



Administering standalone Avaya WebLM

Release 10.1
Issue 5
July 2024

Notices

© 2026 Avaya LLC. All Rights Reserved.

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 INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in 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: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

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

Copyright

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](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](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 Inc.

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

Contents

Chapter 1: Introduction	7
Purpose	7
Change history	7
New in WebLM Release 10.1.2	7
Chapter 2: WebLM overview	10
Chapter 3: Getting started with WebLM	12
Logging on to the WebLM web console	12
Changing the WebLM password	12
Change Password field descriptions	13
Resetting the WebLM password through CLI	13
WebLM Home field descriptions	13
Installing a license file	14
Install license field descriptions	15
Licensed products	16
Viewing the license capacity and utilization of the product features	16
Viewing peak usage for a licensed product	17
Configure whitelist	19
Enterprise Licensing	21
Viewing the license capacity of the licensed features of a product	21
Viewing the connectivity status of the local WebLM servers	22
Validating connectivity to local WebLM servers for a product	23
Configuring enterprise licensing	23
Retrieving the local WebLM certificate from browser	27
Adding local WebLM certificate as trusted certificate in System Manager	27
Managing local WebLM	28
Usages	33
Allocations	38
Periodic status of the WebLM server	41
Migrating enterprise WebLM model to standard WebLM model	42
Uninstalling the license file	44
Uninstalling a license file	44
Server properties	44
Viewing the server properties	44
Setting the usage history count	45
Managing users	46
Adding a new user	46
Deleting the user	46
Editing the user password	46
Configuring the inactivity timeout for the user	47

Manage users field descriptions.....	47
WebLM Password Policy.....	48
Password history policy.....	48
Password strength policy.....	48
Configuring password policies.....	49
Password Policy field descriptions.....	49
WebLM command-line password policies.....	51
Metering Collector configuration overview.....	58
Metering Collector Configuration field descriptions.....	58
Deleting the metering collector configuration.....	59
Centralized subscription licensing.....	59
Centralized licensing.....	60
About centralized licensing.....	60
Enabling centralized licensing.....	60
Configure centralized licensing field descriptions.....	61
Adding an element instance and assigning the element instance to a license file.....	61
Editing an element instance and license file assignment.....	62
Deleting an element instance.....	63
Element instance field descriptions.....	63
Disabling centralized licensing.....	64
Uninstalling the Communication Manager 6.3.x, 7.x, and 8.x license file and installing the	
Communication Manager 10.1.x license file.....	64
Managing the WebLM Application server.....	65
Logging out of the WebLM server.....	65
Chapter 4: WebLM Certificate Management.....	66
Credential store and certificate management.....	66
Import CA certificate into WebLM client truststore.....	66
Toggling cipher suites for WebLM.....	67
Configuring the TLS version for WebLM.....	68
manageWebLMCertificate command.....	69
Viewing a WebLM certificate.....	69
Replacing a WebLM certificate with a third-party certificate.....	70
Regenerating a self-signed WebLM certificate	70
manageCACertificates command.....	71
Viewing a CA certificate from the WebLM truststore.....	71
Importing a CA certificate into the WebLM truststore.....	72
Deleting a CA certificate from the WebLM truststore.....	72
setWebLMClientAuth command.....	72
Displaying existing WebLM client certificate authentication configuration.....	73
Enabling WebLM client certificate authentication.....	73
Disabling WebLM client certificate authentication.....	74
Chapter 5: Troubleshooting standalone WebLM.....	75
Overview.....	75

Adopter application cannot communicate with WebLM Server.....	75
Adopter application cannot communicate with WebLM Server.....	75
WebLM launching errors.....	76
Launching of WebLM fails.....	76
Proposed solution 1.....	77
Proposed solution 2.....	77
Proposed solution 3.....	77
Proposed solution 4.....	78
Proposed solution 5.....	78
License file installation errors.....	78
Installation of license file on the WebLM server fails.....	78
Scenario 01.....	78
Proposed solution.....	79
Scenario 02.....	80
Proposed solution.....	80
Scenario 03.....	81
Proposed solution.....	81
Scenario 04.....	82
Proposed solution.....	83
Scenario 05.....	83
Proposed solution.....	84
WebLM password errors.....	84
WebLM password resetting.....	84
Proposed solution.....	85
Chapter 6: Avaya WebLM commands	86
WebLM CLI operations.....	86
Chapter 7: Resources	92
Avaya WebLM documentation.....	92
Finding documents on the Avaya Support website.....	92
Accessing the port matrix document.....	93
Avaya Documentation Center navigation.....	93
Training.....	94
Viewing Avaya Mentor videos.....	94
Support.....	95
Using the Avaya InSite Knowledge Base.....	95
Appendix A: Recommendations to select a WebLM configuration model	97
WebLM standard licensing model.....	97
WebLM enterprise licensing model.....	98
WebLM configuration model checklist.....	99

Chapter 1: Introduction

Purpose

This document provides procedures for configuring standalone Avaya WebLM.

The primary audience for this document is anyone who is involved with configuring, troubleshooting Avaya WebLM for licensing Avaya software products at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Change history

The following changes have been made to this document since the last issue:

Issue	Date	Summary of changes
5	July 2024	Updated the sections: • Enabling WebLM client certificate authentication on page 73 • WebLM CLI operations on page 86
4	April 2024	Updated the section Logging on to the WebLM web console on page 12
3	April 2024	• Updated the section Installing a license file on page 14 • Updated the sections Scenario 05 on page 83 and Proposed solution on page 84
2	January 2024	Updated the section WebLM CLI operations on page 86
1	February 2023	Release 10.1.2 document.

New in WebLM Release 10.1.2

WebLM Release 10.1.2 supports the following new features and enhancements:

Support of Avaya Aura® application OVA with SHA256 hash algorithm

From Release 10.1.2, Avaya Aura® applications support the SHA256 hash algorithm for OVAs.

Support of deployment and upgrade of OVA with SHA256 hash algorithm on Solution Deployment Manager

From Release 10.1.2, System Manager Solution Deployment Manager and Solution Deployment Manager Client support the deployment and upgrade of an application using the OVA with the SHA256 hash algorithm.

Support for TLS 1.3

From Release 10.1.2, WebLM supports TLS version 1.3.

Support of new CLI command for managing the password policies

From Release 10.1.2, WebLM supports the `setSecurityPolicy` command to manage password policies using the command-line interface (CLI). This command is only applicable for changing or setting up the password for a CLI user or a root user that you create during deployment.

Support of the new Password Policy page

From Release 10.1.2, you can configure the WebLM password history and strength policies on the Password Policy page.

If the password policy is enabled, WebLM also applies those password policies while changing the WebLM password on the Change Password page of the WebLM web console.

Support to manage the WebLM Application server

From Release 10.1.2, WebLM supports the following new commands:

- `weblmStart` to start the WebLM Application server.
- `weblmStatus` to check the status of the WebLM Application server.
- `weblmStop` to stop the WebLM Application server.
- `weblmRestart` to restart the WebLM Application server.

Configuration of the whitelist for client certificate identity

From Release 10.1.2, you can configure the whitelist to validate the client certificate identity for the installed product license.

Support for configuring the user inactivity timeout value

From Release 10.1.2, you can configure the inactivity timeout for the user, after which the WebLM web console times out. To configure, you can use the **User inactivity timeout (minutes)** field on the Manage Users page.

Support to manage WebLM certificates in the WebLM server keystore

From Release 10.1.2, WebLM supports the following new commands:

- `manageWebLMCertificate -display` to view the WebLM certificate that is stored in the WebLM server keystore.
- `manageWebLMCertificate -replace` to replace the WebLM certificate with a new third-party certificate.
- `manageWebLMCertificate -generateSelfSigned` to replace the existing certificate with a new self-signed server certificate.

Support to manage CA certificates in the WebLM truststore

From Release 10.1.2, WebLM supports the following new commands:

- **manageCACertificates -list** to display a CA certificate stored in the WebLM server truststore.
- **manageCACertificates -add** to import a CA certificate into the WebLM truststore.
- **manageCACertificates -remove** to delete a CA certificate from the WebLM truststore.

Support to manage WebLM client certificate authentication

From Release 10.1.2, WebLM supports the following new commands:

- **setWebLMClientAuth [1]** to display existing WebLM client certificate authentication configuration.
- **setWebLMClientAuth [2]** to enable WebLM client certificate authentication.
- **setWebLMClientAuth [3]** to disable WebLM client certificate authentication.

Chapter 2: WebLM overview

Avaya provides a Web-based License Manager (WebLM) to manage licenses of one or more Avaya software products for your organization. WebLM facilitates easy tracking of licenses. To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com>.

WebLM supports two configurations models:

- WebLM standard model. In this model, a single WebLM server supports one or more licensed products. The WebLM standard model supports the Standard License File (SLF) and Enterprise License File (ELF) types.
- WebLM enterprise model. This model includes multiple WebLM servers. One WebLM server acts as a master WebLM server and hosts the license file from PLDS. The remaining WebLM servers act as the local WebLM servers and host the allocation license files from the master WebLM server. You require an ELF to set up the WebLM enterprise model. PLDS generates license files that are SLFs or ELFs.

 Note:

The master and local WebLM servers must be deployed on the same major release. The master WebLM server must be on same or latest service pack than the local WebLM server resides on.

For example, if the local WebLM server is on Release 7.1, the master WebLM server must be on Release 7.1, 7.1.1, 7.1.2, or 7.1.3. The master WebLM server cannot be higher than Release 7.1.x.

You can purchase two products and choose the enterprise model of licensing for one product and the standard model of licensing for the other product. PLDS generates a separate license file for each product.

The license file is an SLF or ELF based on how the product is configured in PLDS. Verify the installation options that the product supports before you install the WebLM server. To configure the standard licensing, you can use an ELF or SLF. To configure enterprise licensing, you must have an ELF. After you install the license file on the WebLM server, a product with an ELF can have multiple instances of the WebLM server. However, a product with an SLF can have only one instance of the WebLM server.

The license file of a software product is in an XML format. The license file contains information regarding the product, the major release, the licensed features of the product, and the licensed capacities of each feature that you purchase. After you purchase a licensed Avaya software product,

you must activate the license file for the product in PLDS and install the license file on the WebLM server.

Chapter 3: Getting started with WebLM

Logging on to the WebLM web console

About this task

The WebLM web console is the main interface of Avaya WebLM. You must log on to the WebLM web console to perform any task. The WebLM home page displays the navigation menu that provides access to shared services to perform operations that WebLM supports.

Before you begin

Get a user account to log on to the WebLM web console. To create a new account, go to the Avaya Support website at <https://support.avaya.com>.

Procedure

1. On a web browser, type the WebLM URL: `https://<IP Address or Fully Qualified Domain Name>/WebLM` or `https://<IP Address or Fully Qualified Domain Name>/`.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Click **Log On**.

WebLM validates the credentials with the WebLM user account and displays the home page with the WebLM `<version_number>`. If the credentials fail, WebLM displays an error message and prompts you to reenter the credentials.

Changing the WebLM password

About this task

WebLM Release 10.1.2 supports password policies. If the password policy is enabled on the Password Policy page, the Change Password page displays the password policy rules.

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. At the top-right corner of the web page, click **Change Password**.

3. On the Password page, enter the required details.

For more information about the details, see “Change Password field descriptions”.

Change Password field descriptions

Name	Description
Current Password	The current password.
New Password	The new password.
Confirm Password	The new password for confirmation.

Button	Description
Submit	Saves the new password.

Resetting the WebLM password through CLI

About this task

Any CLI user who is part of the gcliuser and admin groups created during deployment can run the command to reset the WebLM password through CLI.

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type the `weblm_password` command and press `Enter`.
3. In **Enter new WebLM UI Admin Password**, type a new password.

The password must be 6-14 characters long.

4. In **Re-enter new WebLM UI Admin Password**, type the new password again.

WebLM successfully resets the password. You can log in to the WebLM UI with user 'admin' and the new password.

WebLM Home field descriptions

If the TLS version is set to TLS 1.0 or TLS 1.1, the WebLM Home page displays the following message:

```
Warning! TLSv1 or TLSv1.1 is enabled.
```

```
For increased security, it is recommended that the Minimum TLS Version  
be set to TLS 1.2 or higher if these protocol levels can be supported  
in your configuration.
```

You can view information about the products and associated license files installed on the WebLM server.

Name	Description
Product Name	The name of the product for which the license file is installed.
Product Version	The version of the product for which the license file is installed.
Type of License	The type of license file installed for the product. The options are: • solution (Avaya Subscription License) • standard • enterprise
Date of Installation	The date and time of installing the license file.
Active License Mode	The type of license file installed for the product.
License State	The status of the installed license file.
Avaya Subscription License Available	The availability status of the Avaya Subscription license.
Standard License Available	The availability status of the standard license.

Button	Description
Export All Licenses	Exports the licenses to the <code>/tmp/all_licenses.zip</code> file on the WebLM server.

Installing a license file

About this task

You can install a license file on the WebLM server. Use the Uninstall functionality to remove the license file from the WebLM server.

Licenses installed for WebLM Release 7.1 and later must support a SHA256 digital signature and 14-character host ID.

There is a limit of 50 licenses per WebLM server.

Note:

If you have a mix of Communication Manager Release 6.3.x, 7.x, 8.x, and 10.1.x software with Communication Manager 6.3.x, 7.x, 8.x, and 10.1.x license files, use the Communication Manager 10.1.x license file for all the Communication Manager Release software.

For more information, see [Uninstalling the Communication Manager 6.3.x, 7.x, and 8.x license file and installing the Communication Manager 10.1.x license file](#) on page 64.

Before you begin

- Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com>.
- Log on to the WebLM web console with administrator privilege credentials.
- For the standard license file, remove the older license file before you install the new file.

Note:

WebLM displays an error message if an older license file is still available.

For a centralized license file, the system automatically overwrites the older license file during installation.

For information about the license file installation errors while installing the license file, see *Administering standalone Avaya WebLM*.

Procedure

1. In the navigation pane, click **Install license**.
2. On the Install license page, click **Browse** and select the license file.
3. Read the terms and conditions, and click **Accept the License Terms & Conditions**.
4. Click **Install**.

WebLM displays a message on the successful installation of the license file. The installation of the license file might fail for reasons such as the following:

- The digital signature on the license file is invalid. If you get such an error, request PLDS to redeliver the license file.
- The current capacity use exceeds the capacity in the installed license.
- An acquired license does not cover a licensed feature or product.
- An over-installation of licenses. In this scenario, free the already acquired licenses and retry installing the new license file. You could also try uninstalling the existing installed license file and installing a new license file.

Related links

[Scenario 01](#) on page 78

Install license field descriptions

Name	Description
Enter license path	The complete path where the license file is saved.
Browse	The option to browse and select the license file.
Avaya Global License Terms & Conditions	Avaya license terms and conditions that the user must agree to continue the license file installation.

Button	Description
Install	Installs the product license file.

Licensed products

Viewing the license capacity and utilization of the product features

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

About this task

Use this procedure to view the license capacity and license utilization of a product for which you installed a license file.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View license capacity**.

Related links

[View License Capacity field descriptions](#) on page 16

View License Capacity field descriptions

Name	Description
License File Host IDs	The host ID of the license file.

The following fields are applicable for the Solution license:

Name	Description
Active License Mode	The type of license active on WebLM. The default value is Avaya Subscription . The WebLM server can have Avaya Subscription and Standard (Perpetual) licenses installed. However, at a time only one license can be active. These licenses are used while switching between two modes.
License State	The status of the Avaya Subscription license. The default value is Granted .

Table continues...

Name	Description
Avaya Subscription License Available	The availability status of the Avaya Subscription license on WebLM. The default value is Yes .
Standard License Available	The availability status of the standard license on WebLM. The default value is No .

Licensed Features

You can view the total number of feature licenses in the license file and the current usage of those licenses.

Name	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Expiration Date	The date on which the feature license expires.
Licensed capacity	The number of licenses for each licensed feature. WebLM fetches the number of feature licenses information from the license file. For the Solution license, the value is Metered .
Currently Used	The number of feature licenses that are currently in use by the licensed application. For features of type Uncounted, the column displays <i>Not counted</i> .

Acquired Licenses

The Acquired licenses table displays information about the licenses acquired by the licensed application. You can view the information in the table only if the licensed product has acquired feature licenses.

Name	Description
Feature	The feature keyword for each licensed feature that is currently acquired by a licensed application.
Acquired by	The name of the licensed application that has acquired the license.
Acquirer ID	The unique identifier of the licensed application that has acquired the license.
Count	The number of feature licenses that are currently acquired by the licensed application.

Viewing peak usage for a licensed product

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View peak usage**.

Related links

[View Peak Usage field descriptions](#) on page 18

View Peak Usage field descriptions

You can view information about the usage of feature licenses of a licensed application at different time intervals.

For the Solution license, the usage fields shows the number of used license file, but not the percentage (%) of usage.

Name	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Currently Allocated	The number of feature licenses purchased by the organization. For the Solution license, the value is Metered .
Usage: qty/%	The number of feature licenses for each licensed feature that a licensed application currently uses. The column also displays the percentage of usage. For example, if 50 feature licenses are available and five feature licenses are used by applications, the column displays 5/10%.
Peak Usage (today): qty	The highest number of feature licenses for each licensed feature used for the day.
Peak Usage (Last 7 days): qty/%	The highest number of feature licenses for each licensed feature used in the last seven days. For example, if the peak usage for a feature license in the past seven days was 25, and the number of available licenses during these seven days was 50, then the column displays 25/50%.
Peak Usage (Last 30 days): qty/%	The highest number of feature licenses for each licensed feature used in the past 30 days. For example, if the peak usage for a feature license in the past 30 days was 50, and the number of available licenses during these 30 days was 50, then the column displays 50/100%.
Time of Query	The date and time when the last usage query for WebLM was executed.
Status	The success or failure of the last usage query executed for the WebLM server.

Button	Description
Back	Cancels the action and returns to the previous page.

Configure whitelist

Adding the whitelist for client certificate identity

Before you begin

Install the license file on the WebLM server for the licensed product.

About this task

From WebLM Release 10.1.2, you can add the whitelist for the client certificate identity for a product you installed a license file. The whitelist must be a valid IP or hostname.

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, under **Licensed Products**, click the required product.
3. Click **Configure white list**.
4. In Whitelist for client certificate identity, click **Add**.
5. In **Client certificate identity**, type IP Address or hostname.
6. Click **Submit**.

WebLM adds the whitelist entry.

Related links

[Enabling WebLM client certificate authentication](#) on page 73

Editing the whitelist for client certificate identity

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, under **Licensed Products**, click the required product.
3. Click **Configure white list**.
4. In Whitelist for client certificate identity, select a whitelist entry, and click **Edit**.
5. In **Client certificate identity**, edit the IP Address or hostname.
6. Click **Submit**.

Importing the whitelist for client certificate identity

Before you begin

- Install the license file on the WebLM server for the licensed product.
- Create and save a `.csv` file with the whitelist details on your local computer.

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, under **Licensed Products**, click the required product.

3. Click **Configure white list**.
4. In Whitelist for client certificate identity, click **Import**.
5. In **Enter CSV file path**, click **Choose File** and do the following:

- a. Select the `.csv` file from your local computer.

For example, `<ClientCertificateIdentity_Sample_Product>.csv`

- b. Click **Open**.

6. Click **Submit**.

WebLM imports the whitelist entries and displays the entries in the Whitelist for client certificate identity section.

Exporting the whitelist for client certificate identity

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, under **Licensed Products**, click the required product.
3. Click **Configure white list**.
4. In Whitelist for client certificate identity, click **Export**.

WebLM exports the configured whitelist entries in a CSV format file.

For example, `ClientCertificateIdentity_Sample_Product.csv`

Deleting the whitelist

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, under **Licensed Products**, click the required product.
3. Click **Configure white list**.
4. In Whitelist for client certificate identity, select one or more whitelist entry, and click **Delete**.

WebLM displays the following confirmation message:

Are you sure to delete the selected identities?

5. Click **OK**.

WebLM deletes the selected whitelist entries.

Enabling the whitelist validation for client certificate identity

Before you begin

Add the whitelist entries for the client certificate identity for a product you installed a license file.

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, under **Licensed Products**, click the required product.
3. Click **Configure white list**.
4. Click **Enable**.

WebLM enables the validation of the whitelist for the client certificate identity.

Disabling the whitelist validation for client certificate identity**Procedure**

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, under **Licensed Products**, click the required product.
3. Click **Configure white list**.
4. Click **Disable**.

WebLM disables the validation of the whitelist for the client certificate identity.

Enterprise Licensing

Viewing the license capacity of the licensed features of a product**Before you begin**

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View by feature**.

Related links

[View by feature field descriptions](#) on page 21

View by feature field descriptions

Name	Description
License File Host IDs	The host ID of the license file.

Name	Description
Feature (License Keyword)	The display name and the keyword for the licensed features of the product.

Table continues...

Name	Description
License Capacity	The total number of feature licenses that the organization purchases for each feature.
Currently available	The number of floating licenses of each feature that is currently available with the master WebLM server. The feature licenses that are not allocated to any local WebLM server are known as floating licenses.  Note: For uncounted features, this column displays Not counted.

Related links

[Viewing the license capacity of the licensed features of a product](#) on page 21

Viewing the connectivity status of the local WebLM servers

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View by local WebLM**.

The page displays the connectivity status of the local WebLM servers.

Related links

[View by local WebLM field descriptions](#) on page 22

View by local WebLM field descriptions

Use this page to view the information related to local WebLM servers of a product.

Name	Description
Local WebLM name	Specifies the name of the local WebLM server.
IP address	Specifies the IP address of the local WebLM server.
Last contacted	Specifies the date and time when the local WebLM server was last contacted.
Status	Lists the success or failure of the last connection request to each local WebLM server.

Related links

[Viewing the connectivity status of the local WebLM servers](#) on page 22

Validating connectivity to local WebLM servers for a product

Procedure

1. In the left navigation pane, click **Licensed Products** from the enterprise product name.
2. In the left navigation pane, click **Local WebLM Configuration**.
3. On the Local WebLM Configuration: View Local WebLMs page, select the local WebLM servers you want to validate for connectivity.
4. Click **Validate Connectivity** to query the selected local WebLM servers.

Result

The status column on the Local WebLM Configuration: View Local WebLMs page of the selected WebLM servers displays whether the connection request made to the local WebLM server is successful or not.

View Local WebLMs field descriptions

Use this page to validate the local WebLM server connection. To validate the connection, the master WebLM server tries to connect to the specified local WebLM server.

* Note:

To validate the connectivity of a local WebLM server, the local WebLM server must be already added for the product.

Name	Description
Local WebLM Name	The name of the local WebLM server.
IP Address	IP address of the local WebLM server.
Last Contacted	Date and time when the local WebLM server was last contacted.
Status	Lists the success or failure of the last connection request to each local WebLM server.

Button	Description
Validate Connectivity	Validates the connectivity of the selected WebLM server.
Check All	Selects all the local WebLM server.
Clear All	Clears the selections of local WebLM servers.

Configuring enterprise licensing

Before you begin

- Log on to WebLM Home.
- Install the enterprise license file on the WebLM server for the product.

To verify the license file for a product, in the left navigation pane, click **Licensed products** and select the product. The content pane displays the product name, System Identification number (SID), and the license file type installed for the product at the top of the page.

 Note:

System Manager WebLM can be configured as master WebLM but cannot be configured as local WebLM to an external WebLM.

Standalone WebLM OVA-based deployment can be configured as master WebLM or local WebLM.

No other WebLM flavor can be configured as master WebLM.

	Enterprise Master WebLM	Enterprise Local WebLM
System Manager WebLM	Yes	No
Standalone WebLM OVA-based deployment	Yes	Yes
Other WebLM flavors	No	Yes

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. In the navigation pane, click **Enterprise configuration**.
3. On the Enterprise Configuration page, enter the appropriate information in the fields.
For more information, see “Enterprise Usage field descriptions”.
To successfully set up and configure the master WebLM server, enter valid information in the mandatory fields that are marked with a red asterisk.
4. In the **Master WebLM Configuration** section, enter the name, description, and IP address of the master WebLM server.
5. In the **Default Periodic Operation Settings** section, enter the retry count and the retry interval in minutes for the periodic operations.
6. In the **SMTP Server settings** section, enter the name of the SMTP server.
7. In the **E-mail notification settings for periodic operation** section, perform the following:
 - a. Set the **E-mail notification** to **On**.
 - b. In the **E-mail address** field, enter an email address.
 - c. To add the email address to the list of recipients for the WebLM server to send email notifications, click **Add To List**.
8. In the **Default Periodic License Allocation Schedule** section, select the day and time for periodic license allocations.
The values you enter in this section remain as the default setting for periodic allocation for all local WebLM servers in the enterprise.
9. In the **Default Periodic Usage Query Schedule** section, select the day and time of the query for periodic usage.
The values you enter in this section remain as the default setting for periodic usage for all local WebLM servers in the enterprise.

 Note:

For any periodic operations, you must perform the manual allocation at least one time.

10. Click **Submit**.

The system validates the information. The system displays the host ID in the **Host ID** field. The host ID is the host ID of the computer where you installed the WebLM server.

Related links

[Enterprise Configuration field descriptions](#) on page 25

Enterprise Configuration field descriptions

Use this page to specify the master WebLM server settings and the default settings for the periodic operations of the server. The settings you specify in the Enterprise Configuration Web page applies to the entire enterprise unless you override the setting while you add a local WebLM.

The master WebLM server uses the settings of the periodic operations to query itself and generate the usage report for licenses.

Master WebLM Configuration

Name	Description
Name	Specifies the name of the WebLM server.
Description	Provides a brief description of the server.
IP address	Specifies the IP address of the WebLM server.
Host ID	Specifies the host ID of the computer where you installed the WebLM server. You cannot edit the Host ID field.

Default periodic operation settings

Name	Description
Retry count	Specifies the number of times a master WebLM server must try to connect to a local WebLM server for a periodic operation after a connection failure. For example, set the count to 2. The master WebLM server makes an initial unsuccessful attempt to connect to a local WebLM server. The master WebLM server makes two more attempts to connect to the local WebLM server.
Retry interval	Specifies the duration in minutes, within which the retry count specified in the Retry count field must be carried out. For example, suppose the Retry count is 2 and the Retry interval is 10 minutes. If the attempt to connect to the server fails, the master WebLM server makes two attempts in 10 minutes to connect to the local WebLM server.

SMTP Server Settings

Name	Description
Server name	Specifies the name of the SMTP server.

E-mail notification settings for periodic operation

Name	Description
E-mail notification	Specifies the e-mail notification. The notification options are: - On: Sends an e-mail notification to the administrator if the periodic operations fail. - Off: Does not send an e-mail notification to the administrator if the periodic operations fail.
E-mail address	Specifies the e-mail address to which the WebLM application sends the e-mail notification if the periodic operations fail to execute.  Note: Click Add To List to add the e-mail address in the list of recipients who must receive the e-mail notification of the periodic operation status.
E-mail addresses	Provides the list of e-mail addresses to which the WebLM application sends the e-mail notifications.
Add To List	Adds the e-mail address that you enter in the E-mail address field to the list of recipients who must receive the e-mail notification of the periodic operation status.
Remove Selected	Removes the selected e-mail address from the E-mail addresses field.

Default Periodic License Allocation Schedule

Name	Description
Day	The day of the week on which the master WebLM server must send the ALF (Allocation license file) again to the local WebLM server.
Time	The time of the day specified in the Day field when master WebLM must send the ALF again to the local WebLM server.

Default Periodic Usage Query Schedule

Name	Description
Day	The day of the week on which the master WebLM server must query local WebLM servers for usage reports.
Time	The time of the day you specify in the Day field when the master WebLM server must query local WebLM servers for usage reports.

Button	Description
Submit	Saves the enterprise configuration.
Reset	Resets the values in the fields to the values you previously saved.

Related links

[Configuring enterprise licensing](#) on page 23

Retrieving the local WebLM certificate from browser

About this task

Use this procedure to retrieve the local WebLM certificate from the Firefox browser.

Procedure

1. On the web browser, type the local WebLM server URL, `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**.
6. On the Certificate dialog box, do the following:
 - a. Click the **Details** tab.
 - b. Click **Export**.
 - c. Save the certificate to your local computer.

Adding local WebLM certificate as trusted certificate in System Manager

About this task

To add standalone WebLM as local WebLM in System Manager (master WebLM), you must add local WebLM certificate to the truststore of System Manager.

Before you begin

Download the local WebLM certificate using the browser.

Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, select one or more elements, and click **More Actions > Manage Trusted Certificates**.
3. On the Manage Elements page, select System Manager, and click **More Actions > Manage Trusted Certificates**.
4. On the Manage Trusted Certificates page, click **Add**.
5. On the Add Trusted Certificates page, in **Select Store Type to add trusted certificate**, select the store type as **TM_INBOUND_TLS**.
6. Click **Import from file**.

7. Type the file name or click **Browse** to select a file.

 Note:

System Manager validates the file type. If you provide an invalid file type, the system displays an error message.

8. Click **Retrieve Certificate**.
9. Click **Commit**.
10. To restart the Application server, type `smgr restart`.

During a restart the System Manager web console will be unavailable for 10-15 minutes.

Managing local WebLM

Adding a local WebLM server

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the enterprise license file.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Local WebLM Configuration > Add local WebLM**.
3. On the Local WebLM Configuration: Add local WebLM page, enter the appropriate information.

To successfully set up and configure the local WebLM server, fields that are marked with a red asterisk (*) are mandatory.

For detailed descriptions of the fields, see “Add local WebLM field descriptions”.
4. In the **Local WebLM Configuration** section, enter the name, description, IP address, and port of the local WebLM server.
5. Select a protocol for the master WebLM server to communicate with the local WebLM server.
6. In the **Periodic license allocation schedule** section, select the day and time for periodic license allocations.
7. In the **Periodic usage query schedule** section, select the day and time of the query for periodic usage.
8. Click **Configure and validate**.

The system validates the information. If the information is valid, the system displays the host ID of the computer where the server is installed in the **Host ID** field.

Related links

[Add local WebLM field descriptions](#) on page 29

Add local WebLM field descriptions

Local WebLM configuration

Name	Description
Name	The name of the server.
Description	A brief description of the server.
IP Address	A unique IP address of the server. If you enter an IP address that is already configured for a local WebLM server, the system displays the message: <code>IP Address is being duplicated</code> .
Protocol	The protocol scheme over which the master WebLM server communicates with the local WebLM server.  Note: If the local WebLM server that you add is a standalone WebLM server in Virtualized Environment, use HTTPS. You cannot use HTTP for communication with the standalone WebLM server in Virtualized Environment.
Port	The port number on which the master WebLM server communicates with the local WebLM server in the specified protocol scheme.
Host ID	The host ID of the computer on which you installed the server. You cannot edit the Host ID field.

Periodic License Allocation schedule

Name	Description
Day	The day of the week on which the master WebLM server must send the ALFs again to the local WebLM server. By default, the system displays the settings specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.
Time	The time of the day specified in the Day field when the master WebLM server must send the ALFs again to the local WebLM server. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.

Periodic Usage Query schedule

Name	Description
Day	The day of the week on which the master WebLM server must query local WebLM servers for usage reports. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.
Time	The time of the day specified in the Day field when the master WebLM server must query local WebLM servers for usage reports. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.

Button	Description
Configure and validate	Configures the local WebLM server and validates the creation of the local WebLM server.
Back	Returns to the View local WebLMs page.

Removing a local WebLM server

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the enterprise license file.
- Add at least one local WebLM server.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Local WebLM Configuration > Delete local WebLM**.
3. On the Local WebLM Configuration: Delete local WebLM page, select the local WebLM server that you want to delete.
4. Click **Delete**.

Note:

The system displays a warning message before removing the local WebLM server from the master WebLM server.

5. Click **OK**.

Related links

[Delete local WebLM field descriptions](#) on page 31

Modifying a local WebLM server configuration

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the enterprise license file.
- Add at least one local WebLM server.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Local WebLM Configuration > Modify local WebLM**.
3. On the Local WebLM Configuration: Modify local WebLM page, select the local WebLM server that you require to configure.
4. Click **Modify**.

The system displays another Local WebLM Configuration: Modify local WebLM page with a different set of WebLM configuration fields.

5. Modify the information in the following fields:
 - In the **Local WebLM configuration** section, **Name**, **Description**, **Protocol**, and **Port**
 - In the **Periodic License Allocation schedule** section, **Day** and **Time**
 - In the **Periodic Usage Query schedule** section, **Day** and **Time**
6. Click **Modify**.

The system saves your changes.

Related links

[Local WebLM configuration - modify field descriptions](#) on page 31

[Modify local WebLM field descriptions](#) on page 32

Delete local WebLM field descriptions

Use this page to delete a local WebLM server.

Name	Description
Local WebLM name	The name of the local WebLM server.
IP address	The IP Address of the local WebLM server.
check box	Use to select the local WebLM servers that you require to delete.

Button	Description
Delete	Removes the local WebLM server you selected.
Reset	Clears the selection of the local WebLM servers.

Local WebLM configuration - modify field descriptions

Use this page to select the local WebLM server whose information you want to modify.

Name	Description
Local WebLM name	The name of the local WebLM server.
IP address	The IP address of the server.
Select	Select the local WebLM server you want to modify.

Button	Description
Modify	Saves the local WebLM configuration changes. * Note: The system opens another Modify Local WebLM page with the fields you must modify.
Reset	Clears the selection of the local WebLM servers.

Modify local WebLM field descriptions

Use this page to modify the information of a local WebLM server.

Local WebLM configuration

Name	Description
Name	Specifies the name of the server.
Description	Displays a brief description of the server.
IP Address	Specifies the IP address of the server. * Note: You cannot modify the information in the IP address field.
Protocol	Specifies the protocol scheme over which the master WebLM server listens to the local WebLM server. * Note: If the local WebLM server that you add is a standalone WebLM server in Virtualized Environment, use HTTPS. You cannot use HTTP for communication with the standalone WebLM server in Virtualized Environment.
Port	Specifies the port number on which the master WebLM server listens to the local WebLM server in the specified protocol scheme.
Host ID	Specifies the host ID of the computer where you installed the server. * Note: You cannot modify the information in the Host ID field.

Periodic License Allocation schedule

Name	Description
Day	Specifies the day of the week on which the master WebLM server must send the ALFs again to the local WebLM server.
Time	Specifies the time of the day you entered in the Day field when the master WebLM server must send the ALFs again to the local WebLM server.

Periodic Usage Query schedule

Name	Description
Day	Specifies the day of the week on which the master WebLM server must query the local WebLM servers for usage reports.
Time	Specifies the time of the day you entered in the Day field when the master WebLM server must query the local WebLM servers for usage reports.

Button	Description
Modify	Navigates to the Modify Local WebLM page for the local WebLM server you select.
Back	Discards the configuration changes and returns to the Modify local WebLM page.

Usages

Viewing usage summary

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, in **Licensed products**, click the required product.
3. Click **Usages**.

The system displays the Usage Summary page.

Related links

[Usage Summary field descriptions](#) on page 35

Viewing usage by WebLM

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Usages > Usage by WebLM**.

The system displays the Usages: Usage by WebLM page.

3. In the **Select WebLM** field, select the master or local WebLM server.
4. Click **Query System**.

Related links

[Usage by WebLM field descriptions](#) on page 35

Viewing enterprise usage of a license feature

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Usages > Enterprise Usage**.

The system displays the Usages: Enterprise Usage page.

3. In the **Select Feature (License Keyword)** field, select the licensed feature.

The page displays the usage of the licensed feature for the master WebLM server and the local WebLM servers.

Related links

[Enterprise Usage field descriptions](#) on page 36

Querying usage of feature licenses for master and local WebLM servers

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Usages > Query Usage**.

The system displays the Usages: Query Usage page.

3. To view the usage details by feature licenses of a server, select the master or local WebLM server.
4. Click **Query Usage**.

If you select all WebLM servers or click **Check All** and click **Query usage**, the system displays the progress of the query request.

Result

If you select one local WebLM server, the Usages: Usage by WebLM page displays the details of the local WebLM server you selected.

Related links

[Query Usage field descriptions](#) on page 37

Usage Summary field descriptions

Use this page to view the usage summary for a master WebLM server, a local WebLM server, or all the WebLM servers of the product.

Name	Description
WebLM Name	Displays the names of the master WebLM server and local WebLM servers of the product.
IP address	Specifies the IP address of the master WebLM server and local WebLM servers of the product.
Time of Query	Specifies the date and time when the system executed the last usage query for the WebLM server. If the status of the last usage query is Failed , this column also displays the date and time of the usage query that was last successful.
Status	Specifies the success or failure status of the last usage query that the system executed for each WebLM server. The Status column of a WebLM server remains blank if the server is not queried even once for feature license usage. The usage query can be a periodic usage query or a nonperiodic usage query.

Related links

[Viewing usage summary](#) on page 33

Usage by WebLM field descriptions

Use this page to query the feature license usage by the master and local WebLM servers.

Name	Description
Select WebLM	The master and local WebLM servers for which you can view the usage.
Feature (License Keyword)	The name and keyword of the counted features of the product.
Currently Allocated	The number of feature licenses for each feature that the system currently allocates to the selected WebLM server. For the master WebLM server of the product, this column lists the floating licenses available with the server.
Usage: qty/%	The number of feature licenses for each feature that the licensed applications currently use from the allocated feature licenses. The column also displays the percentage of usage. For example, if 50 feature licenses are allocated and applications use five feature licenses, this column displays 5/10%.

Table continues...

Name	Description
Peak Usage (last 7 days): qty/%	The highest number of feature licenses for each feature that the applications use in the past seven days. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days was 25 and 50 feature licenses were available during the peak usage calculation, the column displays 25/50%.
Peak Usage (last 30 days): qty/%	The highest number of feature licenses for each feature that the applications use in the past 30 days. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days was 50 and 50 feature licenses were available during the peak usage calculation, the column displays 50/100%.
Time of Query	The date and time when the system executed the usage query for the WebLM server you select.
Status	The success or failure of the last usage query process executed for each WebLM server. The Status column remains blank if the server is queried even once for feature license usage. The usage query can be a periodic usage query or a nonperiodic usage query.

Button	Description
Query System	Queries the selected WebLM server for the feature license usage.

Related links

[Viewing usage by WebLM](#) on page 33

Enterprise Usage field descriptions

You can view the feature license usage of all WebLM servers for the selected feature.

Name	Description
Select Feature (License Keyword)	Specifies the license features for which you can view the license usage.
License capacity	Specifies the total number of feature licenses the organization purchases for each feature.
Available	Lists the number of licenses currently available with the master WebLM server.
WebLM Name	Specifies the names of the WebLM servers of the product.
Currently Allocated	Specifies the number of feature licenses that the system currently allocates to the WebLM servers for the selected feature.

Table continues...

Name	Description
Usage qty/%	Specifies the number of feature licenses that the licensed applications currently use, from the allocated feature licenses for the selected feature. The column also displays the percentage of usage. For example, if 50 is the allocated feature licenses and 5 feature licenses have been used by the applications, this column displays 5/10%.
Peak Usage (last 7 days): qty/%	Specifies the highest number of feature licenses that applications use in the past seven days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days is 25 and the feature licenses those were available during the peak usage calculation is 50, the column displays 25/50%.
Peak Usage (last 30 days): qty/%	Specifies the highest number of feature licenses that applications use in the past 30 days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days is 50 and the feature licenses those were available during the peak usage calculation is 50, the column displays 50/100%.
Time of Query	Specifies the date and time when the system executes the usage query for the selected feature.
Status	Specifies the status of the last usage query process that the system executes for each WebLM server. The status can be <i>Success</i> or <i>Failure</i> .

Related links

[Viewing enterprise usage of a license feature](#) on page 34

Query Usage field descriptions

Use this page to query the master WebLM server, a local WebLM server, or all the WebLM servers of the product for the feature license usage report.

Name	Description
WebLM Name	The names of the master and the local WebLM servers of the product as links. To view the feature license usage of a server, select the name of the required server in the WebLM Name column.  Note: If the specified WebLM server is not queried even once for feature license usage, the table on the Usage by WebLM page remains blank.
IP address	The IP address of the master WebLM server and the local WebLM servers of the product.

Table continues...

Name	Description
Time of Query	The date and time when the system executes the last usage query for the WebLM server. If the status of the last usage query is Failed, the Time of Query column displays the date and time of the usage query that was last successful.  Note: If the server does not receive a query request even once for feature license usage, the Time of Query column of a WebLM server remains blank.
Status	The success or failure of the last usage query that the system executes for each WebLM server. If the server does not receive a query request even once for feature license usage, the Status column of a WebLM server remains blank. The usage query can be a periodic usage query or a nonperiodic usage query.
Select Check box	Use to select the WebLM server for which you require to determine the usage query.

Button	Description
Check All	Selects all the WebLM servers.
Clear All	Clears the selections for all the WebLM servers.
Query Usage	Queries the WebLM servers of the product you select for their feature license usage report.

Related links

[Querying usage of feature licenses for master and local WebLM servers](#) on page 34

Allocations

Viewing allocations by features

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Allocations > View by feature**.

The system displays the Allocations: View by Feature page.

Related links

[Allocations by Features field descriptions](#) on page 39

Viewing allocations by the local WebLM server

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Allocations > View by local WebLM**.
The system displays the Allocations: View by Local WebLM page.
3. In the **Select Local WebLM** field, select the local WebLM server.

Result

The page displays the allocation details for the local WebLM server you select.

Related links

[Allocations by Local WebLM field descriptions](#) on page 40

Changing allocations of licensed features for a local WebLM server

Use this functionality to change the license allocations of a feature that resides on a local WebLM server for the product.

Procedure

1. Log in to the master WebLM server.
2. In the navigation pane, in **Licensed products**, click the required product.
3. Click **Allocations > Change allocations**.
The system displays the Allocations: Change Allocations page.
4. In the **New Allocation** column, enter the number of licenses you require to allocate for the feature that resides on a local WebLM server.
5. Click **Submit Allocations**.

Related links

[Change Allocations field descriptions](#) on page 41

Allocations by Features field descriptions

Use this page to view the feature license allocation information for each counted type feature of the product.

Name	Description
Feature (License Keyword)	Specifies the name and license keyword of the counted features of the product.

Table continues...

Name	Description
Local WebLM Name	Specifies the name of the local WebLM servers of the product. By default, this column is blank. The system displays the names of the local WebLM servers only when you select the arrow head in the Feature (License Keyword) column. If a local WebLM server does not exist for the product, the Local WebLM Name column remains blank for all the licensed features.
IP address	Specifies the IP addresses of the local WebLM servers of the product. By default, this column is blank. The system displays the IP address of the local WebLM servers only when you select the arrow-head in the Feature (License Keyword) column. If a local WebLM server does not exist for the product, the IP address column remains blank for all the licensed features.
License Capacity	Specifies the total number of feature licenses purchased by the organization for the respective feature.
Currently Allocated	Specifies the total number of feature licenses of the respective feature that the system allocated to the local WebLM servers of the product. If a licensed feature is not allocated to any local WebLM server, the system displays <i>zero</i> in the Currently Allocated column for the licensed feature.
Available	Lists the number of floating licenses of the respective feature that is currently available with the master WebLM server.

 Note:

To view the information about the number of feature licenses of a feature that the system allocates to each local WebLM server, click the arrow-head beside the name of the required feature. The system displays new rows below the feature row with the feature license allocation information for each local WebLM server to which the feature is allocated.

Allocations by Local WebLM field descriptions

You can view the feature license allocation information by local WebLM.

Name	Description
Select Local WebLM	Specifies the local WebLM servers for which you can view the feature license allocation information.
Last Allocation	Specifies the date and time when feature licenses were last allocated to the local WebLM server you select.
Status	Specifies the success or failure status of the last license allocation process that the system executes for the local WebLM server you select. The allocation process can be a periodic allocation process or a nonperiodic allocation process. If the status of the last license allocation process is <i>Failed</i> , and if the status of a previous license allocation process for the server is <i>Success</i> , the system displays the date and time of the last license allocation process that was successful in the Last Allocation field.

Table continues...

Name	Description
Feature (License Keyword)	Specifies the name and license keyword of the counted features that the system allocates to the local WebLM server.
License Capacity	Specifies the total number of feature licenses the organization purchases for each feature.
Currently Allocated	Specifies the total number of feature licenses of each feature that the system allocates to the local WebLM server.
Available	Lists the number of licenses currently available on the master WebLM server for allocation to local WebLM servers.

Change Allocations field descriptions

Use this page to change current feature license allocation information for each local WebLM server of a product.

Name	Description
Feature (License Keyword)	The name and license keyword of the counted features that the system allocates to the local WebLM server you select.
Local WebLM Name	The name of the local WebLM server.
IP address	The IP addresses of the local WebLM servers of the product.
License Capacity	The total number of feature licenses that the organization purchases for each feature.
Currently Allocated	The total number of feature licenses of each feature that the system allocates to the local WebLM server you select.
Currently Used	The total number of feature licenses of each feature that the product uses.
Available	The number of floating licenses of each feature that is currently available with the local WebLM server.
New Allocation	The number of new licenses that the system allocates to a local WebLM server.

Button	Description
Submit Allocations	Allocates the number of feature licenses that you specify in the New Allocation field to the corresponding local WebLM servers.
Reset	Resets the values that you specify in the New Allocation field to the previously saved value.

Periodic status of the WebLM server

Viewing the periodic status of the master and local WebLM servers

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Periodic status**.

The system displays the Periodic Status page.

Periodic Status field descriptions

Use the Periodic Status option to view the status of periodic operations such as the periodic allocation of the feature licenses to the local WebLM server and querying of the local WebLM server for usage report.

Periodic Allocation

Name	Description
Local WebLM Name	Specifies the name of the local WebLM server of a product.
IP Address	Specifies the IP addresses of all the local WebLM servers of the product.
Last Allocation	Displays the date and time when the system executed the last periodic license allocation process for each local WebLM server. If the status of the last periodic license allocation process is Failed , the Last Allocation column displays the date and time of the periodic license allocation process that was last successful.
Status	Displays the success or failure status of the last periodic license allocation process that the system executed for each local WebLM server.

Periodic Usage

Name	Description
WebLM Name	Displays the name of the master WebLM server and local WebLM servers of a product.
IP Address	Displays the IP addresses of the master and local WebLM servers of a product.
Last Usage Query	Displays the date and time when the system executed the last periodic usage query for each WebLM server. If the status of the last periodic usage query is Failed , the Last Usage Query column also displays the date and time of the periodic usage query that was last successful.
Status	Displays the success or failure status of the last periodic usage query that the system executed for each WebLM server. If the server is not queried even once for feature license usage, the Status column of a WebLM server remains blank.

Migrating enterprise WebLM model to standard WebLM model

About this task

Use this procedure to migrate:

- Specific local WebLM to standard WebLM model

- All local WebLM servers and master WebLM server to standard WebLM server

Before you begin

1. Free all the licenses acquired from local WebLM and master WebLM for the particular Enterprise License product.
2. During the migration, ensure that the product does not acquire licenses from local WebLM and master WebLM.

Procedure

1. Log on to the master WebLM server.
2. In the navigation pane, in **Licensed products**, click the required product.
3. Click **Local WebLM Configuration > Delete local WebLM**.
4. On the Local WebLM Configuration: Delete local WebLM page, select the local WebLM server that you want to delete.
5. Click **Delete**.

The system displays a warning message before removing the local WebLM server from the master WebLM server.

6. Click **OK**.

This concludes the migration of a specific local WebLM to the standard WebLM model.

To migrate all local WebLM servers and master WebLM server to standard WebLM server, continue the next steps.

7. Delete all configured local WebLM servers by using Step 2 through Step 6.
8. Disable configured email notifications by using the following:
 - a. In the navigation pane, click **Enterprise configuration**.
 - b. In E-mail notification settings for periodic operation, set **E-mail notification** to **Off**.
 - c. Click **Submit**.
9. **(Optional)** Uninstall the enterprise license by using the following:
 - a. In the navigation pane, click **Uninstall license**.
 - b. On the Uninstall license page, select the required license file.
 - c. Click **Uninstall**.
 - d. On the Uninstall License Confirmation page, click **Uninstall**.

Result

You can now use Master WebLM and Local WebLM as independent Standard WebLM.

Related links

[Delete local WebLM field descriptions](#) on page 31

[Enterprise Configuration field descriptions](#) on page 25

[Uninstall license field descriptions](#) on page 44

Uninstalling the license file

Uninstalling a license file

Procedure

1. In the navigation pane, click **Uninstall license**.
2. On the Uninstall license page, select the required license file.
3. Click **Uninstall**.
4. On the Uninstall License Confirmation page, click **Uninstall**.

If you do not have permission to uninstall the selected license file, the system only displays the **Cancel** button.

Related links

[Uninstall license field descriptions](#) on page 44

Uninstall license field descriptions

Use this page to remove a license file from the WebLM server for a licensed product. The **Allocation Table License Files** table displays the ALF files. You cannot uninstall the ALF files.

Name	Description
License Host Name	The WebLM server where the license files are installed.
Host ID	The host ID of the license file.
Products	The products for which licenses are installed on the WebLM server.
SID	The System ID of the license file.
Select Check box	Use to select the license files that you require to remove from the WebLM server. You cannot uninstall the ALF license files.

Button	Description
Uninstall	Removes the selected license files from the WebLM server.

Server properties

Viewing the server properties

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

In the left navigation pane, click **Server properties**.

* Note:

The host ID specified in PLDS is embedded in the license file. You can install the license file only if the host ID of the server that hosts WebLM matches the host ID in the license file. Therefore, when you request for a license file, specify the correct host ID of the server that hosts WebLM.

Related links

[Server Properties field descriptions](#) on page 45

Server Properties field descriptions

Server Host ID

Name	Description
Primary Host ID	The MAC address of the server. For non-VMware deployments, the primary host ID is the MAC address of the server. For VMWare deployments, the primary host ID is a 14 character combination of the IP address and the UUID of the system. You must use the host ID to generate licenses which you later install on the current instance of the WebLM server.

Setting the usage history count

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the left navigation pane, click **Server properties**.
2. In the **Usage history count** section, set the **Count** from the list.
3. Click **Submit**.

The **Count** specifies the number of usage query results that the server maintains.

* Note:

You can view the **Usage history count** section only if you install at least one enterprise license file in the WebLM server.

Managing users

Adding a new user

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the left navigation pane, click **Manage users**.
2. Click **New**.
3. On the New User page, type the appropriate values in the **User Name**, **Password**, and **Confirm Password** fields.
4. Click **Add**.

Related links

[Manage users field descriptions](#) on page 47

Deleting the user

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. On the left navigation pane, click **Manage users**.
2. On the Manage Users page, select the users you require to delete.
3. Click **Delete**.
4. To delete the users, on the confirmation dialog box, click **OK**.

Related links

[Manage users field descriptions](#) on page 47

Editing the user password

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the left navigation pane, click **Manage users**.
2. On the Manage Users page, select the user you require to modify.
3. Click **Edit**.
4. In the **New Password** field, type a new password.

5. In the **Confirm Password** field, type the new password again.
6. Click **Change**.

 Note:

You cannot edit the user name from the Manage Users page.

Related links

[Manage users field descriptions](#) on page 47

Configuring the inactivity timeout for the user

About this task

From WebLM Release 10.1.2, you can configure the inactivity timeout for the user after which the WebLM web console times out.

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, click **Manage users**.
3. On the Manage Users page, in **User inactivity timeout (minutes)**, type the inactivity timeout value in minutes for the user after which the WebLM web console times out.

By default, the duration is set to 10 minutes.

4. Click **Save**.

When the inactivity timeout value is left by a minute, WebLM displays a message on the top-right corner of the WebLM web console.

For example, Your session is about to expire in <54>s. Click here to extend.

- If you click the Click here to extend link, WebLM extends the timeout duration by the value configured in the **User inactivity timeout (minutes)** field.
- If you do not click the Click here to extend link, WebLM web console times out and displays the login page with the following message:

Your session has been invalidated. Log in to WebLM again.

Manage users field descriptions

Name	Description
User inactivity timeout (minutes)	The time for which the user is inactive. After the timeout value expires, WebLM logs out the user. By default, the duration is set to 10 minutes. The minimum duration that you can set for timeout is 1 minute.

Button	Description
Save	Saves the timeout value for the WebLM user.

Name	Description
User Name	The username of the admin or non-admin WebLM user.
Reset Password	Specifies whether the login password has changed at least once after creating the user ID. The Reset Password column displays true for user IDs whose password is not changed once after the creation of the ID. The column displays false for user IDs whose login password is changed at least once.

Button	Description
New	Adds the user to the WebLM database.
Edit	Modifies the user password.
Delete	Deletes the user from the WebLM database.

WebLM Password Policy

Password history policy

The password history policy keeps a history of the previously used passwords and ensures that you must not use the previous password when changing the password. When the history policy is enabled, the default value to block the number of previously used password is 10.

The valid range to block the number of previously used passwords is from 0 to 24.

You can also disable the password history policy.

Password strength policy

The password strength policy that the system administrator defines enforces the following constraints:

- Passwords must be 6 to 25 characters long. The default character length is 14.
- Passwords must contain a combination of the following characters: a-z, A-Z, 0-9, {, }, |, (,), <, >, ,, /, ., =, [,], ^, _, @, !, \$, %, &, -, +, ", :, ?, `, or \
- Passwords do not require a minimum character type. However, the default is 0 lowercase, 0 uppercase, 0 numeric, and 0 special character. The sum cannot exceed the minimum total length.

The policy allows the minimum number of characters of certain types (lowercase, uppercase, numeric, special) in the password. The default is 0 for each of them.

- Password can contain a maximum of 2 consecutive characters. The valid values are from 1 through 5. The default value is 2.
- Password can contain a maximum number of 4 consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4.

When you enable the password strength policy, passwords must not be your user ID in forward or reverse order.

Passwords must not be a value based on a dictionary word.

You can also disable the password strength policy.

Configuring password policies

About this task

WebLM Release 10.1.2 supports the following password policies:

- Password history policy
- Password strength policy

You can enable or disable both the password policies (history or strength) or can enable or disable one of the password policy independently.

On the fresh deployment of WebLM Release 10.1.2, the WebLM password policy is disabled.

A user with the system administrator role can edit the password settings.

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, click **Password Policy**.
WebLM displays the Password Policy page.
3. To enable the password history policy, select the **History** check box and enter the required details.
4. To enable the password strength policy, select the **Strength** check box and enter the required details.
5. Click **Submit**.

For more information on password policies, contact the system administrator.

Password Policy field descriptions

This page is accessible only for system administrator.

The password policy applies to all administrator logins. There are no exceptions.

History

Name	Description
History	The option to enable or disable the password history policy of the previously used passwords . By default, the password history policy is disabled. To enforce the check for the previously used passwords, select the check box. If you clear the check box, the password policy to check for the previously used passwords is not applicable.
Previous passwords blocked	The number of latest passwords that the system maintains in history. When the history policy is enabled, the default value to block the number of previously used password is 10. The valid range to block the number of previously used passwords is from 0 to 24.

Strength

Name	Description
Strength	The option to enable or disable the password strength. By default, the password strength is disabled. To enforce the password strength, select the check box. If you clear the check box, the password strength is not applicable.
Minimum Total Length	The minimum number of characters to use in the password. The minimum password length can be between 6 to 25 characters. The default value is 14.
Minimum by character Type: Lower case	The minimum number of lowercase characters to use in the password. The default value is 0.
Minimum by character Type: Upper case	The minimum number of uppercase characters to use in the password. The default value is 0.
Minimum by character Type: Numeric case	The minimum number of numeric characters to use in the password. The default value is 0.
Minimum by character Type: Special case	The minimum number of special characters to use in the password. The default value is 0.
Maximum repeated consecutive characters	The maximum number of repeated consecutive characters. The valid values are from 1 through 5. The default value is 2. For example, if the maximum repeated consecutive characters value is set to 2: - Valid password is: Buildd123\$ - Invalid password is: Builddd123\$

Table continues...

Name	Description
Maximum consecutive characters from same character type	The maximum number of consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4. For example, if the maximum repeated consecutive characters of the same character type is set to 4: - Valid password is: Build123\$ - Invalid password is: Build12345\$

Button	Description
Submit	Saves all the entries on the Password Policy page.
Cancel	Cancels the changes and returns to the previous page.

WebLM command-line password policies

setSecurityPolicy command

From Release 10.1.2, you can use the **setSecurityPolicy** command to modify the default password policy settings of WebLM. This command is only applicable for changing or setting up the password for the CLI or root user created during deployment.

Note:

When you create a user through the WebLM web console, the WebLM web console password policy applies.

You can run the **setSecurityPolicy** command in the following modes:

- **Interactive mode:** This is the default mode for operating this command. You can display, change, and refresh the password policy settings.
- **Non-interactive mode:** You can view the status, display the current settings, restore the default settings, and refresh the current profile, including any custom settings.

Syntax

```
setSecurityPolicy
```

Displays the interactive mode to change the password policy settings.

Syntax

```
setSecurityPolicy [--status] [--display-only] [--restore-defaults] [--refresh-custom]
```

- status** Displays the password policy settings status.
- display-only** Displays all the password policy settings.
- restore-defaults** Removes all customized values and restores the password policy settings to the default profile settings.

--refresh-custom Refreshes the custom profile settings in case of backup and restore.

Managing the command-line password policies

Procedure

1. Log in to the WebLM command-line interface with CLI user credentials that you create during application deployment.
2. Type **setSecurityPolicy**.
3. At the [sudo] password prompt, type the password.

WebLM displays the set of options.

For example:

Main Menu:

```
Custom Profile: no

1) Display Current Property Settings
2) Change Property Settings
3) Refresh Current Property Settings and Exit
4) Exit (no settings changed)

Select Action:
```

Where:

Custom Profile: The options are:

- **no:** Specifies that WebLM is using the default values from the loaded profile. This is the default value.
- **yes:** Specifies that a user has made some changes to customize the default password profile.

When the **Custom Profile** setting is **yes**, WebLM displays the **Custom Settings** field with the number of changes made to the default password profile.

For example:

```
Custom Settings: <n>
```

4. In **Select Action**, type one of the following:
 - **1:** to display the current property settings.
 - **2:** to change the current property settings.
 - **3:** to restore the current property settings and exit the command.

When you change the default password profile settings, WebLM displays this option.

- **4:** to refresh the current property settings and exit the command.
- **5:** to exit the command without saving the changes.

Changing the password policies through CLI

Procedure

1. Log in to the WebLM command-line interface with CLI user credentials that you create during application deployment.
2. Type **setSecurityPolicy**.
3. At the [sudo] password prompt, type the password.

WebLM displays the set of options.

For example:

Main Menu:

```

Custom Profile: no

1) Display Current Property Settings
2) Change Property Settings
3) Refresh Current Property Settings and Exit
4) Exit (no settings changed)

```

Select Action:

4. In **Select Action**, type 2.

WebLM displays the set of options to change the parameters.

Change Property Settings:

```

Custom Profile: no

Note: [Current Value: M=modified C=customized D=disabled]

1) Return to Main Menu
2) Change minimum password length [14]
3) Change minimum required uppercase characters [0: D]
4) Change minimum required lowercase characters [0: D]
5) Change minimum required numeric characters [0: D]
6) Change minimum required special characters [0: D]
7) Change remember previous passwords [10]
8) Change maximum repeated characters [2]
9) Change maximum class repeat [4]

```

Select Action:

5. In **Select Action**, type the number for which you want to change the value.

For example, if you want to change the minimum password length, type 2.

When you type 2, WebLM displays the following prompt.

```

Changing minimum password length:
Current Value: 14 (Minimum: 6, Maximum: 25)

Enter new value:

```

6. In **Enter new value**, type the required value.

When you type the value, WebLM displays the following prompt with the number of pending changes made.

For example:

Change Property Settings:

```
Custom Profile: no
Pending Changes: 1
```

Note: [Current Value: M=modified C=customized D=disabled]

- 1) Return to Main Menu
- 2) Change minimum password length [17: M]
- 3) Change minimum required uppercase characters [0: D]
- 4) Change minimum required lowercase characters [0: D]
- 5) Change minimum required numeric characters [0: D]
- 6) Change minimum required special characters [0: D]
- 7) Change remember previous passwords [10]
- 8) Change maximum repeated characters [2]
- 9) Change maximum class repeat [4]

Select Action:

7. To return to the main menu, in **Select Action**, type 1.

WebLM displays the main menu.

For example:

Main Menu:

```
Custom Profile: no
Pending Changes: 1
```

- 1) Display Current Property Settings
- 2) Change Property Settings
- 3) Apply Changes and Exit
- 4) Exit (discarding all pending changes)

Select Action:

8. To apply the changes to the password policy settings, in **Select Action**, type 3.

WebLM applies the profile changes, updates the system settings, and displays the number of changes made to the password policy settings.

For example:

```
Custom Profile: no
Pending Changes: 1
```

Applying Profile Changes:

```
Custom Profile: yes    (Custom Settings: 1)
```

Updating System Settings:

```
Executing pam-settings.sh
Executing password-policy.sh
```

Executing authselect for custom profile:

Profile "custom/av-password-policy" was selected.

The following nsswitch maps are overwritten by the profile:

- aliases
- automount
- ethers
- group

```
- hosts
- initgroups
- netgroup
- networks
- passwd
- protocols
- publickey
- rpc
- services
- shadow
```

Viewing the password policy status

Procedure

1. Log in to the WebLM command-line interface with CLI user credentials that you create during application deployment.
2. Type **setSecurityPolicy --status**, and press Enter.

WebLM displays the password policy status.

Following is the example where the default password policy has not been changed.

```
Custom Profile: no
```

Following is the example where one setting of the default password policy has been changed.

```
Custom Profile: yes (Custom Settings: 1)
```

Displaying the password policies

Procedure

1. Log in to the WebLM command-line interface with CLI user credentials that you create during application deployment.
2. Type **setSecurityPolicy --display-only**, and press Enter.

WebLM displays the configured password policy.

For example:

```
setSecurityPolicy --display-only
```

```
Custom Profile: yes (Custom Settings: 2)
```

Property	Value	Notes
minimum password length:	17	Custom(default: 14)
minimum required uppercase characters:	0	Disabled
minimum required lowercase characters:	0	Disabled
minimum required numeric characters:	1	Custom(default: 0)
minimum required special characters:	0	Disabled
remember previous passwords:	10	
maximum repeated characters:	2	
maximum class repeat:	4	

Restoring the default password policy settings

About this task

To restore the default password policy for the current customized profile, use the following procedure.

- In the Interactive mode, do the following:
 1. Type **setSecurityPolicy**.
 2. At the [sudo] password prompt, type the password.

WebLM displays the set of options.

For example:

```
Main Menu:

          Custom Profile: yes      (Custom Settings: <n>)

1) Display Current Property Settings
2) Change Property Settings
3) Restore Default Property Settings and Exit
4) Refresh Current Property Settings and Exit
5) Exit (no settings changed)

Select Action:
```

3. In **Select Action**, type 3.

WebLM updates the system settings and restores the default password policy settings.

```
Custom Profile: no

Updating System Settings:
    Executing pam-settings.sh
    Executing password-policy.sh

Executing authselect for custom profile:
Profile "custom/av-password-policy" was selected.
The following nsswitch maps are overwritten by the profile:
- aliases
- automount
- ethers
- group
- hosts
- initgroups
- netgroup
- networks
- passwd
- protocols
- publickey
- rpc
- services
- shadow
```

- In the Non-interactive mode, do the following:
 1. Type **setSecurityPolicy --restore-standard**, and press Enter.
 2. At the [sudo] password prompt, type the password.

WebLM updates the system settings and restores the default password policy settings.

```
Custom Profile: no

Updating System Settings:
    Executing pam-settings.sh
    Executing password-policy.sh

Executing authselect for custom profile:
Profile "custom/av-password-policy" was selected.
The following nsswitch maps are overwritten by the profile:
- aliases
- automount
- ethers
- group
- hosts
- initgroups
- netgroup
- networks
- passwd
- protocols
- publickey
- rpc
- services
- shadow
```

Refreshing the default password policy settings

About this task

When a custom profile is restored during a backup and restore, use the following procedure to apply the changes to the system settings.

- In the Interactive mode, do the following:
 1. Type **setSecurityPolicy**.
 2. At the [sudo] password prompt, type the password.

WebLM displays the set of options.

For example:

```
Main Menu:

      Custom Profile: yes      (Custom Settings: <n>)

1) Display Current Property Settings
2) Change Property Settings
3) Restore Default Property Settings and Exit
4) Refresh Current Property Settings and Exit
5) Exit (no settings changed)

Select Action:
```

3. In **Select Action**, type 4.

WebLM refreshes the system settings.

- In the Non-interactive mode, do the following:
 1. Type **setSecurityPolicy --refresh-custom**, and press Enter.

2. At the [sudo] password prompt, type the password.

WebLM updates the system settings and refreshes the default password policy settings.

Metering Collector configuration overview

With Release 8.1.2, you can manage the Avaya Subscription license on the WebLM server when metering collector is registered with WebLM. The metering collector configuration is applicable only for the Avaya Subscription license. The Solution-Avaya Subscription license contains more than one application.

Using the metering collector configuration, the WebLM server tracks the license usage information from the deployed applications. The WebLM server provides the license information to the metering collector when metering collector requests.

Related links

[Metering Collector Configuration field descriptions](#) on page 58

[Deleting the metering collector configuration](#) on page 59

Metering Collector Configuration field descriptions

If the metering collector is not registered with WebLM, the system displays the following message:

No Metering Collector currently configured for this WebLM.

Metering Collector is required for Avaya Subscriptions and is configured via the Metering Collector UI.

Name	Description
Name	The name of the metering collector. Each collector has its own unique metering collector id, which is displayed as Name on the WebLM server.
URL	The URL of the metering collector. It contains the IP Address or FQDN of the metering collector.
Link Status	The status of the collector link. Default value of the status is Active . The options are: • Active • Error WebLM checks the connectivity status in every 12 hours from the time last communication takes place with registered metering collector. If the metering collector does not send a request to WebLM for at least 24 hours, then the link status is displayed as Error .

Table continues...

Name	Description
Last Status Date/Time	The last synchronization timestamp of the metering collector with the WebLM server. The value is in the MM/DD/YYYY hh:mm:ss format.
Button	Description
Delete	Deletes the metering collector configuration.

Related links

[Metering Collector configuration overview](#) on page 58

Deleting the metering collector configuration

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, click **Metering Collector Configuration**.
3. On the Metering Collector Configuration page, click **Delete**.

The system displays the message: Are you sure you want to delete the collector configuration?

4. Click **Ok** to delete the metering collector configuration.

Related links

[Metering Collector configuration overview](#) on page 58

Centralized subscription licensing

With WebLM Release 8.1.3, the FEAT_CENTRALIZED_SUBSCRIPTION_MODE license feature is available in the Solution license file. To use the centralized subscription licensing feature, you need to select the Centralized Subscription Mode license feature when you generate the Solution license file from the Avaya PLDS website.

With the centralized subscription licensing feature, WebLM provides the full license capacity of a solution license file to multiple instances of the allowed application.

You can check the:

- Usage details of every instance in the **Acquired Licenses** table.
- Total usage of all instances in the **Licensed Features** table as **Currently Used**.

Centralized licensing

About centralized licensing

Some Avaya products do not share licenses from a single license file as each element instance requires a separate license file. You require a dedicated WebLM server to host the relevant license file of the associated element instance. In this licensing model, you require the same number of WebLM servers as the number of products that you install and configure. In the virtualized environment, this model requires additional virtual machines for each element instance, thus increasing the VMware licensing cost. Thus, you cannot centrally manage the licenses for a product and must log in to each WebLM server and manage licenses for each element instance.

WebLM supports centralized licensing feature so that products can have multiple license files installed for multiple instances of the product. On a single WebLM server, you can install multiple license files of a product and associate specific license files to specific element instances.

After you enable centralized licensing from the WebLM interface, you can install multiple license files for the same product. You can add multiple element instances, and associate each license file to an element instance. The WebLM server provides licenses to the element instances based on the association you define.

Enabling centralized licensing

Before you begin

Install a product license file that supports centralized licensing. Centralized licenses contain the FEAT_WLM_CENTRALIZED feature in the product license file.

About this task

By default, centralized licensing is disabled. You must enable centralized licensing to use this feature.

Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. Click **Enable Centralized Licensing**.



Warning:

After enabling the Centralized Licensing feature for a product, you must link the license file to the associated product server instance. If you do not link the license file to a product server instance, the product server instance cannot acquire the license file from the WebLM server.

Configure centralized licensing field descriptions

Elements and License File Assignments

Name	Description
Element Display Name	
Centralized Licensing ID	
Host ID - Centralized Licensing ID	The host ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID. The centralized licensing ID is a unique number across multiple license files for the same product.
License Host Name	The hostname of the license, as defined in the license file.
Date of Installation	The date of installation of the license file.

Installed License Files

Name	Description
Host ID - Centralized Licensing ID	The host ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID. The centralized licensing ID is a unique number across multiple license files for the same product.
License Host Name	The hostname of the license, as defined in the license file.
Assigned To Element	• Yes: The license file is associated with an element instance. • No: The license file is not associated with an element instance.
Date of Installation	The date of installation of the license files.

Button	Description
New	Adds an element instance and the mapping of an element to a license file.
Edit	Edits the properties of the element instance.
Delete	Deletes an element instance.

Adding an element instance and assigning the element instance to a license file

Before you begin

Enable the Centralized Licensing feature.

Install the license files to assign to an element instance.

Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.

3. Click **New**.
4. On the Add Element Instance page, type the element display name and the centralized licensing ID of the instance. For more information, see “Element instance field descriptions”.
5. In the **Select License File** table, select the license file to map to the element instance.
6. Click **Save**.

 Note:

If you select the license file already assigned to an element, WebLM displays the following warning message:

Assigning Multiple Centralized Licensing IDs/Element IPs to same license.

Related links

[Element instance field descriptions](#) on page 63

Editing an element instance and license file assignment

Before you begin

- Enable the centralized licensing feature.
- Install the license file that you want to assign to the element instance.
- Add an element instance.

About this task

Use this procedure to edit the properties of an element instance.

Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. On the Configure Centralized Licensing page, select the element instance.
4. Click **Edit**.
5. On the Edit Element Instance page, modify the display name and element IP address of the element instance.
6. In the **Select License File** table, you can select a new license file for the element instance.
7. Click **Save**.

 Note:

If you select the license file already assigned to an element, WebLM displays the following warning message:

Assigning Multiple Centralized Licensing IDs/Element IPs to same license.

Related links

[Element instance field descriptions](#) on page 63

Deleting an element instance

Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. On the Configure Centralized Licensing page, select the element instance that you want to delete.
4. Click **Delete**.

The system displays the Delete Element Confirmation page.

5. Click **Delete**.

The system deletes the element instance and its assignment with the license file.

Element instance field descriptions

Name	Description
Element Display Name	
Centralized Licensing ID	

Select License File

Name	Description
Host ID - Centralized Licensing ID	The host ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID. The centralized licensing ID is a unique number across multiple license files for the same product. For centralized licensing scenarios with just one license file, the host ID has 12 characters.
License Host Name	The host name of the license as defined in the license file.
Assigned To Element	• Yes: The license file is associated with an element instance. • No: The license file is not associated with an element instance. • Yes: The license file is associated with a Communication Manager server. • No: The license file is not associated with a Communication Manager server.
Date of Installation	The date of installation of the license file.

Button	Description
Save	Adds or edits the element instance.
Cancel	Cancels the add or delete element instance operation.

Disabling centralized licensing

Before you begin

Ensure that:

- You have not added an element instance for the product. If you have added the element instances, delete the element instances.
- You have installed only a single license file for the product. If you have installed multiple license files, uninstall all the files except any one license file.

Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. Click **Disable Centralized Licensing**.

Uninstalling the Communication Manager 6.3.x, 7.x, and 8.x license file and installing the Communication Manager 10.1.x license file

About this task

If you have a mix of Communication Manager Release 6.3.x, 7.x, 8.x, and 10.1.x software with Communication Manager 6.3.x, 7.x, 8.x, and 10.1.x license files, then Avaya recommends to use the Communication Manager 10.1.x license file for all the Communication Manager Release software.

If you cannot use the Communication Manager 10.1.x license file for all the Communication Manager Release software, do the following:

Procedure

1. Disable the Centralized Licensing.
2. Uninstall the Communication Manager 6.3.x, 7.x, and 8.x license files.
3. Install the Communication Manager 10.1.x license file.
4. Enable the Centralized Licensing.
5. Install the Communication Manager 6.3.x, 7.x, and 8.x license files.

Managing the WebLM Application server

- To start the Application server, type the `weblmStart` command.
- To check the status of the Application server, type the `weblmStatus` command.
- To stop the Application server, type the `weblmStop` command.
- To restart the Application server, type the `weblmRestart` command.

Logging out of the WebLM server

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. At the top-right corner of the web page, click **Log off**.

The system displays the log-in page.

Chapter 4: WebLM Certificate Management

Credential store and certificate management

Important:

From Release 10.1.2, the functionality of the `importCACertificate` command is merged with the `manageCACertificates` command. The standalone WebLM server no longer uses the `importCACertificate` command.

Before Release 10.1.2, in standalone WebLM, the default password for keystore and truststore was set as password. To add a CA certificate, you needed to enter the keystore password.

From Release 10.1.2, for security purposes, the credential store automatically generates unique passwords at random for the keystore and truststore. You no longer need to enter the keystore password, as the credential store generates different passwords every time and populates the password automatically.

You can still continue to manage certificates. For more information on managing a trust certificate, see [manageCACertificates command](#) on page 71.

Self-signed certificate

When you do a fresh install, a newly self-signed generated certificate and credential store is created with a new password.

Third-party certificate

Before Release 10.1.2, when you imported the previously configured third-party certificate along with CA, you had to provide the password you used to create the certificate. After Release 10.1.2, if you have a third-party certificate configured or an identity certificate issued by one of the third-party CAs, you need to re-import the third-party certificate after an upgrade.

Import CA certificate into WebLM client truststore

WebLM client residing on products connect to the WebLM server using HTTPS for licensing.

To authenticate the server, import the server public certificate into the client trust store.

You can add or set the WebLM server CA certificate in the trusted store on the following clients:

- **C++:** Refer the WebLM C++ client product documentation to add or set the WebLM server CA certificate in the trusted store.

- **Java:** See “Importing CA certificate into WebLM Java client truststore”.

Toggling cipher suites for WebLM

About this task

From WebLM Release 8.1.3.5, you can toggle between the following cipher suites:

- Relaxed cipher suites
- Strict cipher suites

When you install WebLM, by default, WebLM is set up with Relaxed cipher suites.

Use the following procedure to toggle the required cipher suites for WebLM.

Procedure

1. Log in to the WebLM command-line interface.
2. Type the **configureCiphersList** command and perform one of the following:

- To view the configured cipher suites, at the prompt, type 1.

WebLM displays the list of existing configured cipher suites.

- To configure relaxed cipher suites, at the prompt, type 2.

The WebLM Application server restarts, and the standalone WebLM console is not accessible during this time. Additionally, if products are configured to acquire licenses from this WebLM server, the license request fails.

After the configuration is complete, WebLM displays the following message with the list of configured relaxed cipher suites:

```
Relaxed cipher suites configured successfully
```

- To configure strict cipher suites, at the prompt, type 3.

The WebLM Application server restarts, and the standalone WebLM console is not accessible during this time. Additionally, if products are configured to acquire licenses from this WebLM server, the license request fails.

After the configuration is complete, WebLM displays the following message with the list of configured strict cipher suites:

```
Strict cipher suites configured successfully
```

Configuring the TLS version for WebLM

About this task

WebLM supports the following TLS versions:

- TLSv1.3

From Release 10.1.2, WebLM supports TLS version 1.3.

- TLSv1.2
- TLSv1.1
- TLSv1.0

When you deploy WebLM, by default, WebLM is set up with minimum TLS version 1.2.

* Note:

- WebLM does not preserve the minimum TLS version setting and cipher suite setting during the Backup and Restore operations.
- WebLM does not retain the TLS version value after upgrading from earlier release to Release 10.1.2 and later.

Procedure

Do one of the following:

- To configure minimum TLS version 1.3, type the command: **configureTLS**
-ENABLE_TLS_VERSIONS TLSv1.3
- To configure TLS version 1.2 and above, type the command: **configureTLS**
-ENABLE_TLS_VERSIONS TLSv1.2
- To configure TLS version 1.1 and above, type the command: **configureTLS**
-ENABLE_TLS_VERSIONS TLSv1.1
- To configure TLS version 1.0 and above, type the command: **configureTLS**
-ENABLE_TLS_VERSIONS TLSv1.0

If you set the TLS version 1.0 or TLS version 1.1, WebLM displays the following message:

```
Warning! You are setting Minimum TLS Version to TLSv1.0 or TLSv1.1.
For increased security, it is recommended to set Minimum TLS Version to
TLSv1.2 or higher, if these protocol levels can be supported in your
configuration.
```

```
Are you sure you want to proceed with selected TLS Version? [y/N]
```

At the prompt, type **y** to proceed.

WebLM enables the required TLS version.

For example, when you enable the TLSv1.3, WebLM displays the following message:

```
Enabling TLSv1.3
Stopping WebLM server
Starting WebLM server
Enabling TLSv1.3 completed successfully
```

manageWebLMCertificate command

From Release 10.1.2, use the **manageWebLMCertificate** command, a command line utility that is used to manage WebLM certificates.

Important:

From Release 10.1.2, the standalone WebLM server no longer uses the **toggleWebLMCert** command.

Syntax

```
manageWebLMCertificate [-display] [-replace -certpath <file> -password <password>] [-generateSelfSigned]
```

-display	To list all WebLM certificates that are stored in the WebLM server database.
-replace	To replace a WebLM certificate with a new third-party certificate.
-certpath <file>	The full path of the PKCS certificate file.
-password <password>	The password of the PKCS certificate file.
-generateSelfSigned	To regenerate and configure self-signed WebLM certificate.

Viewing a WebLM certificate

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. Type **manageWebLMCertificate -display** and press Enter.

WebLM displays the WebLM certificate that is stored in the WebLM server keystore.

For example:

```
Keystore type: PKCS12
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: 1
Creation date: Sep 8, 2022
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=weblm54.avaya.com, O=Avaya Inc., C=US
Issuer: CN=weblm54.avaya.com, O=Avaya Inc., C=US
Serial number: 5e2f2a3872c1cbb7c5e87cb6e077f9dccbbaef9
Valid from: Wed Sep 07 12:03:26 IST 2022 until: Mon Sep 06 12:03:26 IST 2027
Certificate fingerprints:
SHA1: 1E:1E:40:EB:57:2E:CA:F3:28:F3:0D:CE:8E:70:F3:79:1E:C4:EE:29
```

```

SHA256:
72:4F:ED:1F:92:78:A5:F9:19:28:07:83:A9:C8:A1:B6:61:09:C5:5C:28:E3:3E:E4:D0:19:3E:F
A:A9:2E:38:4C
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 1

```

Replacing a WebLM certificate with a third-party certificate

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. Type **manageWebLMCertificate** -replace -certpath <file> -password <password> and press Enter.

Where,

- <file>: The file name of the WebLM certificate that you are about to replace with a third-party certificate.

 Note:

The PKCS file must contain the full certificate chain that includes the private key and the corresponding public certificate with all the intermediate CA certificates and the root CA certificate.

- <password>: The password of the PKCS certificate file.

WebLM displays the following message:

```
Warning! You are installing a new server certificate which will
replace the existing one.
```

3. In the Do you wish to proceed? prompt, type y.
WebLM replaces the WebLM certificate with the new third-party certificate.
4. Restart the WebLM application service.

Regenerating a self-signed WebLM certificate

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. Type **manageWebLMCertificate** -generateSelfSigned and press Enter.

WebLM displays the following message:

```
Warning! You are creating a new self-signed server certificate
which will replace the existing certificate.
It is recommended to use a certificate issued from a trusted CA.
```

3. In the Do you wish to proceed? prompt, type y.

WebLM replaces the existing certificate with a new self-signed server certificate.

4. Restart the WebLM application service.

manageCACertificates command

From Release 10.1.2, use the **manageCACertificates** command to view, add, and delete CA certificates from the Avaya WebLM truststore.

Syntax

```
manageCACertificates [-list] [-add -certpath <file> -alias <alias>] [-remove -alias <alias>]
```

-list	To list all CA certificates that are stored in the WebLM server database.
-add	To import a CA certificate into the WebLM server truststore.
-certpath <file>	The full path of the certificate to be imported into the WebLM server truststore.
-alias <alias>	The alias of the certificate to be imported in the WebLM server truststore.
-remove	To remove a CA certificate from the WebLM server truststore.
-alias <alias>	The alias of the certificate to be removed from the WebLM server truststore.

Viewing a CA certificate from the WebLM truststore

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. Type **manageCACertificates -list** and press Enter.

WebLM displays a specific CA certificate that is stored in the WebLM server truststore.

For example:

```
Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: weblmselfsigned
Creation date: Aug 1, 2022
Entry type: trustedCertEntry

Owner: CN=weblm51.avaya.com, O=Avaya Inc., C=US
```

```
Issuer: CN=weblm51.avaya.com, O=Avaya Inc., C=US
Serial number: 5074c60351e786ad9d62b93ff24b7972adf0aada
Valid from: Mon Aug 01 09:54:47 IST 2022 until: Sat Jul 31 09:54:47 IST 2027
Certificate fingerprints:
    SHA1: 5E:4C:18:61:27:4D:B3:8A:E9:BB:E5:82:8C:B4:A0:60:38:40:53:36
    SHA256:
A4:CC:85:60:77:8F:D8:C9:87:E1:DD:F4:3A:01:2C:54:AC:3F:64:F2:05:7C:F3:51:9D:2A:B3:E
5:73:35:E2:73
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 1
```

Importing a CA certificate into the WebLM truststore

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. Type **manageCACertificates -add -certpath <file> -alias <alias>** and press **Enter**.

Where,

- **<file>**: The file name of the CA certificate that you import into the WebLM server truststore.
- **<alias>**: The alias name that you need to assign to the alias.

Deleting a CA certificate from the WebLM truststore

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. Type **manageCACertificates -remove -alias <alias>** and press **Enter**.

Where, **<alias>** is the alias name that you need to delete from the WebLM truststore.

setWebLMClientAuth command

The **setWebLMClientAuth** command enables and disables client certificate authentication for WebLM port 52233.

Syntax

```
setWebLMClientAuth [1] [2] [3]
```

- 1 Displays existing WebLM client certificate authentication configuration.

- 2 Enables WebLM client certificate authentication.
- 3 Disables WebLM client certificate authentication.

Displaying existing WebLM client certificate authentication configuration

Procedure

1. Log in to the WebLM command-line interface with CLI user credentials that you create during application deployment.
2. Type the **setWebLMClientAuth** command and press `Enter`.
3. In the `Enter any other key to exit prompt`, type 1.

If client certificate authentication is disabled, WebLM displays the following message:

```
WebLM client certificate authentication enabled: false
```

If client certificate authentication is enabled, WebLM displays the following message:

```
WebLM client certificate authentication enabled: true
```

Enabling WebLM client certificate authentication

About this task

From 10.1.3.3 onwards, the WebLM client certificate authentication configuration is ON by default and you need to setup WebLM client certificate for communication with WebLM server for licensing to work. You must disable client certificate authentication if you do not require it (WebLM client certificate for communication). You can re-enable it once the WebLM client certificate for communication is configured.

Procedure

1. Log in to the WebLM command-line interface with CLI user credentials that you create during application deployment.
2. Type the **setWebLMClientAuth** command and press `Enter`.
3. In the `Enter any other key to exit prompt`, type 2.
4. In the `Are the clients configured with identity certificate? (Y/N)` prompt, type Y.

 Note:

If you type N, WebLM exits the **setWebLMClientAuth** command.

5. In the Are signed client CA certificates have been added to this WebLM server truststore? (Y/N) prompt, type Y.

WebLM enables client certificate authentication and displays the following message:

```
WebLM client authentication enabled successfully.
```

WebLM server restarts, and the WebLM web console will be inaccessible for approximately 2 to 5 minutes.

Related links

[Adding the whitelist for client certificate identity](#) on page 19

Disabling WebLM client certificate authentication

Procedure

1. Log in to the WebLM command-line interface with CLI user credentials that you create during application deployment.
2. Type the **setWebLMClientAuth** command and press `Enter`.
3. In the `Enter any other key to exit` prompt, type 3.

WebLM disables client certificate authentication and displays the following message:

```
WebLM client authentication disabled successfully.
```

WebLM server restarts, and the WebLM web console will be inaccessible for approximately 2 to 5 minutes.

Chapter 5: Troubleshooting standalone WebLM

Overview

This section provides detailed information to help you resolve issues with the standalone version of WebLM. The section is intended for people who install, configure, and maintain WebLM for both standard and enterprise license configurations.

Adopter application cannot communicate with WebLM Server

Cause

Due to higher security settings on the WebLM Server Release 7.1 system, the adopter applications that are using WebLM Server earlier to Release 7.1 might not communicate with WebLM Server to fetch the license file from WebLM Server by using the WebLM client.

Solution

To fetch the license file from the WebLM Server Release 7.1 system, locate the `trusted_weblm_certs.jks` file from the adopter application system, take the backup of the file, delete the file, and then restart the adopter application.

Do this if the adopter application cannot communicate with WebLM Server regardless of the WebLM Server version on the adopter system.

Adopter application cannot communicate with WebLM Server

Cause

If you provide a slash at the end of the licensing URL, the adopter application will not be able to communicate with WebLM Server. For example:

- For IPv4, `https://IPv4_Address:52233/WebLM/LicenseServer/`

- For IPv6, `https://[IPv6_Address]:52233/WebLM/LicenseServer/`

The adopter application that is being licensed displays the following alarm:

Alarm Id: 400 Severity: Critical Component: Resource Manager Date & Time: <Timestamp> Description: WebLM Connection Failed Probable Cause: WebLM server is down or unreachable. Corrective Action: Check status of configured WebLM server and verify network connectivity to it.

Solution

To fetch the license file from WebLM Server, type the URL, as following:

- For IPv4, `https://IPv4_Address:52233/WebLM/LicenseServer`
- For IPv6, `https://[IPv6_Address]:52233/WebLM/LicenseServer`

WebLM launching errors

Launching of WebLM fails

Symptom	The system fails to launch WebLM with the following errors: • A 404 error when you gain access to WebLM from the browser. • A <code>Connection refused</code> error when you communicate with WebLM server using the client API.
Cause of the issue	• If the JBoss service fails to run. • If you use an incorrect URL to gain access to WebLM. • If you have network connectivity issues while gaining access to WebLM from a remote computer. • If the configuration of HTTPS in the <code>standalone.xml</code> file of JBoss is incorrect. • If several applications run on the server that hosts JBoss, and the server caters to a large number of simultaneous requests.

Related links

- [Proposed solution 1](#) on page 77
- [Proposed solution 2](#) on page 77
- [Proposed solution 3](#) on page 77
- [Proposed solution 4](#) on page 78
- [Proposed solution 5](#) on page 78

Proposed solution 1

Before you begin

Obtain a valid license file for the WebLM server.

Procedure

If JBoss is started as a service, to verify that the service is running, perform one of the following:

- For Windows, to verify the status of the JBoss service, click **Control Panel > Administrative Tools > Services**.
- For Linux, at the command prompt, type `service JBoss status`.

From the list of services, the system must display the status of **JBoss** as `Started`.

Proposed solution 2

Procedure

To gain access to the WebLM server, enter the URL in one of the following formats:

- From the browser, enter one of the following:
 - For IPv4, use the following:
 - `http://<HOST_NAME/IPv4_ADDRESS>:<HTTP_PORT>/WebLM/index.jsp`
 - `https://<HOST_NAME/IPv4_ADDRESS>:<HTTPS_PORT>/WebLM/index.jsp`
 - For IPv6, use the following:
 - `http://<HOST_NAME/[IPv6_ADDRESS]>:<HTTP_PORT>/WebLM/index.jsp`
 - `https://<HOST_NAME/[IPv6_ADDRESS]>:<HTTPS_PORT>/WebLM/index.jsp`
- From the client API, enter one of the following:
 - For IPv4, use the following:
 - `http://<HOST_NAME/IPv4_ADDRESS>:<HTTP_PORT>/WebLM/LicenseServer`
 - `https://<HOST_NAME/IPv4_ADDRESS>:<HTTPS_PORT>/WebLM/LicenseServer`
 - For IPv6, use the following:
 - `http://<HOST_NAME/[IPv6_ADDRESS]>:<HTTP_PORT>/WebLM/LicenseServer`
 - `https://<HOST_NAME/[IPv6_ADDRESS]>:<HTTPS_PORT>/WebLM/LicenseServer`

Proposed solution 3

About this task

To gain access to the WebLM server over the network:

Procedure

1. Ensure that the connectivity to the network exists.
2. Verify that the firewall does not block any ports that JBoss listens to.

Proposed solution 4

Procedure

To use HTTPS protocol, you must enable HTTPS in one of the following files:

- On a Linux system: `/opt/Avaya/JBoss/wildfly/standalone/configuration/standalone.xml`
- On a Windows system: `%CATALINA_HOME%\conf\server.xml`

Proposed solution 5

A number of applications run on the WebLM server that hosts JBoss, and the server caters to several requests simultaneously.

Procedure

1. Ensure that the JBoss configuration supports the load expected on the system.
2. If required, modify the JBoss configuration to support more requests simultaneously.

For details about changing the JBoss configuration, see *JBoss configuration guide*.

License file installation errors

Installation of license file on the WebLM server fails

Scenario 01

The installation of a license file on the WebLM server fails for several reasons. The following sections provide some troubleshooting scenarios and proposed solutions:

Symptom1

The system displays the following error:

```
Error installing license. An error occurred while
performing license installation checks. Please ensure that
all the required steps were performed before deploying
WebLM server.
```

Cause of the issue

- If the following sequence of events occurs:
 1. You run an instance of the JBoss/WebLM server as `root`.
 2. You successfully install a license file for a product, for example product A.

3. The instance of the JBoss/WebLM server exits ungracefully. As a result, the file cleanup process fails.
4. Redeploy or restart the JBoss/WebLM server as another user, for example JBoss5. As a result, an existing license file fails to load on startup.
5. If you attempt to install a new license file for the same product, product A.
 - If multiple instances of the WebLM server run on the same server, and you install a license file for a product on an instance of the WebLM server when a license is already hosted on another instance of the WebLM server.
 - If the user ID you use to start the JBoss service does not have the write permission for the following directory:
 - On a Linux system, `/var/tmp`
 - On a Windows system, `C:\temp`

Related links

[Proposed solution](#) on page 79

Proposed solution

Before you begin

Obtain a valid license file for the WebLM server.

Procedure

1. Start only one instance of the WebLM server on the system at a time.
2. Ensure that the user ID you use to start the JBoss service has write permissions for the following directory:
 - On a Linux system, `/var/tmp`
 - On a Windows system, `C:\temp`
3. If the system still displays the error, do the following:
 - a. Verify that a lock file exists and has the `##machineNameproductName.l` file naming convention.
 - b. To view the lock file, do one of the following:
 - On a Windows system, the lock file exists in the `C:\temp` directory and the file is hidden. Enable the view hidden files option using the following steps:
 - a. Browse to the `C:\temp` directory.
 - b. Click **Tools > Folder Options**.
 - c. Click the **View** tab.
 - d. In the **Advanced settings** section, select **Files and Folders > Hidden files and folders > Show hidden files and folders**.
 - e. Click **Apply** and then click **OK**.

The system displays the lock file in the list.

- On a Linux system, to view the lock file, type `ls -al /var/tmp`.
 - c. If the lock file exists, stop JBoss gracefully, and delete the lock file.
 - d. If the license file exists, remove the file from the `$JBOSS_HOME/avmgmt/configuration/webalm/licenses.xml` directory on a Linux system or `%CATALINA_HOME%\webapps\WebLM\licenses` on a Windows system. The license file must have a `.xml` extension.
 - e. Start JBoss.
4. To install the license file, on the WebLM Home page, click **Install license**, and proceed with the installation steps.

For information about installing a license file, see [Installing a license file](#) on page 14.

The system installs the license file on the WebLM server.

Scenario 02

Symptom 2	The system displays the following error: Error installing license. License file is invalid or not created for this server. License file was not installed.
Cause of the issue	The error occurs due to one of the following reasons: • If the MAC address in the license file fails to match the MAC address of the system hosting the WebLM server. • If you modify the license file. • If the license file name contains special characters that the system fails to support.

Related links

[Proposed solution](#) on page 80

Proposed solution

Procedure

Depending on the cause of the error, perform one of the following:

- a. Log on to the WebLM web console with administrator privilege credentials.
- b. In the navigation pane, click **Server properties**, and verify that the MAC address in the license file matches the MAC address displayed on the Server Properties page.

The Server properties page displays the MAC addresses for all available NICs on the system on which you installed WebLM. The MAC address in the license file must match the MAC address of the system on which the WebLM server is running.

- Verify that the license file is not edited. If the license file is edited, revert the changes or install the original license file that you receive from PLDS.

- Verify that the name of the license file does not contain the following characters:

- On a Windows system, % ^ { } # `
- On a Linux system, % ^ { } # ` []

If the name of the license file uploaded on the WebLM server contains any of the characters that the system does not support, remove the characters from the file name and install the license file.

! Important:

The system supports the following sets of characters in the name of the license file for both Windows and Linux: ~ ; , ! ' = + @ () & \$ - and whitespace.

Scenario 03

Symptom 3	The system displays the following error: Error installing license. License installation failed. The product already exists with a SID <SID_IN_EXISTING_LICENSE_FILE>, which is different than the one present, <SID_IN_NEW_LICENSE_FILE>, in new license file.
Cause of the issue	If a license file for a product is already installed on the WebLM server and you attempt to install another license file for the same product with a different System Identification number (SID) on the WebLM server. You encounter this issue when you have a license file generated by Remote Feature Activation (RFA) installed on a WebLM server for a product. The license file that RFA generates has an RFA generated SID value. You then receive an updated license file for the same product from PLDS. The new license file for the same product contains a different SID value. The system displays the error message when you attempt to install the new file on the existing file.

Related links

[Proposed solution](#) on page 81

Proposed solution

When the existing license file and the new license file for a given product have different SID values, you cannot install the new license file when a license file exists on the WebLM server. You must uninstall the existing license file from the WebLM server and then install a new license file on the server.

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. For a standard or an enterprise license file, where enterprise or local WebLM configuration is not set:

- a. To uninstall the existing license file, click **Uninstall license**, and follow the instructions provided in [Removing a license file](#) on page 44.

 Note:

The system removes the existing license file for the product. You lose all the existing usage data for the product.

- b. To install a new license file, click **Install license**, and follow the instructions provided in [Installing a license file](#) on page 14.

The system installs the new license file for the product.

2. For an enterprise license file, where you added local WebLM servers:

- a. In the left navigation pane, click **Licensed products** and select the product name.
- b. Click **Local WebLM Configuration > Delete local WebLM**.
- c. Click **Delete**.

 Note:

The system removes the license file allocated to the local WebLM servers that you added to this enterprise setup. As a result, licensed applications which are in the process of acquiring licenses from the local WebLM servers fail to acquire any new licenses or renew the existing licenses.

- d. To uninstall the existing license file, click **Uninstall license**, and follow the instructions provided in [Removing a license file](#) on page 44.

 Note:

The system removes the existing license file for the product. You lose all the existing usage data for the product.

- e. To install a new license file, click **Install license**, and follow the instructions provided in [Installing a license file](#) on page 14.

The system installs the new license file for the product. You must configure the enterprise again, add local WebLM servers, and allocate the license for the local WebLM servers you added.

Scenario 04

Symptom 4

The system displays the following error:

```
Unsupported content type. License contents must be "text/xml".
```

Cause of the issue

The error occurs due to the following reasons:

- If you click **Install** before you select a license file.
- If you fail to select a license file that has a `.xml` extension.
- If the license file you use to install contains invalid XML content.
- If the browser settings are incorrect.
- If the registry settings are incorrect.

Related links

[Proposed solution](#) on page 83

Proposed solution

The installation of the license file might fail if you install the license file on a WebLM server from a particular browser or a system. However, you can successfully install the same file on the WebLM server by gaining access to the same WebLM server from another browser or system. The failure might be due to invalid browser or registry settings.

Before you begin

- Obtain a valid license file.
- Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. To install a new license file, click **Install license**, and follow the instructions provided in [Installing a license file](#) on page 14.
2. Verify that the browser setting are appropriate. You can use the default settings to upload the license file.
3. To verify that the registry settings on Windows are appropriate, perform the following procedure:
 - a. At the command prompt, enter `regedit`.
 - b. On the Registry Editor window, ensure that the **Extension Key** in the `HKEY_CLASSES_ROOT/MIME/Database/Content Type/application/xml` directory is `.xml`.
4. Verify if you can install the license file from a different browser or from a different system.

Scenario 05**Symptom5**

The system displays the following error:

```
Failed to install new license file as the current usage for feature, "VALUE_OL_TRANSCRIPTION_USERS" is XXXX while the new license file only has <XXXX licenses. Procure and install
```

a license file with a license count greater than XXXX for feature "VALUE_OL_TRANSCRIPTION_USERS".

Cause of the issue

- The license file is already acquired. The new license file which you are trying to install has fewer licenses than the already acquired license file.
- The current capacity use exceeds the capacity in the installed license.
- An acquired license does not cover a licensed feature or product.
- An over installation of licenses. In this scenario, free the already acquired licenses and retry installing the new license file. You could also try uninstalling the existing installed license file and installing a new license file.

Proposed solution

About this task

A proposed solution describes how to free the already acquired licenses and retry the installation of the new license file.

You can also try uninstalling the existing installed license file and installing a new license file. For more information, see [Proposed solution](#) on page 81.

Before you begin

- Obtain a valid license file for the WebLM server.
- Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View license capacity**.
3. Check the **Acquired Licenses** table for details of acquired licenses.
4. Free the acquired licenses.

The steps for freeing the acquired licenses vary according to the product. Use the same client that you used to acquire the licenses to free them.

WebLM password errors

WebLM password resetting

Symptom

When you provide your credentials to log in to WebLM, the system displays a log-in failure error message.

Cause of the issue

You forget or lose the password for the WebLM login.

Proposed solution

If a non-admin user fails to log in to the WebLM server using the existing credentials, you must reset the password.

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, click **Manage Users**.
3. Select the user whose password you want to reset.
4. Enter a new password for the user.

Next steps

When the user logs in to WebLM, the system prompts for a password change. The user must change the password on the first login.

Chapter 6: Avaya WebLM commands

WebLM CLI operations

*** Note:**

Any CLI user who is part of the gcliuser, and admin groups created at the time of deployment can execute the following commands:

#	Command	Parameters	Description	Usage
1.	changeIPFQDN	• IP < new IP address for WebLM > • FQDN < new fully qualified domain name of WebLM > • GATEWAY < new gateway address for WebLM > • NETMASK < new netmask address for WebLM > • dns < new DNS address for WebLM > • SEARCH < new search list for DNS addresses >	Updates the IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value.	• changeIPFQDN -IP < new IP address > • changeIPFQDN -FQDN < new fully qualified domain name > • changeIPFQDN -IP < new IP address > -GATEWAY < new gateway address for WebLM > -SEARCH < new search list for DNS addresses >
2.	configureNTP	< IP address of the NTP server >	Configures the NTP server details.	configureNTP < IP address of the NTP server > Separate the IP addresses or the host names of the NTP servers with commas (,).
3.	configureTimeZone	< Time zone that you want to select >	Configures the time zone with the value that you select.	Select a time zone. For example, America/Denver

Table continues...

#	Command	Parameters	Description	Usage
4.	WebLMPatchdeploy	< absolute path to the WebLM service pack, feature pack, or the software patch >	Installs the software patch, the service pack, or the feature pack for WebLM.	WebLMPatchdeploy <absolute path to home/admin/< WebLM FeaturepackName >  Note: Copy the WebLM feature pack or patches that you install to /home/admin/.
5.	weblm_password		Resets the WebLM password through CLI. Any CLI user who is part of the gcliuser and admin groups, created at the time of deployment can execute the command.	
6.	configureTLS	• -ENABLE_TLS_VERSIONS TLSv1.3 • -ENABLE_TLS_VERSIONS TLSv1.2 • -ENABLE_TLS_VERSIONS TLSv1.1 • -ENABLE_TLS_VERSIONS TLSv1.0	Configures the TLS version.	Type one of the following options: • configureTLS -ENABLE_TLS_VERSIONS TLSv1.3 • configureTLS -ENABLE_TLS_VERSIONS TLSv1.2 • configureTLS -ENABLE_TLS_VERSIONS TLSv1.1 • configureTLS -ENABLE_TLS_VERSIONS TLSv1.0
7.	collectLogs		Collects the WebLM logs in the /tmp/WebLM_Logs_DDMonYY_XXXXXXXXXXXXXXXXX.zip file.	
8.	swversion		Verifies the WebLM software version.	

Table continues...

#	Command	Parameters	Description	Usage
9.	swversion -s		Verifies the WebLM software version and also displays information about the application name, profile, and deployment type.	swversion -s * Note: The output varies based on the application deployment and the virtualization environment.
10.	WebLMBackup	<backup_location>	Performs the WebLM backup.	WebLMBackup <backup_location> * Note: You can copy the backup files to a remote computer or to an external storage device.
11.	WebLMRestore	<Full path where the Backup files have been saved>	WebLM restores user, data, and license information from the backup based on the data available in the backup file.	WebLMRestore <Full path where the Backup files have been saved>
12.	configureCiphersList	• 1: To view the configured cipher suites. • 2: To configure relaxed cipher suites. • 3: To configure strict cipher suites.	You can toggle between the Relaxed cipher suites or Strict cipher suites.	
13.	weblmStart		Starts the WebLM Application server.	weblmStart
14.	weblmStatus		Checks the status of the WebLM Application server.	weblmStatus
15.	weblmStop		Stops the WebLM Application server.	weblmStop
16.	weblmRestart		Restarts the WebLM Application server.	weblmRestart

Table continues...

#	Command	Parameters	Description	Usage
17.	manageWebLMCertificate	• -display • -replace • -generateSelfSigned	Allows you to view a WebLM certificate, replace a WebLM certificate with a third-party certificate, and generate a self-signed WebLM certificate.	Type one of the following options: • manageWebLMCertificate -display • manageWebLMCertificate -replace -certpath <file> -password <password> • manageWebLMCertificate -generateSelfSigned
18.	manageCACertificates	• -list • -add • -remove	Allows you to view, add, and delete CA imported certificates in the WebLM server truststore.	Type one of the following options: • manageCACertificates -list • manageCACertificates -add -certpath <file> -alias <alias> • manageCACertificates -remove -alias <alias>

Table continues...

#	Command	Parameters	Description	Usage
19.	setWebLMClientAuth	• 1: Displays existing WebLM client certificate authentication configuration. • 2: Enables WebLM client certificate authentication. • 3: Disables WebLM client certificate authentication.	Allows you to manage the client certificate authentication for WebLM port 52233.  Note: From 10.1.3.3 onwards, the WebLM client certificate authentication configuration is ON by default and you need to setup WebLM client certificate for communication with WebLM server for licensing to work. You must disable client certificate authentication if you do not require it (WebLM client certificate for communication). You can re-enable it once the WebLM client certificate for communication is configured.	

Table continues...

#	Command	Parameters	Description	Usage
20	<code>toggleOldWebLMClientCommunication</code>	Run this utility as the following: • Type 1 to check the old WebLM client communication status • Type 2 to enable the old WebLM client communication status • Type 3 to disable the old WebLM client communication status  Note: The user can enter the values specified above based on their usage.	This utility is used to check, enable, and disable the old WebLM client communication status with releases 10.1.3.1 and later. For the older WebLM client communication, the default status is ENABLED.	• Type 1 to check the old WebLM client communication status. • Type 2 to enable the old WebLM client communication status. • Type 3 to disable the old WebLM client communication status. If your input is 1 and the current status is enabled, the message <pre>Old WebLM client communication status is ENABLED</pre> is displayed. If the current status is disabled, the message <pre>Old WebLM client communication status is DISABLED</pre> is displayed. If your input is 2, the message <pre>Old WebLM client communication is now ENABLED</pre> is displayed. If your input is 3, the message <pre>Old WebLM client communication is now DISABLED</pre> is displayed.

Chapter 7: Resources

Avaya WebLM documentation

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

Title	Description	Audience
Implementing		
<i>Deploying standalone Avaya WebLM in Virtualized Environment</i>	Deploy the application in virtualized environment.	Implementation personnel
<i>Deploying standalone Avaya WebLM in Software-Only and Infrastructure as a Service Environment</i>	Deploy the application on software-only environment and cloud services.	Implementation personnel
<i>Upgrading standalone Avaya WebLM</i>	Upgrade the application.	Implementation personnel
Administering		
<i>Administering standalone Avaya WebLM</i>	Perform administration tasks	System administrators

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**.

Accessing the port matrix document

Procedure

1. Go to <https://support.avaya.com>.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support by Product > Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
 - **Application & Technical Notes**
 - **Design, Development & System Mgt**

The list displays the product-specific Port Matrix document.

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.

Training

The following courses are available at <http://www.avaya-learning.com/>. To search for the course, enter the course code in the **Search** field and click **Go**.

Course code	Course title
71201V	Integrating Avaya Aura® Core Components

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

 Note:

Videos are not available for all products.

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: Recommendations to select a WebLM configuration model

Depending on the need and infrastructure of an organization, the organization can configure WebLM in one of the following licensing models:

- WebLM standard model
- WebLM enterprise model

Related links

[WebLM standard licensing model](#) on page 97

[WebLM enterprise licensing model](#) on page 98

[WebLM configuration model checklist](#) on page 99

WebLM standard licensing model

WebLM standard licensing is an old model and offers an easy and simple solution with limited functionality. Use the standard configuration model if the Avaya product is a standalone product installed on a computer.

To configure a standard model, you must install a standard license file (SLF) and configure the WebLM server for the licensed applications to acquire the feature licenses.

The standard model provides the following information regarding the feature license usage:

- Usage at a particular time
- Peak usage for the last 7 days
- Peak usage for the last 30 days

The standard licensing model does not support many new features of WebLM.

The standard licensing model has the following limitations:

- The model does not offer any redundancy because the model uses only one WebLM server as the source of feature licenses. If the WebLM server fails or becomes unavailable due to any reason, the licensed applications do not have other means to acquire feature licenses or renew the acquired feature licenses.

- The model does not suit an organization that has licensed applications spread globally. All the licensed applications must contact a single WebLM server that might lead to network issues.
- In this model, the WebLM server does not maintain the usage history.

Related links

[Recommendations to select a WebLM configuration model](#) on page 97

[WebLM configuration model checklist](#) on page 99

WebLM enterprise licensing model

WebLM enterprise licensing is a more recent model and offers more features to the end user as compared to the WebLM standard licensing model. The WebLM enterprise licensing model provides the following features:

- Provides the flexibility to move feature licenses across various WebLM servers, master and local. Therefore, even if a WebLM server is unavailable or is out of feature licenses, the licensed applications can still acquire feature licenses from the other servers.
- Suits an organization that has licensed applications spread globally. With the enterprise model, the organization can have feature licenses allocated to various local WebLM servers, which in turn can serve licensed applications in a region. Additionally, with the usage history, the administrator can move WebLM feature licenses from local WebLM servers that have low usage to the local WebLM servers that have high usage.
- Periodic allocation. The licensed application can also acquire feature licenses from the master WebLM server. The unallocated feature licenses available with the master WebLM server are known as floating licenses. To avoid feature licenses being stagnant in a single location and maximize feature license usage, the allocation license files to local WebLM servers are valid only for 30 days. However, to ensure that local WebLM servers never run out of feature licenses, the master WebLM server copies the ALFs to the local WebLM servers after every seven days. If the periodic allocation process fails, the retry feature ensures that the system makes decent number of attempts to execute the process. If the periodic allocation process is not successful even after the retry attempts, the system notifies the administrator through an e-mail.
- Periodic usage query. The periodic usage query process retrieves feature license usage information from each local WebLM server configured on the master WebLM server or the floating license usage information from the master WebLM server after every seven days. Using the periodic usage query feature, administrators of the master WebLM server can ensure that administrators periodically receive feature license usage information, even if the administrators forget to execute a usage query.

The usage information from the WebLM servers across the organization helps administrators to determine if the purchased feature licenses are sufficient for the organization. If the feature licenses are insufficient, administrators can plan to purchase more feature licenses for the organization.

Related links

[Recommendations to select a WebLM configuration model](#) on page 97

[WebLM configuration model checklist](#) on page 99

WebLM configuration model checklist

The checklist for WebLM configuration model lists the features of WebLM with the summary of the features each configuration model supports.

The WebLM team creates the WebLM configuration model checklist. Use the checklist to decide the WebLM configuration model that suits the needs and infrastructure of your organization.

Feature	WebLM Standard model	WebLM Enterprise model
License Installation using user interface (UI)	Yes	Yes
Change Password	Yes	Yes
Feature Overuse	Yes	Yes
Manage Users (add, modify and delete)	Yes	Yes
License acquisition using client APIs - Pull model	Yes	Yes
Acquired license details	Yes	Yes
Update history count	No	Yes
Peak Usage (last 7 days)	Yes	Yes
Peak Usage (last 7 days) with history (max - 5)	No	Yes
Peak Usage (last 30 days)	Yes	Yes
Peak Usage (last 30 days) with history (max - 5)	No	Yes
Usage query	Yes	Yes
Usage query with history (max - 5)	No	Yes
LAR license type support	Yes	Yes
Enterprise configuration	No	Yes
E-mail notification - in case of failure (periodic operations)	No	Yes
Local WebLM configuration - Add	No	Yes
Local WebLM configuration - Delete	No	Yes
Local WebLM configuration - Modify	No	Yes
Perform validate connectivity test	No	Yes
View usage at Enterprise level	No	Yes

Table continues...

Recommendations to select a WebLM configuration model

Feature	WebLM Standard model	WebLM Enterprise model
Allocations (push ALF to Local WebLM) - Push mode	No	Yes
Periodic allocation (every 7th day)	No	Yes
Periodic usage query (every 7th day)	No	Yes
Redundancy	No	Yes
Floating license (available for acquisition)	No	Yes
Long term vision	No	Yes
HTTPS support	Yes	Yes
Client API Support (all APIs)	Yes	Yes

Related links

[Recommendations to select a WebLM configuration model](#) on page 97

Index

A

accessing port matrix	93
actual license usage	16
add	71
add element instances	63
Add local WebLM page	29
adding a local WebLM server	28
adding new users	46
adding trusted certificates	
WebLM	27
adding whitelist	
client certificate identity	19
adopter application	
cannot communicate with WebLM	75
Allocations by Local WebLM	40
attempt to reinstall license file	
fails	81
attempt to reinstall license file for a product fails	81
attempt to reinstall the license file for the same product	
fails	81
Avaya support website	95

C

CA certificate	71 , 72
CA Certificate	66 , 72
centralized licensing	60
adding elements	61
disable	64
enable	60
overview	60
centralized subscription licensing	59
overview	59
change password field description	13
changing	
password policy through CLI	53
WebLM password	12
changing allocations of a licensed feature	39
checklist	
WebLM configuration model	99
cipher suites	67
CLI operations	
WebLM	86
client certificate identity	
add whitelist	19
delete whitelist	20
disable whitelist validation	21
edit whitelist	19
enable whitelist validation	20
export whitelist	20
import whitelist	19
client truststore	72

collection	
delete	93
edit name	93
generating PDF	93
sharing content	93
command	
setSecurityPolicy	51
configure centralized licensing	61
field description	61
field descriptions	61
configure enterprise licensing	23
configuring	
TLS version	68
configuring inactivity timeout	47
configuring password policies	49
connectivity status of the local WebLM servers	22
content	
publishing PDF output	93
searching	93
sharing	93
sort by last updated	93
watching for updates	93
credential store	66

D

delete element instance mapping	63
delete element instances	63
Delete local WebLM page	31
delete mapping	63
deleting	
metering collector configuration	59
deleting an element instance	63
deleting CA certificate	72
deleting element instances	63
deleting instances	63
deleting users	46
deleting whitelist	
client certificate identity	20
disables the client certificate authentication	72
disabling centralized licensing	64
Disabling WebLM client certificate authentication	74
disabling whitelist validation	
client certificate identity	21
display	69
Display existing WebLM client certificate authentication	
configuration	73
displaying	
password policies	55
Displaying the password policies	55
documentation	
WebLM	92
documentation center	93

documentation center (*continued*)

finding content	93
navigation	93
documentation portal	93
finding content	93
navigation	93

E

edit assignment of a license file	62
edit element instances	63
editing element instances	62
editing password	46
editing the properties of an element instance	62
editing whitelist	
client certificate identity	19
element instance	
delete	63
edit	62
edit properties	62
remove	63
element instance field description	63
enable HTTPS	78
Enable WebLM client certificate authentication	73
enables the client certificate authentication	72
enabling	60
enabling whitelist validation	
client certificate identity	20
Enterprise Configuration page	25
enterprise licensing	
configure	23
enterprise WebLM model	
migrating to standard WebLM model	42
exporting whitelist	
client certificate identity	20

F

field descriptions	
Allocations by Feature	39
Change Allocations	41
Enterprise Usage	36
Metering Collector Configuration	58
Password Policy	49
server properties	45
view by feature	21
View License Capacity	16
View Peak Usage	18
WebLM Home	13
finding content on documentation center	93
finding port matrix	93
firewall block the port	77
forgot the password for WebLM	84
forgot WebLM password	85

I

Import CA Certificate	66
importCAcertificate	66
importing CA certificate	72
importing whitelist	
client certificate identity	19
inactivity timeout	
configure	47
incorrect	
browser settings	83
content type	83
registry settings	82, 83
InSite Knowledge Base	95
install license file	14
Install License page	15
installation of license file on the WebLM server fails	78, 83
invalid XML file	83

J

JBoss	78
JBoss configuration	78
JBoss failure	79

L

license file	
add mapping	62
install	14
special characters	80
tampered	80
license file installation	15
license file installation on the WebLM fails	78, 83
license file installation on WebLM fails	79–81, 83, 84
License file installation on WebLM fails	82
license file name	
special characters	80
license files and elements	61
list	71
local WebLM	29
local WebLM model	
migrating to standard WebLM model	42
local WebLM server	
remove	30
logging on	
WebLM web console	12
logging out	
WebLM server	65

M

MAC address mismatch	80
MAC address of server	45
Manage users field description	47
manageCACertificates	71

manageWebLMCertificate	69	removing local WebLM server	30
managing		removing users	46
command-line password policy	52	Replacing WebLM certificate with a third-party certificate ...	70
WebLM application server	65	resetting the password	13
managing users	46	restoring	
mapping elements and license files	61	default password policy settings	56
Metering Collector configuration		Restoring the default password policy settings	56
overview	58	retrieving	
migrating		local WebLM certificate	27
enterprise WebLM model to standard WebLM model ..	42		
local WebLM model to standard WebLM model	42	S	
modify local WebLM field description	31	searching for content	93
Modify local WebLM page	32	Server Host ID	45
modifying a local WebLM server configuration	31	Server Properties	45
modifying password	46	server properties; view	44
My Docs	93	setting usage history count	45
		setWebLMClientAuth	72
		setWebLMClientAuth command	73, 74
		sharing content	93
		sort documents by last updated	93
		support	95
N			
network connectivity	77	T	
new in release		tampered license file	80
WebLM 10.1.2	7	toggleing	
new users; add	46	cipher suites on WebLM	67
		Training	94
P		troubleshooting	
password history policy	48	WebLM	75
password policies		truststore	72
configure	49		
Password Policy field description	49	U	
password reset	84	unable to launch WebLM	76–78
password strength policy	48	Uninstall License page	44
peak usage for a licensed product	17	uninstalling a license file	44
peak usage; view	17	unsupported content type	82
Periodic Status	42	Upgrading CM license file version to 10.1	64
periodic status of master and local WebLM servers	41	URL formats	77
port matrix	93	Usage by local WebLM page	35
proposed solution	77, 78, 83, 85	usage history count	45
		Usage Summary page	35
Q		users; delete	46
Query Usage page	37		
querying usage of feature licenses for master and local		V	
WebLM servers	34	Validating connectivity to local WebLM servers	23
		videos	94
R		view	71
recommendations to select WebLM enterprise model	98	View by local WebLM page	22
recommendations to select WebLM standard model	97	view last contacted status of the local WebLM servers	22
refreshing		view license capacity	16
default password policy settings	57	View Local WebLMs page	23
refreshing the default password policy settings	57	view periodic status of master and local WebLM servers ...	41
Regenerating a self signed WebLM certificate	70		
reinstall license file	81		
related training courses	94		
remove	71		

viewing	
password policy status	55
Viewing a WebLM certificate	69
viewing allocations by features	38
viewing allocations by local WebLM	39
viewing enterprise usage of a license feature	34
viewing license capacity	16
viewing license capacity of a feature	21
viewing peak usage	17
viewing server properties	44
viewing the password policy status	55
viewing usage by WebLM	33
viewing usage summary	33

W

watch list	93
WebLM	72
forgot password	84 , 85
overview	10
WebLM 10.1.2	
new in release	7
WebLM CLI operations	86
WebLM Client	66
WebLM Client Truststore	66
WebLM command line interface operations	86
WebLM configuration model	97 , 99
WebLM overview	10
WebLM server	
deleting	30
removing	30
WebLM servers	
periodic status	41
WebLM standard model	97
WebLM TLS configuration	68

X

XML file invalid	82
------------------------	--------------------