLM server to an Avaya OneCloud Subscription system on page 89.

   After the Usage Metering Collector successfully registers to the WebLM server, Usage Metering automatically retrieves the subscription license for the subscribed applications from the Avaya back-office systems and installs it on the WebLM server.
5. Do the following if your on-premise application is of an earlier version than the minimum version supported by Avaya OneCloud™ Subscription:

   - Upgrade your on-premise application to at least the minimum version that is supported by Avaya OneCloud™ Subscription.

     You can also upgrade the on-premise application to any later version than the minimum supported version.

     For more information, see Avaya UC and CC applications supported by Avaya OneCloud Subscription on page 30 and Application upgrade on page 128.
6. Use the Usage Metering Collector to add the on-premise applications that are entitled by the subscription license to your Avaya OneCloud™ Subscription system.

   Note:

   The on-premise applications that are entitled by the subscription license can run by using the subscription license only after you add the applications to the Avaya OneCloud™ Subscription system.

   For more information, see Adding an application to the Avaya OneCloud Subscription system on page 111.
7. Register the applications to the Avaya Global Registration Tool.

For more information, see Technical onboarding of applications to the Avaya Global Registration Tool on page 123.

8. Manage the Avaya OneCloud™ Subscription system state.

   For more information, see Managing the Avaya OneCloud Subscription system state on page 126.

Result

Avaya OneCloud™ Subscription uses the subscription license to enable application entitlements and capacities. The billing is done based on your fixed quantity subscription offer.

Application upgrade

The following are the scenarios when an on-premise application needs to be upgraded:

- During migration, if the version number of the on-premise perpetually-licensed application does not match the minimum version number that is supported by Avaya OneCloud™ Subscription.

  For more information, see Migrating applications from perpetual licenses to subscription license on page 127.

- You already have an existing Avaya OneCloud™ Subscription system and you want to upgrade the on-premise applications subscribed under this Avaya OneCloud™ Subscription system.

  In this case, upgrade the on-premise application to the version number that you want. Because your Avaya OneCloud™ Subscription offer entitles you to the latest version of the subscribed applications, the upgrade version of the application is automatically licensed under the same subscription license. After you upgrade the on-premise application, update the application details in your Avaya OneCloud™ Subscription system.

  For more information, see Editing an application on page 122.

Note:

When upgrading the on-premise applications in your solution, ensure that you upgrade System Manager before you upgrade the other applications in your solution.

You can choose between any of the following two upgrade methods depending on whether the existing infrastructure capacities of the currently installed application version meet the requirements for the application version which you want to upgrade to:

- In-place
- Donor/Target

In-place

You can perform an in-place upgrade if the existing infrastructure resource capacities of the current running version of the application meet the requirements for the upgrade version. An in-place upgrade is service impacting for all users of the application.

Donor/Target

You can perform a Donor/Target upgrade when the existing infrastructure resource capacities of the current running version do not meet the requirements for the upgrade version.

In this model you must: deploy the new Target infrastructure, install the upgrade version, and modify the Donor system configuration as required. Only individual users are impacted when the users are migrated from the Donor system to the Target system.

Chapter 7: Usage Metering backup, restore, and geo-redundancy

Usage Metering server failure scenarios

About this task

For a catastrophic failure of the Usage Metering server, see Usage Metering restore on page 132.

Usage Metering server does not work if:

- Disk fails.
- Host fails as the Partner does not use VMware HA.
- VMware host is deleted.

Data collection failure and recovery

Data collection failure

This failure occurs when the system:

- Detects that the configured data source is inactive.
- Fails to connect to the data source.
- Detects a change in the credentials of the data source that you configured. For example, change in the database password.

  For Avaya Aura® Experience Portal, the system detects a change in the name of the Avaya Aura® Experience Portal database.
- Fails to connect to Avaya back-office systems.
- A new Usage Metering server is added.
- A new meter is added.
- Incorrect meter configuration.
- Usage Metering disaster.

  For example, virtual machine (VM) is accidentally deleted and recovered by using a backup file.

Recovery from data collection failure

To recover from this failure, the system automatically:

- Collects and sends data at regular intervals.
- Generates relevant alerts.

If Usage Metering is configured to support active geo-redundant data sources, then it also supports the configuration of primary and secondary data sources.

If the data collection from the primary data source fails, Usage Metering collects data from the secondary data source.

If the data collection from both data sources fails, Usage Metering sends an alert. For more information, see Configuring alerts on page 54.

Usage Metering backup and restore

The system stores a backup of the Usage Metering files in the Avaya back-office systems.

You must perform a new installation of the Usage Metering server and restore the Usage Metering data by using the Usage Metering backup file in the following scenarios:

- You accidentally delete the Usage Metering server or the Usage Metering server stops responding.
- The Usage Metering system gets corrupted.
- You upgrade RHEL 7.x to 8.x and want to restore Usage Metering from RHEL 7.x on 8.x.

Usage Metering backup

Usage Metering creates a backup:

- Every day at 2:00 a.m. local time.
- Within minutes after you change the configuration for a meter.

  For example,

  - Change the password of a meter.
  - Add a user to the system.
  - Change the configuration of the system.

The system stores and uploads a backup of the file to the Avaya back-office system.

Important:

Usage Metering saves only the last backup file.

Usage Metering restore

You must perform a new installation of the Usage Metering server and restore the Usage Metering data by using the Usage Metering backup file in the following scenarios:

- You accidentally delete the Usage Metering server or the Usage Metering server stops responding.
- The Usage Metering system gets corrupted.
- You upgrade RHEL 7.x to 8.x and want to restore Usage Metering from RHEL 7.x on 8.x.

Ensure that you do not run two instances of Usage Metering at the same time.

The new or replaced Usage Metering retroactively collects the missing usage data for the period in which it was not working. This is to a maximum of 60 previous days.

For scenarios in which Usage Metering does not collect usage data, see Data collection failure and recovery on page 130.

Ensure that you install a new Usage Metering first, and then restore a Usage Metering backup file.

Restoring Usage Metering

About this task

Install a new copy of the Usage Metering server first, and then restore the system by using the Usage Metering backup file.

If your IT infrastructure uses a proxy server, you have configured the proxy details in the `bash_profile` file, and you are using root credentials, then run the commands in this procedure without using **`sudo`**. If you run the commands by using **`sudo`**, Usage Metering Collector installation tries to connect to the cloud services without using the proxy server.

Before you begin

Before restoring the system, check that the latest CentOS or RHEL server is configured with the same hostname as that of the earlier server.

Install the software backup file on a new server that has the same host name.

This procedure restores all certificates.

Caution:

The browser does not connect if the host name of the new Usage Metering server is not identical to the host name of the earlier Usage Metering server.

Procedure

1. Open an SSH session to the CentOS or RHEL server on which you want to install and restore Usage Metering.

   You can use an application such as PuTTY.

2. Perform the Usage Metering Collector pre-installation configuration.

   For more information, see the Planning and pre-installation configuration section.

3. **(Optional)** Install the man-in-the-middle attack proxy root CA certificate file on the server.

   You can use one of the following options:

   - By using the WinSCP software to place the certificate file in the location that you want on the server.
   - By using the following procedure:
     a. Open the web proxy root CA certificate file.
     b. Copy and paste the certificate content into your SSH session.
     c. To install the certificate file, run the following commands in your SSH session:

        ```
        sudo yum -y install ca-certificates
        sudo cp proxy-root-ca.pem /etc/pki/ca-trust/source/anchors/
        sudo update-ca-trust
        ```

     d. Rename the certificate file according to the `.pem` format.

        The `.pem` certificate format must have the following:

        - Plain text
        - Must start with the text, "-----BEGIN CERTIFICATE-----"
        - Must end with the text, "-----END CERTIFICATE----".

4. To add the Usage Metering Yum repository to your Yum configuration, do one of the following:

   - If you are installing Usage Metering Collector on CentOS 7.x or RHEL 7.x, run the following command in your SSH session:

     ```
     sudo curl -o /etc/yum.repos.d/avaya-um.repo \
     https://yum.avaya.com/um-repo/avaya-um.repo
     ```

     You can type or copy the entire command on one line.

     Ensure that there is a space before the backslash (\) and no space after the backslash (\) on the first line.

   - If you are installing Usage Metering Collector on RHEL 8.x, run the following command in your SSH session:

     ```
     sudo curl -o /etc/yum.repos.d/avaya-um-rhel8.repo https://
     yum.avaya.com/um-repo-rhel8/avaya-um-rhel8.repo
     ```

5. Run the following command to install Usage Metering Collector and all required dependencies:

   ```
   sudo yum -y install avaya-usage-metering
   ```

6. Run the following command to specify the stage name of the Usage Metering deployment:

   ```
   echo "stage=<stage name>" | sudo tee -a /opt/Avaya/usage-metering/
   um.properties
   ```

The stage name must match the stage name of the Usage Metering system you are restoring.

7. Run the following command to restart Usage Metering:

   ```
   um-restart
   ```

8. If your IT infrastructure uses a proxy server, configure the proxy details in the Usage Metering Collector.

   For more information, see Configuring non-transparent proxy in the Usage Metering Collector on page 46.

9. In a web browser, type the IP address of the CentOS or RHEL server on which you installed the Usage Metering Collector.
10. Click through the Self-Signed SSL certificate warning.

    You can click **Continue to this website (not recommended)**.

11. After you read the terms and conditions, select the **I accept the terms and conditions in the license agreement** check box and click **ACCEPT**.
12. On the Create Initial User page, click **Restore from backup**.
13. In the **Database Restore** dialog box, enter the following credentials:
    a. In the **AWS Access Key** field, type your valid Access key.
    b. In the **AWS Secret Key** field, type your valid Secret key.
    c. In the **Collector ID** field, click the ID of the Usage Metering Collector that you want to restore.
    d. Click **RESTORE**.

       After the system validates your credentials, Usage Metering restarts.

       You must refresh the page to log in to Usage Metering.

    e. Click **REFRESH**.

Uninstalling Usage Metering Collector

Procedure

1. Open an SSH session to the server where Usage Metering Collector is installed.
2. At the command prompt, run the following command:

   ```
   sudo yum remove avaya-usage-metering
   ```

   Note:

   If you are uninstalling Usage Metering Collector and then reinstalling, the system is in the same state as a new installation.

Based on your requirement, you can do one of the following:

- To perform a fresh installation of Usage Metering Collector without retaining the previous data, select **Create Initial User**.
- To restore previous data, select **Restore from Backup**.

Restoring Usage Metering Collector after uninstallation

About this task

You can restore the backup file of Usage Metering Collector only on a fresh installation of the Collector software. After reinstallation of Usage Metering Collector, the system displays the EULA page.

Procedure

1. On the EULA page, click **ACCEPT**.
2. Click **Restore from backup**.
3. In the **AWS Access Key** field, type the access key.
4. In the **AWS Secret Keys** field, type the secret key.
5. In the **Collector ID** field, click the ID of the Usage Metering Collector that you want to restore.
6. Click **Restore**.

   Usage Metering Collector retrieves the backup archive and attempts to restore the data.

   Note:

   You must restore the backup on a server with the same hostname. All certificates, including the server certificate, are restored.

Usage Metering in a geo-redundant environment

In a geo-redundant environment, if the Usage Metering server fails in the primary data center or if a network outage is detected, you must perform a new installation of the Usage Metering server in the secondary data center. You must then restore the backup of the primary Usage Metering server on the secondary Usage Metering server by using the Usage Metering backup file.

To implement the Usage Metering Collector, you must create a secondary data center virtual machine to run the Usage Metering Collector application if the primary data center fails. The deployment process of a Usage Metering Collector in a geo-redundant data center starts with installation, configuration, usage data collection and ends with verification of the collected data.

You can create a virtual machine in the secondary data center, and then install the Usage Metering Collector on the virtual machine in the secondary data center. For more information, see Moving Usage Metering Collector between data centers on page 136.

After the primary data center starts working, you can install the Usage Metering Collector in the primary data center and restore the data by using the Usage Metering backup file.

The topics in the section provide the following information to configure Usage Metering for geo-redundancy:

- Primary Usage Metering.
- Secondary Usage Metering.
- Cold standby.
- Method to move the service back to the primary data center.
- Secondary data center recovery process.
- Test the recovery process.

Verifying data collection on primary and secondary Usage Metering

Perform the following steps for verifying the data collection from the data source:

1. During the deployment of the primary data center Usage Metering Collector, configure the data sources according to the initial primary and secondary data sources and verify the collection.
2. Reverse the primary and secondary data sources.
3. Verify the usage data collection.
4. Move the Usage Metering Collector between data centers and verify the collection from the secondary data center data sources.

   For more information, see Moving Usage Metering Collector between data centers on page 136.
5. Re-configure the data sources as the original primary and secondary data sources and verify the collection from primary data sources.
6. Move the Usage Metering Collector between data centers and verify the usage data collection from the primary data source.

Moving Usage Metering Collector between data centers

About this task

Use this procedure to move the usage data collection to an alternate data center.

Before you begin

- Verify the **ssh** access and root privilege on the active Usage Metering Collector virtual machine and the alternate data center virtual machine. The verification of ability to login to the Usage Metering Collector virtual machine is done using an **ssh** tool and using the Usage

Metering Collector IP address. Use the **sudo su** command to verify root privileges required to install the Usage Metering Collector.

- Ensure that the Access key and Secret key are available for the restore procedure. The Access key and Secret key are the keys that you receive from Avaya to enable the Usage Metering Collector to connect to the Avaya back-office systems.

Procedure

1. On the active Usage Metering Collector virtual machine, uninstall the Usage Metering Collector application.

   For more information, see Uninstalling Usage Metering Collector on page 134.

2. On the alternate data center virtual machine, install the Usage Metering Collector application and restore the backup of the Usage Metering Collector database file.

   For more information, see Restoring Usage Metering Collector after uninstallation on page 135.

Preparing a cold standby server

About this task

Use this procedure to configure the Usage Metering server as a cold standby server.

Procedure

1. Turn on the power to the Usage Metering server.
2. On the Usage Metering server, install CentOS or RHEL.
3. Configure the secondary SAL GW with the SEID of Usage Metering.
4. Connect the following to the secondary data center:
   - SAL GW
   - SNMP Trap Host
   - Avaya cloud
5. Turn off the power to the Usage Metering server.

   For geo-redundant deployment, the Usage Metering server connected to the data source on the secondary data center is configured as a cold standby.

Secondary data center recovery process

Procedure

1. If the Usage Metering server fails in the primary data center, you must perform a new installation of the Usage Metering server in the secondary data center. You must then restore the backup of the primary Usage Metering server on the secondary Usage Metering server by using the Usage Metering backup file.

   For more information, see Usage Metering restore on page 132.

2. Configure the IP addresses of SAL GW or SNMP Trap Host, to the corresponding IP addresses of the secondary data center.

   You can deploy the secondary data center as a cold standby.

Moving service back to the primary data center

Procedure

1. Turn off power to the Usage Metering server in the secondary data center.
2. To restore the primary Usage Metering server in the primary data center, see Restoring Usage Metering on page 132.
3. Configure the IP addresses of SAL gateway or SNMP Trap Host, which are on the secondary data center, to the corresponding IP addresses of the primary data center.
4. Delete the cold standby Usage Metering server in the secondary data center.
5. To configure Usage Metering server as a cold standby, see Preparing a cold standby on page 137.

Testing the recovery process

Procedure

1. Turn off power to the Usage Metering server in the primary data center.
2. Delete the old Usage Metering server instance from the primary data center.
3. Recover Usage Metering in the secondary data center.

   For more information, see Secondary data center recovery process on page 137.
4. Verify the following:
   - Usage Metering starts collecting usage data.
   - Usage Metering sends alerts to SAL GW and SNMP Trap Host.
5. Turn off power to the cold standby Usage Metering server.
6. Delete the secondary cold standby.
7. Recover the Usage Metering server on the primary data center.
8. Prepare the cold standby.

   For more information, see Preparing a cold standby server on page 137.

Chapter 8: Upgrade Usage Metering Collector

Upgrading Usage Metering Collector

About this task

Usage Metering automatically detects daily if a Usage Metering update is available.

If an update is available, Usage Metering automatically upgrades to the newer version at 3:00 a.m. local time.

If a restart is required, Usage Metering automatically restarts after the upgrade is completed.

After the Usage Metering software is upgraded, Usage Metering sends a notification email.

Important:

Periodically upgrade the CentOS or RHEL operating system. Updating the system changes some components that the system uses. Restart Usage Metering after you upgrade the system.

Avaya recommends you to periodically update the `yum` software on the server to get the latest updates and security enhancements.

You can, however, use the following procedure if you want to upgrade Usage Metering manually.

If your IT infrastructure uses a proxy server, you have configured the proxy details in the `bash_profile` file, and you are using root credentials, then run the commands in this procedure without using **`sudo`**. If you run the commands by using **`sudo`**, Usage Metering Collector upgrade tries to connect to the cloud services without using the proxy server.

Procedure

1. Run the following command to update Usage Metering:

   ```
   sudo yum -y update avaya-usage-metering
   ```

2. Run the following command to verify if Usage Metering requires a restart after the update:

   ```
   sudo um-needs-restarting
   ```

3. If the output of the preceding command indicates that Usage Metering requires a restart, run the following command to restart Usage Metering:

   ```
   sudo um-restart
   ```

Chapter 9: Troubleshooting

No more mirrors to try error message is displayed during Usage Metering Collector installation

Condition

The following error message is displayed during Usage Metering Collector installation:

```
No more mirrors to try
```

Cause

The following are the possible causes:

- The `/etc/yum.repos.d` directory contains other `yum` repositories in addition to the RHEL repositories or avaya-um.repo repository.
- Your corporate firewall does not provide access to the URLs that are required for the Usage Metering Collector.
- The repository URL is unreachable due to network-related problems.

Solution

Depending on the cause of the problem, do any of the following:

- Do the following to ensure that the `/etc/yum.repos.d` directory contains the correct repository:
  a. Open an SSH session to the server where the Usage Metering Collector is installed and run the following command to view the repositories that are present in the `/etc/yum.repos.d` directory:

     `11 /etc/yum.repos.d`

     If you are installing Usage Metering Collector on CentOS, ensure that the `/etc/yum.repos.d` directory contains the `avaya-um.repo` repository.

     If you are installing Usage Metering Collector on RHEL, ensure that the `/etc/yum.repos.d` directory contains the RHEL repositories.

  b. If the `/etc/yum.repos.d` directory contains any other unused `yum` repository, run the following command to delete such repository.

     Before deleting the repository, ensure that the repository is not used by any other application that is installed on the operating system.

     `rm -rf /etc/yum.repos.d/<repository name>`

- Ensure that your corporate firewall allows access to the URLs that are required for the Usage Metering Collector.

  For more information, see Required URLs for Usage Metering Collector on page 42.
- Rectify network-related problems, if any.

For more information, see https://access.redhat.com/solutions/203603.

Usage Metering SNMP MIB file location

The `AVAYA-USAGE-METERING-MIB.txt` Management Information Base (MIB) file is located in the following directory on the Usage Metering Collector server:

`/opt/Avaya/usage-metering/bin/`

Related links

Configuring alerts on page 54

Verifying Usage Metering Collector connectivity and operating system parameters

About this task

Use this procedure to:

- Identify connectivity problems between Usage Metering Collector and Avaya back-office systems.
- Monitor the Usage Metering Collector-relevant parameters of the operating system.

Procedure

1. Log in to the Usage Metering Collector CLI by using root credentials.
2. To verify the connectivity between Usage Metering Collector and Avaya back-office systems, do one of the following:
   - If the Usage Metering Collector is installed on CentOS 7.x or RHEL 7.x, run the following command:

     `bash /opt/Avaya/usage-metering/bin/validateUM.customer -a`
   - If the Usage Metering Collector is installed on RHEL 8.x, run the following command:

     `bash /opt/Avaya/usage-metering/bin/validateUM.customer f trial -a`

   The system displays the following:
   - Connectivity status of the various Usage Metering components.

- Status of the Usage Metering-relevant parameters of the operating system where Usage Metering Collector is installed.

These logs are stored in the `validateUM.<date of file generation>-<process ID>.<hostname of Usage Metering server>.tbz` file at the `/var/log/validate/` location.

For example, `validateUM.20200611-1350.Monitor.tbz`

3. To view the existing log files for connectivity, do any of the following:
   - To view the list of .tbz files, run the following command:

     `ls -lrt /var/log/validate`
   - To view the contents of the latest .tbz file, run the following command:

     `bash /opt/Avaya/usage-metering/bin/validateUM.customer -x`
   - To view the contents of the .tbz file that was generated on a specific date, run the following command:

     `bash /opt/Avaya/usage-metering/bin/validateUM.customer --dump one -x /var/log/validate/<filename>.tbz`

     For example:

     `bash /opt/Avaya/usage-metering/bin/validateUM.customer --dump one -x /var/log/validate/validateUM.20200611-1350.Monitor.tbz`

Viewing the recent logs and downloading the log files

About this task

Usage Metering retains the log files for a period of 30 days. Usage Metering automatically deletes the log files that are older than 30 days.

When viewing the logs, you can select the **Pause** check box to pause log monitoring.

Selecting the **Pause** check box stops adding new rows of recent logs in the **Recent Logs** area. Thus, enabling you to read the displayed logs without the line numbers getting changed.

The **Recent Logs** area shows the Usage Metering server logs.

You can clear the **Pause** check box to resume viewing the new logs.

Note that all logs are written to the log files irrespective of whether the **Pause** check box is selected or cleared.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click **OVERVIEW**.

3. To view the recent logs, select the **Show Recent Logs** check box.

   Usage Metering Collector shows the recent logs in the **Recent Logs** area.

4. **(Optional)** To filter, pause, and view only specific number of logs, do the following:

   a. In the **Recent Logs** area, click **Show Log Options** .

   b. In the **Lines** field, type the number of recent logs that you want to view.

      The minimum value is 5 logs and maximum value is 1000 logs. The default value is 100 logs.

   c. Select the **Pause** check box to pause log monitoring.

   d. In the **filter logs** field, type the filtering criteria to filter the logs. For example, date or text.

5. To download the log files, click **DOWNLOAD LOGS**.

   The log files are downloaded in a .zip file.

   The .zip file contains the Usage Metering server logs and the Usage Metering Collector installation logs.

Viewing the audit log of user activity in Usage Metering

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click **AUDIT LOGS**.

   Usage Metering shows the logs of user activities.

3. Click **DOWNLOAD AUDIT LOGS** to download the audit logs in a .csv file.

Usage Metering does not display data when you log in by using the same window after two days

Condition

In the web browser, you stay logged in to the Usage Metering window for one or two days.

Cause

The web browser auto expires the certificates that the system uses, while establishing your previous session.

Solution

1. Refresh the same webpage.

2. Alternatively, in the web browser, open a new window to log in to Usage Metering.

Usage Metering Collector cannot recognize a web proxy CA certificate

Condition

Usage Metering Collector cannot recognize a web proxy CA certificate.

Cause

Your IT infrastructure uses a web proxy to identity a man-in-the-middle attack, but the web proxy CA certificate is not added to the list of CA certificates that are trusted by `curl` and `yum`.

Use this procedure to add a CA certificate of a web proxy server to the list of CA certificates that are trusted by `curl` and `yum`.

A web proxy server inspects the HTTPS traffic between the Usage Metering server and other servers by performing a man-in-the-middle attack.

Note:

Use this procedure while installing the Usage Metering Collector for the first time.

Before you begin with the procedure, ensure that you get the web proxy's Root CA certificate in PEM certificate format from the CA. The PEM certificate format starts with "-----BEGIN CERTIFICATE-----" and ends with "-----END CERTIFICATE----".

Solution

1. Open an SSH session to the CentOS or RHEL server on which Usage Metering Collector is installed.

   You can use an application such as PuTTY.

   If you have manually uploaded the web proxy's Root CA certificate file to the Usage Metering Collector by using a Secure Copy (SCP) command, go to Step 3.

2. Run the following command to add the web proxy's Root CA certificate file to the server:

   `echo | openssl s_client -showcerts -servername yum.avaya.com -connect yum.avaya.com:443 > <filename>.pem`

3. Run the following commands to install the certificate:

   `sudo yum -y install ca-certificates`

   `sudo cp <filename>.pem /etc/pki/ca-trust/source/anchors/`

   `sudo update-ca-trust`

4. If the following error message is displayed, re-run the commands shown in Step 3 to install the certificate:

   `verify error:num=20:unable to get local issuer certificate`

5. Install the web proxy's Root CA certificate for outbound connections.

For more information, see Installing an outbound certificate on page 80.

This allows Usage Metering to communicate with the cloud services.

Usage Metering Collector did not refresh the subscription license

Condition

A subscription license has an expiration period of 30 days. Usage Metering automatically refreshes the subscription license after every 20 days. If Usage Metering is unable to refresh the license after 20 days, Usage Metering sends an alert. If the subscription license is not replaced within the 30 days expiration period, then after 30 days, the applications run in a license error mode.

Solution

Create an IT ticket with Avaya at: https://onecare.avaya.com

Usage Metering Collector cannot connect to Avaya Aura® Messaging

Condition

You have already installed the System Manager-signed CA certificate in Usage Metering Collector and Avaya Aura® Messaging.

However, Usage Metering Collector still shows a connection failure due to invalid certificate message after you click the **TEST** button when adding Avaya Aura® Messaging to your Avaya OneCloud™ Subscription system.

Cause

More than one certificate with the same Common Name (CN) is installed in Avaya Aura® Messaging.

Solution

Remove the unwanted certificates with the same CN from Avaya Aura® Messaging.

Ensure that Avaya Aura® Messaging does not contain two or more certificates with the same CN.

Related links

Adding an application to the Avaya OneCloud Subscription system on page 111

Alert management

Viewing Usage Metering alerts

About this task

Use this procedure to view the Usage Metering alerts.

You must resolve the alerts to avoid automated billing problems. After an alert is resolved, you must clear the alert.

For information about clearing an alert, see Clearing a resolved alert on page 150.

You can also perform the configuration to send the alerts to Avaya and to the email addresses that you want. For more information, see Configuring alerts on page 54.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click **ALERTS**.

   Usage Metering Collector shows the generated alerts.

3. Click **Show Details** corresponding to an alert to view the information related to the alert.

   The alert information is displayed on **Alert Details** page.

Usage Metering alerts

The following table provides the list of Usage Metering alerts along with the possible reasons and solutions:

Alert title	Possible reasons why Usage Metering generated the alert [1]	Solution
UM Alert 1: Internal Error	N/A	Contact Avaya Support.
UM Alert 2: Uncaught exception — restart required	N/A	Restart Usage Metering by using the `sudo um-restart` command after one minute.
UM Alert 3: Service suspended until updated License Terms are accepted	N/A	Log on to the Usage Metering web interface and accept the terms that are displayed.
UM Alert 4: Updated License Terms declined — software uninstalled	N/A	Restore Usage Metering from backup. For more information, see Usage Metering restore on page 132.

Table continues…

Alert title	Possible reasons why Usage Metering generated the alert [1]	Solution
UM Alert 9: Email send failed	• Invalid SMTP server configuration. • Network outage. • SMTP server outage.	Check the SMTP configuration and the SMTP server. For more information, see Configuring SMTP mail server to send email notifications on page 53
UM Alert 10: Snmp trap send failed	• Invalid SNMP server configuration. • Network outage. • SNMP server outage.	Check the SNMP trap server configuration and the SNMP server. For more information, see Configuring alerts on page 54
UM Alert 14: User {EMAIL} locked out	The number of permissible consecutive failed login attempts by user is reached.	Unlock the user account. For more information, see Enabling or disabling a user account on page 59.
UM Alert 30: Failed to connect to data source	• Invalid data source configuration. • Network outage. • Metered solution element server outage.	Check the data source connection address and credentials. For more information, see: • Adding an application to the Avaya OneCloud Subscription system on page 111 • Create Application page field descriptions on page 112
UM Alert 32: Failed to upload collected data	• Network outage. • Man-in-the-middle attacking web proxy is configured, but the web proxy's CA certificate is not installed.	• Check your internet connection and the HTTPS path. • Install the web proxy's CA certificate. For more information, see Usage Metering Collector cannot recognize a web proxy CA certificate on page 144.
UM Alert 34: Primary data source failed — data collection succeeded from Secondary data source	Primary credentials failed, but Usage Metering was able to collect data from the Secondary system.	Rectify the Primary credentials for the data source.
UM Alert 35: Deleting local collection folder structure failed	The cleanup task failed to delete the empty folders in the local upload folder structure.	Examine the log files to view the reason for the deletion failure. For more information, see Viewing the recent logs and downloading the log files on page 142.
UM Alert 37: Recollected data for meter	The data is recollected for a meter for which meter collection has failed in the past.	This is an informative alert.

Table continues…

Alert title	Possible reasons why Usage Metering generated the alert [1]	Solution
UM Alert 100: Disk space is below threshold	N/A	Free up your disk space, or use a server that has the required disk space to run the Usage Metering software.
UM Alert 101: A certificate is about to expire	N/A	Install a new SSL certificate.
UM Alert 102: A certificate has expired	N/A	Install a new SSL certificate.
UM Alert 104: Auto-update of avaya-usage-metering rpm failed	The upgrade is incompatible with the previous release.	Do the following: 1. Stop the current Usage Metering instance. 2. Install a new Usage Metering Collector on another server. 3. Install the avaya-usage-metering rpm. 4. Restore from backup.
UM Alert 105: Unable to check for update of Usage Metering	Man-in-the-middle attacking web proxy is configured, but the web proxy's CA certificate is not installed.	Install the web proxy's CA certificate. For more information, see Usage Metering Collector cannot recognize a web proxy CA certificate on page 144.
UM Alert 106: Avaya Usage Metering update applied	N/A	This is an informative alert.
UM Alert 109: Avaya Usage Metering server started	N/A	This is an informative alert.
UM Alert 115: New orderable service provisioned and available to configure	New orderable service is added in the current offer.	This is an informative alert.

Table continues…

Alert title	Possible reasons why Usage Metering generated the alert [1]	Solution
UM Alert 600: WebLM Operation Failed(<*operationName*>) for WebLM <*WebLMName*>	• Failed to register the Usage Metering Collector with WebLM. • Failed to unregister the Usage Metering Collector From WebLM. • Failed to retrieve the HostId From WebLM. • Failed to install the subscription license file on WebLM. • Failed to share list of allowed applications with WebLM. • Failed to clear the list of denied applications from WebLM.	• Reregister with the WebLM. For more information, see Editing a WebLM server on page 90. • Manually synchronize the Usage Metering Collector with the WebLM. For more information, see License and software enablement on page 24. • If the problem persists, contact Avaya Support.
UM Alert 601: Subscription License Generation Failed(<*operationName*>) for WebLM <*WebLMName*>	• Subscription license creation request failed. • Subscription license retrieval failed.	Usage Metering automatically retries to retrieve the subscription license file within 48 hours of the license generation failure. However, if the problem persists, contact Avaya Support.
UM Alert 602: Failed to install Subscription license	WebLM sends an error code other than `200 OK`.	The system automatically retries to install the subscription license file on the WebLM server within 48 hours of the subscription license installation failure. You can also re-register Usage Metering Collector to the WebLM server. For more information, see Editing a WebLM server on page 90. However, if the problem persists, contact Avaya Support.
UM Alert 603: State Operation For the System Failed for system <*systemName*>	• State retrieval failed. • State Change trigger failed. • State Change event status retrieval failed.	Contact Avaya Support.

Table continues…

Alert title	Possible reasons why Usage Metering generated the alert [1]	Solution
UM Alert 604: Unconfigured applications tried to access the license for WebLM <*WebLMName*>	An application that is not configured on the Usage Metering Collector tries to acquire the subscription license from the WebLM.	Configure the application on the appropriate Usage Metering Collector and remove the application from this Usage Metering Collector.
UM Alert 605: Collector is not able to reach WebLM for WebLM <*WebLMName*>	N/A	• Check if there are any network problems. • Ensure that the WebLM server is running.
UM Alert 606: IX Subscription License has been successfully Installed	N/A	This is an informative alert.
UM Alert 990: Test Alert	• You click **TEST ALERT** on the alert configuration page. For more information, see Configuring alerts on page 54. • Usage Metering Collector has sent an SNMP keep-alive trap message. For more information, see Enabling SNMP keep-alive trap messages from Usage Metering Collector on page 71.	This is an informative alert.

[1] The possible reasons of alert generation are documented in this topic only where the reasons are not obvious in the alert title.

For information about verifying connectivity between Usage Metering Collector and Avaya back-office systems, see Verifying Usage Metering Collector connectivity and operating system parameters on page 141.

Clearing a resolved alert

About this task

After a Usage Metering alert is resolved, you must clear the alert.

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click **ALERTS**.

   Usage Metering Collector shows the list of generated alerts.
3. Click **Clear Alert** corresponding to a resolved alert that you want to clear.

4. Click **OK** on the confirmation message to clear the alert.

Result

- Usage Metering changes the status of the alert to **Cleared Alert** on the **ALERTS** tab.
- Usage Metering updates the audit log of this user activity on the **AUDIT LOGS** tab.

Application maintenance support

About this task

You can create a service request with Avaya for maintenance support of applications that are part of your Avaya OneCloud™ Subscription system.

Procedure

1. Log on to https://support.avaya.com by using your Avaya credentials.
2. Under **Service/Parts Request**, click **Create Service Request**.
3. On the Create a Service Request page, provide the required details.

Note:

Ensure that you specify the SEID of the application that needs maintenance support in the service request.

Chapter 10: Resources

Viewing the Avaya OneCloud™ Subscription online Help

Procedure

1. Log on to the Usage Metering Collector interface by using a web browser.
2. On the Home page, click , and then click **HELP** .

Result

The Avaya OneCloud™ Subscription online Help is displayed in a new browser.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.

- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Appendix A: Port assignment

Port assignments

Inbound ports

Port	Protocol	Purpose
TCP 22	SSH	Installing, troubleshooting.
TCP 80	HTTP	Redirecting to HTTP port 443. **Note:** Usage Metering functions normally without configuring this port. In this case, the HTTP web browser access is not redirected to the web user interface.
TCP 443	HTTPS	Web user interface.

Usage Metering does not use any UDP server ports. You can harden or block access to all other inbound ports.

Note:

Usage Metering software binds to Port 8443. This is for internal use only. You can block an external access to Port 8443.

Outbound ports

Port	Protocol	Purpose
UDP 162	SNMP	Sending alerts as SNMP traps to a local SNMP trap host. Sending alerts to the SAL Gateway.

Table continues…

Port	Protocol	Purpose
TCP 443	HTTPS	• HTTPS access to the public internet, including a Domain Name System (DNS). • Using HTTPS to communicate with services in the Avaya cloud. • Interacting with the Avaya cloud by using the public internet. • Connecting with the Avaya and CentOS or RHEL Yum servers for receiving software updates. • Working with a web proxy that inspects HTTPS content by using man-in-the-middle attacks.
UDP 514	Syslog	Sending alerts to a Syslog server. Configuring a syslog and a system alert. Configuring this port is optional.
TCP 2525	SMTP	Sending email notifications for the following: • Alert • Software upgrades • Self-service password reset **Note:** You can configure the TCP port used to send email. The default port is 2525.

WebLM port

Port	Protocol	Purpose
TCP 52233	HTTPS	Usage Metering uses this port to communicate with the WebLM server.

Glossary

Term	Description
CapEx	Customer pays for software up front from a capital expenditure budget.
OpEx	Customer pays for the use of the software from their operating expense budget on a recurring basis over a term period. For example, monthly or yearly.
Fixed Quantity Subscription	Fixed quantity subscription of software typically billed up front on a recurring basis and used for a specific, limited period of time during which the customer can use the software. The customer is billed for the fixed subscribed quantity, independent of the customer's actual use.
Overage	Overage refers to the additional capacity that the customer is entitled for over the Fixed Quantity Subscription without any additional charges.
Sold To Number (ST) or Functional Location Number (FL)	Avaya site number for a specific location.
Service bundle	A service bundle is a collection of services that are grouped. An example of a service is the Avaya Aura® Experience Portal IVR service. An example of a service bundle is Calling plus Voicemail.

Index

A

account lockout policy parameters 67
adding
  applications 111
  WebLM 89
alerts 54
application
  maintenance support 151
application management 92
application sharing 121
  between Avaya OneCloud™ Subscription systems 23
Avaya OneCloud™ Subscription
  architecture 21
  service usage reports 37
Avaya OneCloud™ Subscription system 82
  deployment models 33
  mandatory applications 85
  process flow 25
Avaya OneCloud™ Subscription systems
  multiple Usage Metering Collectors 36
Avaya support website 154

C

changing
  application state 122
  Usage Metering Collector password 61
checklist
  adding applications 92
clearing
  alert 150
collection
  delete 153
  edit name 153
  generating PDF 153
  sharing content 153
configuring
  account lockout policy 66
  AIDE 73
  alerts 54
  failed login attempt threshold 56
  name for Usage Metering Collector 53
  non-transparent proxy details in bash_profile 43
  non-transparent proxy in Usage Metering Collector 46
  password policy 62
  password reset policy 64
  proxy server authentication 46
  security banner 58
  session timeout 56
  SMTP mail server 53
  Usage Metering and Avaya back-office systems connectivity 52
configuring *(continued)*
  web proxy CA certificate 144
content
  publishing PDF output 153
  searching 153
  sharing 153
  sort by last updated 153
  watching for updates 153
create application page
  field descriptions 112
creating
  initial user 51
  user 58
creating user account
  Experience Portal local Postgres database 97

D

data collection
  failure and recovery 130
data source applications 83
deleting
  application 122
  user 61
  WebLM 91
disabling
  hostname validation 72
  user account 59
disk partition encryption
  Data Privacy 42
documentation center 153
  finding content 153
  navigation 153
documentation portal 153
  finding content 153
  navigation 153
downloading
  list of applications within Avaya OneCloud™ Subscription system 123
  log files 142

E

editing
  application 122
  user 59
  WebLM 90
enabling
  EASG login 57
  hostname validation 72
  keep-alive messages 71
  SSL between Experience Portal database and Usage Metering 97

enabling *(continued)*
SSL between Usage Metering and Avaya Callback Assist ... 105
SSL connection to CMS database ... 108
user account ... 59
exporting
root CA certificate from System Manager ... 88
SIP-CA demo certificate from System Manager ... 88

F

finding content on documentation center ... 153
forcing
password change on first login ... 59

G

generating
CSR ... 75
self-signed certificate ... 77

I

InSite Knowledge Base ... 154
installing
Advanced Intrusion Detection Environment ... 73
CSR response ... 76
outbound certificate ... 80
server certificate ... 77
Usage Metering Collector ... 45
intended audience ... 17

L

license and software enablement ... 24

M

managing
Avaya OneCloud™ Subscription system state ... 126
migrating
perpetual licenses to subscription license ... 127
My Docs ... 153

N

No more mirrors to try
installation error ... 140

O

obtaining
Access key and Secret key ... 28
order type
features available ... 33
overview
Avaya OneCloud™ Subscription ... 18
Usage Metering ... 19

P

password reset parameters ... 65
ports ... 155
preparing
cold standby ... 137
prerequisites
for adding System Manager-provided WebLM ... 87
installing and using Usage Metering Collector ... 39
migrating from perpetual licenses to subscription license ... 126
sharing Experience Portal ... 120
prerequisites and process
for adding Application Enablement Services ... 94
for adding Avaya Aura® Messaging ... 99
for adding Avaya Call Management System ... 106
for adding Avaya Callback Assist ... 104
for adding Avaya IX™ Messaging ... 109
for adding Experience Portal Manager ... 95
for adding System Manager ... 102
purpose ... 9

R

re-registering
WebLM server ... 90
registering applications
Avaya Global Registration Tool ... 124
resetting
Usage Metering password ... 60
restoring
Usage Metering ... 132
Usage Metering after uninstallation ... 135
retrieving certificate
standalone Avaya WebLM ... 79

S

searching for content ... 153
secondary data center
recovery process ... 137
setting
concurrent sessions limit ... 70
time zone ... 44
sharing content ... 153
SNMP MIB file location ... 141
sort documents by last updated ... 153
support ... 154
supported browsers ... 20
supported UC and CC applications ... 30
system requirements ... 40

T

technical onboarding of applications
Avaya Global Registration Tool 123
testing
recovery process 138

U

uninstalling
Usage Metering Collector 134
unregistering
WebLM server 90
upgrade
application 128
upgrading
Usage Metering Collector 139
Usage Metering
alerts 146
backup 131
components 19
data not displayed 143
geo-redundancy 135
keep-alive parameters 72
restore 132
Usage Metering Collector
configuration checklist 48
default password policy 61
installation checklist 38
password policy parameters 63
required URLs 42
user management 58

V

verifying
operating system parameters 141
Usage Metering connectivity 141
verifying data collection
primary and secondary Usage Metering 136
viewing
alerts 146
audit log of user activity 143
certificates 80
online Help 152
recent logs 142
user login history 60

W

watch list 153
WebLM management 86