Oracle® Communications Session Element Manager

SOAP API Guide

Release 9.0
F52431-02
September 2022

Oracle Communications Session Element Manager SOAP API Guide, Release 9.0

F52431-02

Copyright © 2022, 2022, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

About This Guide

My Oracle Support xiii

Revision History

1 Overview

Using the Apache CXF Client on the Session Delivery Manager Server 1-2
- Configure and Run the CXF Client 1-2

Web Services Definition Language Data Structures 1-4
- DeviceInfoObject 1-4
- IntegrityCheckResult 1-4
- NNCDetails 1-5
- NNCServerIPInfo 1-5
- SaveDeviceTaskMessage 1-5
- SBCDetails 1-6
- WSBatch 1-6
- WSBatchOperation 1-6
- WSConfigAttribute 1-6
- WSConfigAttributeMetaData 1-6
- WSConfigAttributeMetaData. AttributeValueTypeInfo 1-7
- WSConfigElement 1-7
- WSConfigElementMetaData 1-8
- WSConfigResult 1-8
- WSDeviceResult 1-8

Exceptions Faults 1-8
- AcmeWSFault 1-8
- AcmeAdminWSFault 1-8
- AcmeConfigWSFault 1-8
- AcmeDeviceWSFault 1-9

Sample Work Flow 1-9

2 Administration Level

UsingExternalAAA 2-1
- Input Parameters 2-1
- Output Parameters 2-1
- Throws 2-1

login 2-1
- Input Parameters 2-1
- Output Parameters 2-1
- Throws 2-1

logOut 2-2
- Throws 2-2
- Input Parameters 2-2
- Output Parameters 2-2
- Throws 2-2

getUserInfo 2-2
- Input Parameters 2-2
- Output Parameters 2-2
- Throws 2-3

getAllUserInfo 2-3
- Input Parameters 2-3
- Output Parameters 2-3
- Throws 2-3

getAccountManagementInfo 2-3
- Input Parameters 2-4
- Output Parameters 2-4
- Throws 2-4

getLoginBanner 2-4
- Input Parameters 2-4
- Output Parameters 2-4
- Throws 2-4

getTrapReceivers 2-4
- Input Parameters 2-4
- Output Parameters 2-4
- Throws 2-5

NorthboundalarmSync 2-5
- Input Parameters 2-5
- Output Parameters 2-5
- Throws 2-6

NorthboundActiveAlarmSync 2-6

3 Device Management

addDevice 3-1
- Input Parameters 3-1
- Output Parameters 3-1
- Throws 3-1

loadDevice 3-1
- Input Parameters 3-1
- Output Parameters 3-2
- Throws 3-2

deleteDevice 3-2
- Input Parameters 3-2
- Output Parameters 3-2
- Throws 3-2

saveConfig 3-2
- Input Parameters 3-2
- Output Parameters 3-2
- Throws 3-3

activateConfig 3-3
- Input Parameters 3-3
- Output Parameters 3-3
- Throws 3-3

saveAndActivateConfig 3-3
- Input Parameters 3-4
- Output Parameters 3-4
- Throws 3-4

getAllManagedDevicesNames 3-4
- Input Parameters 3-4
- Output Parameters 3-4
- Throws 3-4

getAllManagedDevicesbyDeviceGroup 3-4
- Input Parameters 3-4
- Output Parameters 3-5
- Throws 3-5

getSBCDetails 3-5
- Input Parameters 3-5
- Output Parameters 3-5
- Throws 3-5

getDevicePollingInterval 3-5
- Input Parameters 3-5
- Output Parameters 3-5

Throws 3-6
lockDevice 3-6
Input Parameters 3-6
Output Parameters 3-6
Throws 3-6
unlockDevice 3-6
Input Parameters 3-6
Output Parameters 3-6
Throws 3-6
getAllDeviceGroupList 3-7
Output Parameters 3-7
Throws 3-7
addDeviceGroup 3-7
Input Parameters 3-7
Output Parameters 3-7
Throws 3-7
deleteDeviceGroup 3-7
Input Parameters 3-8
Output Parameters 3-8
Throws 3-8
getLCVContentSaveSessionReport 3-8
Specified by 3-8
Input Parameters 3-8
Output Parameters 3-8
Throws 3-8
getAllManagedDevices 3-8
Specified by 3-9
Input Parameters 3-9
Output Parameters 3-9
Throws 3-9
getAllManagedDeviceTargetNames 3-9
Specified by 3-9
Input Parameters 3-9
Output Parameters 3-9
Throws 3-9
getNNCDetails 3-9
Specified by 3-10
Input Parameters 3-10
Output Parameters 3-10
Throws 3-10
getTopLevelElementCount 3-10

Specified By 3-10
Input Parameters 3-10
Output Parameters 3-10
Throws 3-10
getAllAssociatedDevicesInEMSLicense 3-11
addDeviceToEMSLicense 3-11
removeDeviceFromEMSLicense 3-11

4 Configuration Management Level

getPrimaryKeyByElementType 4-1
Input Parameters 4-1
Output Parameters 4-1
Throws 4-1
getTopLevelConfigElementTypeNames 4-1
Input Parameters 4-1
Output Parameters 4-2
Throws 4-2
getSubElementTypesByElementType 4-2
Input Parameters 4-2
Output Parameters 4-2
Throws 4-2
getRequiredSubElementTypesByElementType 4-2
Input Parameters 4-2
Output Parameters 4-3
Throws 4-3
getAllSupportedAttributeInfoByElementType 4-3
Input Parameters 4-3
Output Parameters 4-3
Throws 4-3
deleteConfigElement 4-3
Input Parameters 4-3
Output Parameters 4-4
Throws 4-4
updateConfigElement 4-4
Input Parameters 4-4
Output Parameters 4-4
Throws 4-5
getConfigElement 4-5
Input Parameters 4-5
Output Parameters 4-5

Throws 4-5
getAllConfigElements 4-5
Input Parameters 4-5
Output Parameters 4-5
Throws 4-6
applyBatch 4-6
Input Parameters 4-6
Output Parameters 4-6
Throws 4-6
addConfigElement 4-6
Input Parameters 4-6
Output Parameters 4-6
Throws 4-7
replace 4-7
Input Parameters 4-7
Output Parameters 4-7
Throws 4-7
addSubElement 4-7
Input Parameters 4-7
Output Parameters 4-8
Throws 4-8
deleteSubElement 4-8
Input Parameters 4-8
Output Parameters 4-8
Throws 4-8
getConfigElementMetaData 4-8
Input Parameters 4-9
Output Parameters 4-9
Throws 4-9
getConfigAttributeMetaData 4-9
Input Parameters 4-9
Output Parameters 4-9
Throws 4-9
getValuesForReferenceAttribute 4-9
Input Parameters 4-9
Output Parameters 4-10
Throws 4-10
newConfigElement 4-10
Input Parameters 4-10
Output Parameters 4-10
Throws 4-10

encryptedPassword 4-10
Input Parameters 4-10
Output Parameters 4-10
Throws 4-11
deleteUserChanges 4-11
Input Parameters 4-11
Output Parameters 4-11
Throws 4-11

A Meta Data Tables

Table Name - ikeSanInfo A-1
Security-policy - Table Name - spdConfig A-2
Security-policy - Table Name - networkInterfaceId A-3
Security-policy - Table Name - spdFineGrained A-3
SIP Interface - Table Name - sipInterface A-4
SIP Interface - Table Name - sipPort A-8
SIP Interface - Table Name - addSdpProfilesInMsg A-9
SIP Interface - Table Name - mediaProfile A-10

B ACLI to ACP Mappings

Retrieve Element Metadata and Attributes B-1
Retrieving the ACLI to ACP Mapping B-1
Physical Interface B-3
Network Interface B-4
Realm B-5
Realm Media Address B-8
Surrogate Agent B-9
SIP Interface B-9
SIP NAT B-13
H.323 Stack B-13
MGCP Config B-15
DNS Config B-16
Session Agent B-17
Session Agent Group B-21
Local Policy B-21
Network Management Control B-25
SIP Header Manipulation B-26
Session Constraints B-34
Session Translation B-35

Translation Rules B-35
RPH Profile B-35
RPH Policy B-36
Host Routes B-36
SIP Local Map Entry B-36
Codec Policy B-38
Access Control B-39
Media Profile B-39
SIP Response Map B-40
Diameter Director Agent B-40
Diameter Director Configuration B-41
Diameter Director Constraints B-42
Diameter Director Group B-43
Diameter Director Interface B-44
Diameter Manipulation B-45

C Running a Legacy SOAP Client API

About This Guide

This document and other product-related documents are described in the Related Documentation table.

Related Documentation

Table 1 Oracle Communications Product Plug-in Documentation Library

Document Name	Description
Session Element Manager User Guide	Provides information for managing and optimizing network infrastructure elements and their functions with comprehensive tools and applications used to provision fault, configuration, accounting, performance, and security (FCAPS) support for managed network functions and their associated devices in Oracle Communications Session Delivery Manager (SDM).
Report Manager User Guide	Provides information about configuring Report Manager to interoperate with Oracle BI Publisher as well as creating reports on Session Delivery product network devices.
Report Manager Installation Guide	Provides information for installing Oracle Communications Report Manager product as an addition to SDM including the Oracle database and BI Publisher components. The Oracle session delivery product plugin must be added to Oracle Communications Session Delivery Manager before performing the Report Manager installation.
Route Manager User Guide	Provides information for updating local route table (LRT) data on a single device or multiple devices.

Table 2 Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Administration Guide	Provides the following administration information: • Implement SDM on your network as a standalone server or high availability (HA) server. • Login to the SDM application, access GUI menus including help, customize the SDM application, and change your password. • Access the product plugin service through the GUI to manage product plugin tasks, including how product plugins are uploaded and installed. • Manage security, faults, and transport layer security certificates for east-west peer SDM server communication, and southbound communication with network function (NF) devices. • Configure northbound interface (destination) fault trap receivers and configure the heartbeat trap for northbound systems. • Monitor SDM server health to detect heartbeat messages and display the server status to prevent health problems, or view server disk utilization information and server directory statistics. • Maintain SDM server operations, which includes database backup and database restoration and performing server cluster operations. • Use available SDM server scripts, the contents of fault trap notifications, and a list of northbound notification traps generated by the SDM server.
Installation Guide	Provides the following installation information: • Do pre-installation tasks, which include reviewing system requirements, adjusting linux and firewall settings, completing SDM server settings and configuring your NNCentral account for security reasons. • Do the typical installation to perform the minimal configuration required to run the SDM server. • Do the custom installation to perform more advanced configurations including the mail server, cluster management, Route Manager, transport layer security (TLS), and Oracle database configuration.
Release Notes	Contains information about the administration and software configuration of the SDM feature support new to this release.

Table 2 (Cont.) Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Security Guide	Provides the following security guidelines: • Use guidelines to perform a secure installation of SDM on your server, which includes methods for securing the server, firewall settings, system support for encryption and random number generators (RNG), using HTTPS, and password guidelines. • Review Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system. • Follow a checklist to securely deploy SDM on your network and maintain security updates.
REST API Guide	Provides information for the supported REST APIs and how to use the REST API interface. The REST API interface allows a northbound client application, such as a network service orchestrator (NSO), to interact with SDM and its supported product plugins.
SOAP API Guide	The SOAP API guide provides information for the SOAP and XML provisioning Application Programming Interface (API) client and server programing model that enables users to write client applications that automate the provisioning of devices. The web service consists of operations that can be performed on devices managed by the SDM server and data structures that are used as input and output parameters for these operations.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Revision History

This section provides a revision history for the document.

Date	Revision
April 2022	• Initial Release.
September 2022	• Added the Appendix Metadata Tables.

1 Overview

The deprecated Oracle Communications Session Delivery Manager SOAP API is a SOAP and XML provisioning Application Programming Interface (API) client and server programing model that enables users to write client applications that automate the provisioning of devices. The web service consists of operations that can be performed on devices managed by the Oracle Communications Session Delivery Manager server and data structures that are used as input and output parameters for these operations.

> **Important:**
>
> With the introduction of Oracle Communications Session Delivery Manager, Release 8.0, the SOAP API client is provided for backwards compatibility only. The SOAP API will not support any new APIs for new SDM enhancements. Use the REST API for Oracle Communications Session Delivery Manager if you require access to new SDM features via a programmatic API.

The Oracle Communications Session Delivery Manager server accepts and responds to requests from clients that are coded to use the API. The server responds to requests to read and update configuration data in the Oracle Communications Session Delivery Manager SOAP API database or apply configurations to devices in the same way in which it responds to requests from the GUI client application. These messages that are exchanged between SOAP and XML clients and the server are encapsulated in the standard Simple Object Access Protocol (SOAP) format, as defined by the World Wide Web Consortium (W3C).

The provisioning API has the following components:

- Active configuration—The read-only configuration on the device.
- Session ID—Identifies the connection that is established between a SOAP client application instance and the Oracle Communications Session Delivery Manager server. The session ID (SID) is used by the server to distinguish between multiple clients currently logged in, and is a required parameter for almost all operations supported by the API.
- Managed device—The API supports all managed objects (configuration elements) and sub-objects (sub-elements) available on the device.

> **Note:**
>
> This guide covers the basic configuration parameters for session delivery product devices. See your session delivery product device documentation, such as its ACLI guide, for more configuration information that is beyond the scope of this guide and may be specific to the release of the your devices.

Using the Apache CXF Client on the Session Delivery Manager Server

The Oracle Communications Session Delivery Manager server incorporates Apache CXF technology to handle the processing of the SOAP messages received from the client. Apache CXF is a full-featured, open-source SOAP web services framework. See the W3.org for more information on SOAP.

The Apache CXF client is used by a user to integrate automated provisioning into an existing OSS infrastructure. The CXF client application is custom-built to use the published API to read and set parameters in the configurations in the server database, modify configuration data for device groups associated with an offline configuration, and to apply those settings to devices being managed by the server. The CXF client application is written in any language that supports SOAP/XML-based Web Services and examples are provided for clients written in Java in the software distribution.

The server supports simultaneous connections from multiple SOAP clients and graphical user interface (GUI) clients. User profiles defined in the Oracle Communications Session Delivery Manager SOAP API database are used to validate login requests from either type of client, but profiles can be defined only through the GUI interface. Audit trail entries are generated for operations performed by all clients, whether they are GUI or SOAP-based. For more information about SOAP-based Web Service and examples of client code, see the CXF User's Guide.

Configure and Run the CXF Client

You must perform all the steps below before executing the run script.

Sample client code is available at {CXFClient_HOME}/sampleSource folder.

1. Unzip the CXFClient.zip to a folder on the client system. This folder provides the {CXFClient_HOME}.
2. Go to the following directory:

   ```
   {CXFClient_HOME}/bin
   ```

3. Edit the **run.sh** bash file that allows you to run the sample client code by changing the JAVA_HOME path variable to match the JDK installation path.

   > **Note:**
   >
   > The CXF Client uses JDK 1.8.

4. Edit the **build.sh** bash file to build an executable image by making the same change to the JAVA_HOME path variable.
5. The following substeps enable the Web Service interface to run over HTTPS.

> **Note:**
>
> These steps can be safely ignored if client/server transactions occur over unsecured HTTP.

a. Use FTP to move a copy of the Oracle Communications Session Delivery Manager server public certificate to the ssl folder.

b. Use the Java keytool utility to import the public certificate into a specified Java keystore. For example, the following command imports the **OCSDM.cert** certificate file into a keystore named **trustedCerts**:

```
keytool -import -keystore trustedCerts -alias ocsdm-cert -file
OCSDM.cert
```

This keystore file is referenced by the ocsdm-cert alias.

> **Note:**
>
> You will be prompted for the keystore password before the import operation is initiated.

c. Edit the **run.sh** bash file by changing the TRUST_STORE variable to match the location of the Java keystore that contains the public certificates of associated Oracle Communications Session Delivery Manager servers:

```
TRUST_STORE=../ssl/trustedCerts
```

d. Edit the **run.sh** bash file by changing the TRUST_STORE_PASSWORD to match the password required to access the Java keystore that contains the Oracle Communications Session Delivery Manager server certificates.

e. Use the Java keytool utility to confirm the presence of the key in the keystore. For example:

```
keytool -list -v -keystore trustedCerts
```

This command provides a verbose display of the contents of the target Java keystore, which in this case is trustedCerts.

> **Note:**
>
> You will be prompted for the keystore password before the keystore contents are displayed.

f. Repeat the previous sub steps for each additional Oracle Communication Session Delivery Manager server associated with the client.

6. Optionally edit {CXFClient_HOME}/conf/client.properties by changing the value of the session_timeout_ms property to specify a non-default session timeout value, expressed in milliseconds.

7. Edit the **run.sh** bash file by changing the SERVER_NAME variable to point to NNC server machine name.
8. Edit the **run.sh** bash file by changing the SERVER_PORT variable to point to NNC server machine port.
9. Use build.bat to compile the client application.
10. Use run.bat to run the client application.

Web Services Definition Language Data Structures

Web Services Definition Language (WSDL) files contain data structures that are used in the API. These files are included in the Oracle Communications Session Delivery Manager software distribution by entering the following URL in your browser for the Oracle Communications Session Delivery Manager server:

```
http://<ip address>:8080/ACMEWS/services
```

The <*ip-address*> is the IP address of your Oracle Communications Session Delivery Manager server. Use the links on the right side of the screen to display the following WSDL files that contain WSDL definitions for data structures:

- AdminMgmtIFService.wsdl
- ConfigMgmtIFService.wsdl
- DeviceMgmtIFService.wsdl

DeviceInfoObject

DeviceInfoObject is a data structure that contains the information necessary to add a device to NNC system.

- Arraylist<String> deviceIPList
- String username
- String Password
- String communityName
- int snmpPort
- String deviceGroupName, which will be the full path of device group, if we have a device group (groupAA1) under group1/groupAA, the client need to pass group1/groupAA/groupAA1
- WebServicesProtcolEnum, which is a enumeration contains (HTTP or HTTPS), this piece information is only used by 2600 series device.
- WebServicesProtcolEnum webServicesProtcol, this piece information is only used by 2600 series device.

IntegrityCheckResult

IntegrityCheckResult contains top-level element count information as follows.

- String elementName; the name of the target element

- int ElementCount; the number of element instances

NNCDetails

NNCDetails contains product version information as follows.

- String version; The product version, for example, NNC7.0.0

NNCServerIPInfo

NNCServer contains NNC-Server-specific data as follows.

- String serverIPAddress;
- String serverName;
- String serverStatus;
- long inactivityCount;
- int heartBeatFailureMeter;
- int maxHeartBeatFailureMeter;
- long missedHBCount;
- long heartBeatCount;
- String lastHeartBeatTime;
- String downTime;
- String upTime;
- int resetCount;

SaveDeviceTaskMessage

SaveDeviceTaskMessage contains the result of save and/or activate operation as follows.

- String operation, operation type, Save or SaveAndActivate, Activate
- String tasked, which is task id which will be populated on devicetaskDetails schema once save or save\activate is fully done on server side.
- String username, which contains the user name who is going to perform save or activate operation
- String deviceName, device name the operation is performed.
- String isLockSuccess, specifies SBC Lock status
- isValidationSuccess, does the validation pass for the configuration elements integrity check
- String isEraseCacheSuccess, which is not applicable for granular save
- String isCreateSuccess specifies success or failure
- String isIntegrityCheckSuccess, if EMS count match to the SBC count
- String isRestoreConfigSuccess if Integrity check fail, we need to restore original SBC configuration data.
- String isSaveConfigSuccess, specifies success or failure of Save command

- isActivateConfigSuccess, specifies success or failure of Activate command
- isUnlockSuccess, specifies SBC Unlock status

SBCDetails

SBCDetails contains information describing the SBC configuration as follows.

- String deviceName, device name
- String targetName, target name
- String domainName, which is device group path
- String SBCVersion, SBC version, such as SC620
- String snmpCommunityName, snmp community name
- int snmpPort, snmp port
- String primaryIP, primary IP address
- String secondaryIP, secondary IP address
- String hardwareVersion, hard ware version, such as NN4500, NN4200

WSBatch

WSBatch contains information describing a SOAP batch operation as follows.

- ArrayList < WSBatchOperation > operationsToApply, Arraylist of WSBatchOperations, described in the following section.

WSBatchOperation

WSBatchOperation contains information describing SOAP batch operation content.

- String operation, operation can be ADD, UPDATE, DELETE
- WSConfigElement configElement, which is a data structure described before.

WSConfigAttribute

WSConfigAttribute contains configuration attribute information as follows.

- String name: the name of the attribute
- String value: the value of the attribute

WSConfigAttributeMetaData

WSConfigAttributeMetaData contains attribute-specific meta data as follows.

- String name; The name of the attribute
- String acliName The ACLI name for the attribute
- AttributeValueTypeInfo valueTypeInfo; The type information of attribute.
- String delimiter; null if the value of this attribute is not delimited string.

- boolean isRequired; true, if this attribute is a required to configure the parent element
- String defaultValue; The default value
- String referred_Element_Type_Name;: If this attribute is referring to another element, that element's type name.
- List<String> suggested_Values;: A list of suggested values for this attribute.
- List<WSNumericRange> valid_Numeric_Range; The valid range of numeric values for this attribute. Applicable only if valueTypeInfo is NUMERIC
- List<String> enumerated_values; A list of valid enumeration for this attribute

WSConfigAttributeMetaData. AttributeValueTypeInfo

WSConfigAttributeMetaData.AttributeValueTypeInfo contains Enumerations of valid attribute types as follows.

- This is an enumeration of valid types of an attribute.
- numeric
- string
- delimited_string
- ipaddress
- boolean
- date
- enumerated_value,
- reference_to_another_element
- ipaddress_and_portnumber

WSConfigElement

WSConfigElement is the generic data structure for all configuration elements. This data structure is used by add/update/delete/get functions to describe a new or modified configuration element. It contains the following data:

- String type: identifies the target configuration element. Top-level configuration elements are identified by their Acme Control Protocol (ACP) element names, for example sipManipulation.
- ArrayList<WSConfigAttribute> attributeList: an Arraylist of WSConfigAttributes
- ArrayList <WSConfigElement> children: ArrayList of WSConfigElements. that provides information on sub-elements.
  Sub-elements type (children) are identified by a path expression rooted in an ACP element, for example, sipManipulation/headerRule/elementRule specifies an Element Rule
- String elementTypePath: which is used internally to specify the path expression (for example sipManipulation/headerRule/elementRule). Because this tag is generated internally, the client does not need to set this data.

WSConfigElementMetaData

WSConfigElementMetaData contains element-specific meta data as follows.

- private String type; The type name of the element
- private boolean isSingleInstance;: true, if this element is a single instance
- private String elementTypePath; The full path of the element starting from the root configuration
- private List<String> subElementTypeNames; A list of sublement type names of this element
- private List<WSConfigAttributeMetaData> attributeMetaDataList; A list of attribute metadata for this element

WSConfigResult

WSConfigResult contains the result of an operation as follows.

- Boolean resultFlag: status of the operation
- String objectId: objectId value
- ArrayList of validation message string

WSDeviceResult

WSDeviceResult contains the result of network level (device) operation as follows.

- Boolean resultFlag: status of the operation
- ArrayList<String> validationMessage , the success or fail message

Exceptions Faults

The following exceptions may be generated by the server in attempting to process requests from a SOAP/XML interface client.

AcmeWSFault

AcmeWSFault is the base exception class for the web service interface.

AcmeAdminWSFault

AcmeAdminWSFault is the exception class for managing administrative level (AdminMgmtIF) APIs (login and logOut). In the event of an access error, AdminMgmtIF throws this exception.

AcmeConfigWSFault

AcmeConfigWSFault is the exception class for managing configuration level (DeviceConfigIF) APIs. In the event of a configuration error, AdminConfigIF throws this exception.

AcmeDeviceWSFault

AcmeDeviceWSFault is the exception class for managing device level (DeviceMgmtIF) APIs. In the event of a device-level error, AdminDeviceIF throws this exception.

Sample Work Flow

The following procedure illustrates the creation of a WSConfigElement the defines a specific network interface, and associated keep-alive mechanisms. Refer to WSConfigElement for details.

1. Use the login administrative API to access a Oracle Communications Session Delivery Manager SOAP API server
2. Use the newConfigElement API to create a template (actually a WSConfigElement data structure with default attribute values) of the networkInterface Type.
3. Construct an ArrayList of WSConfigAttribute data structures to assign local attribute values to the default networkInterface template returned by newConfigElement. Refer to WSConfigAttribute for details.
4. Add this attribute ArrayList to the networkInterface WSConfigElement data structure. This step completes configuration of the top-level networkInterface.
5. Use the newConfigElement API to create a second-level (child) template of the networkInterface/GWHeartbeat Type.
6. Construct an ArrayList of WSConfigAttribute data structures to assign local attribute values to the default networkInterface/GWHeartbeat template returned by newConfigElement.
7. Add the attribute ArrayList to the child template. This step completes configuration of the second-level child.
8. Construct an ArrayList of child WSConfigElements; in this case the array contains only a single element.
9. Append this child ArrayList to the WSConfigElement data structure.
10. Use the addConfigElement API to commit the WSConfigElement to the configuration database.
11. Logout, using the logOut API

2
Administration Level

UsingExternalAAA

The UsingExternalAAA object displays the RADIUS server domain for external user authentication.

Input Parameters

None

Output Parameters

- Boolean values are true if external authentication is used or false if it is not.

Throws

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

login

login is used by the CXF client to login to the CXF Web service.

```
public java.lang.String login(java.lang.String username,
java.lang.String password)
throws com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

Input Parameters

- username: username information
- password: password information

Output Parameters

- String sessionId

Throws

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

logOut

logOut ends the current user session.

```
public com.acmepacket.ems.ws.service.userobjects.WSDeviceResult
logOut()
throws com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

Throws

```
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

Input Parameters

None

Output Parameters

- WSDeviceResult data structure

Throws

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getUserInfo

Retrieves the values for the following parameters for a user:

- Account Never Expires
- Account Expires
- Password Never Expires
- Password Expires (Days)
  Public UserInfo getUserInfo(String userName) throws AcmeAdminWSFault

Input Parameters

- userName- - user name

Output Parameters

UserInfo

- Boolean accountExpire
- String accountExpirationDate
- Boolean passwordExpire
- String passwor ExpirationDate

- String userName

Throws

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getAllUserInfo

Retrieves the values for the following parameters for all users added to the system:

- Account Never Expires
- Account Expires
- Password Never Expires
- Password Expires (Days)
  Public UserInfo getUserInfo(String userName) throws AcmeAdminWSFault

Input Parameters

None

Output Parameters

UserInfo

- Boolean accountExpire
- String accountExpirationDate
- Boolean passwordExpire
- String passwor ExpirationDate
- String userName

Throws

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getAccountManagementInfo

Retrieves the values for the following parameters:

- Password Reuse Count
- Inactivity Time for admin user
- Inactivity Time for non-admin user

```
Public AccountManagementInfo getAccountManagementInfo() throws
AcmeAdminWSFault
```

Input Parameters

None

Output Parameters

AccountManagementInfo

- Int passwordResuseCount
- Int adminUserInactivityTimeout
- Int nonAdminUserInactivityTimeout

Throws

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getLoginBanner

Retrieves the the login banner.

```
Public String getLoginBanner() throws AcmeAdminWSFault
```

Input Parameters

None

Output Parameters

- String loginBanner

Throws

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getTrapReceivers

Retrieves the trap receiver information.

```
Public String getLoginBanner() throws AcmeAdminWSFault
```

Input Parameters

None

Output Parameters

TrapReceiver

- String ipaddress
- Int udpPort
- String communityName

Throws

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

NorthboundalarmSync

The NorthboundalarmSync API forwards traps stored in Oracle Communications Session Delivery Manager system to the network management system.

The following trap receiver states are used to identify the status of northbound alarm synchronization:

- Enabled
- Disabled
- Suspended
- Syncing
- SyncSucceed
- SyncFailed

Once you add the trap receiver to Oracle Communications Session Delivery Manager, the initial trap receiver state is set to **Enabled**. Following the Enabled state, the NorthboundalarmSync request is sent to the Oracle Communications Session Delivery Manager server. If unsuccessful, the AcmeWSAdminFault Exception is thrown.

Input Parameters

- destTrapReceiverIP: Destination trap receiver IP address
- startTime - Start sync time in MM/dd/yyyy HH:mm:ss (OCSDM server local time)
- endTime - End sync time in MM/dd/yyyy HH:mm:ss (OCSDM server local time)

Output Parameters

A WSAlarmSyncResult data structure.

The detail of this data structure is as follows:

1. Boolean resultFlag: either true or false
2. ArrayList<String > validationMessage: Validation message
3. Int numOfTrapsTobeSync: The number of the Alarms to be sync if successful

Throws

```
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

NorthboundActiveAlarmSync

The NorthboundActiveAlarmSync API forwards traps stored in the Alarm table in the Oracle Communications Session Delivery Manager database to the destination trap receiver within a specified time period.

The following trap parameters are used to identify the destination trap receiver, the minimum alarm severity state to synchronize, and the time interval for northbound active alarm synchronization:

- trapReceiverIP—The destination trap receiver IP address.
- minimumSeverity—The minimum alarm severity it is a severity String, the possible value can be Clear, Warning, Minor, Major, Critical, the API will forward the user specified severity alarms plus all the way up severity Alarms to the desired network. For example, if the user specifies Minor, It will forward all of Alarms which has severity from Minor, Major, Critical and Emergency to the target trap receiver.
- startSyncTime—The local start time (mm/dd/yyyy hh:mm:ss) for when traps are forwarded from the NNC server. If the user enters a null value, the startSyncTime is not used for a query.
- endSyncTime—The local end time (mm/dd/yyyy hh:mm:ss) for when traps are forwarded from the NNC server. If the user enters a null value, the endSyncTime is not used for a query.

The WSAlarmSyncResult object is returned. If the execution of the API is unsuccessful, the AcmeWSAdminFault exception is thrown.

3
Device Management

addDevice

The addDevice API adds device details to the configuration database.

> **Note:**
>
> When you add a device through the addDevice API, you can only create a network function (NF) with the name of the target device only.

public com.acmepacket.ems.ws.service.userobjects.WSDeviceResult addDevice(com.acmepacket.ems.ws.service.userobjects.DeviceInfoObject deviceInfoObject)throws com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- deviceInfoObject - - DeviceInfoObject data structure

Output Parameters

WSDeviceResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault

loadDevice

loadDevice adds a new managed device to the configuration database.

public com.acmepacket.ems.ws.service.userobjects.WSDeviceResult loadDevice(java.lang.String targetName) throws com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetName: target name information

Output Parameters

WSDeviceResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

deleteDevice

deleteDevice deletes configuration data from database, including device detail and configuration document information.

public com.acmepacket.ems.ws.service.userobjects.WSDeviceResult deleteDevice(java.lang.String targetName) throws com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetName---target name information

Output Parameters

WSConfigResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

saveConfig

saveConfig pushes configuration dataset changes to the SBC.

public com.acmepacket.ems.common.SaveDeviceTaskMessage saveConfig(java.lang.String targetName)throws com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetName - - target name information (for example,sd80_sd8)

Output Parameters

SaveDeviceTaskMessage, a data structure described as before.

Throws

com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

activateConfig

activateConfig promotes a specified configuration to the running configuration area.

public com.acmepacket.ems.common.SaveDeviceTaskMessage
activateConfig(java.lang.String targetName)throws
com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault,
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetName - - target name information

Output Parameters

SaveDeviceTaskMessage, a data structure described as before.

Throws

com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault - - throws exception while error occurs com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

saveAndActivateConfig

> **Note:**
>
> If there is a validation failure when using this API in Oracle Communication Session Delivery Manager Release 8.0 or later, the status flags in the message returned to the SOAP client appear differently than they did in Release 7.5M3. For example, in Release 7.5M3, the **isLockSuccess** and **isUnlockSuccess** flags in the SOAP response are listed as **UNKNOWN** after a validation failure. In Release 8.0, these flags change to **SUCCESS** after a validation failure because the device is locked before validation starts, while in the previous release, the device is locked after completing validation.

saveAndActivateConfig first runs saveConfig, and then activateConfig.

public com.acmepacket.ems.common. SaveDeviceTaskMessage
saveAndActivateConfig(java.lang.String targetname)throws
com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault,
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetName- - name of the target device

Output Parameters

SaveDeviceTaskMessage, a data structure described as before

Throws

com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getAllManagedDevicesNames

getAllManagedDevicesNames returns a list of all managed device names present in the configuration database.

public java.util.ArrayList<java.lang.String> getAllManagedDevicesNames()throws com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

None

Output Parameters

an ArrayList of Managed device target name, such as 172.30.80.81, 172.30.80.150-172.30.80.131

Throws

com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getAllManagedDevicesbyDeviceGroup

getAllManagedDevicesByDeviceGroup returns a membership list for a specified device group.

public java.util.ArrayList<com.acmepacket.ems.ws.service.userobjects.SBCDetails> getAllManagedDevicesByDeviceGroup(java.lang.String devicetGroupPath) throws com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- devicetGroupPath - -- device group full path, for example,group2/groupAC/groupAC1

Output Parameters

ArrayList of SBCDetails object

Throws

com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getSBCDetails

getSBCDetails returns information of a specified SBC.

public com.acmepacket.ems.ws.service.userobjects.SBCDetails getSBCDetails(java.lang.String targetName)throws com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetName, - the target name

Output Parameters

SBCDetails object

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getDevicePollingInterval

Retrieves the the polling interval set to poll SBCs.

Public int getDevicePollingInterval() throws AcmeAdminWSFault, AcmeDeviceWSFault

Input Parameters

None

Output Parameters

Device Polling Interval (seconds)

Throws

com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

lockDevice

lockDevice reserves a specified SBC.

public com.acmepacket.ems.ws.service.userobjects.WSDeviceResult lockDevice(java.lang.String targetName)throws com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetName, - the target name

Output Parameters

WSDeviceResult, a data structure described as before

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

unlockDevice

unlockDevice release a previously reserved SBC.

```
public com.acmepacket.ems.ws.service.userobjects.WSDeviceResult
unlockDevice(java.lang.String targetName)throws
com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault,
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

Input Parameters

- targetName, - the target name

Output Parameters

WSDeviceResult, a data structure described as before

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getAllDeviceGroupList

getAllDeviceGroupList returns an array containing the names of all Device Groups.

```
public java.util.ArrayList<java.lang.String> getAllDeviceGroupList()throws
com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault,
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

Output Parameters

ArrayList of devicegroup name

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

addDeviceGroup

addDeviceGroup adds a specified Device Group to the Configuration Database.

public boolean addDeviceGroup(java.lang.String deviceGroupPath)throws
com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault,
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFaultit will try to add the device group

Input Parameters

- deviceGroupPath: - device group path name(for example,group2/groupAC/groupAC1), which means that we are going to add groupAC1 to the device group group2/groupAC

Output Parameters

True or False

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

deleteDeviceGroup

deleteDeviceGroup deletes a specified Device Group from the Configuration Database.

public boolean deleteDeviceGroup(java.lang.String deviceGroupPath)throws
com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault,
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- deviceGroupPath: - device group path name

Output Parameters

True or False

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getLCVContentSaveSessionReport

getLCVContentSaveSessionReport returns a list if WSConfigElements created or modified by a specified user.

public
java.util.ArrayList<com.acmepacket.ems.ws.service.userobjects.WSConfigElement>
getLCVContentSaveSessionReport(java.lang.String targetame,
java.lang.String userName) throws
com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault,
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Specified by

getLCVContentSaveSessionReport java.lang.String in DeviceMgmtIF interface

Input Parameters

- targetName - -targetname
- userName - -user name

Output Parameters

A list of WSConfigElements

Throws

```
com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault
```

getAllManagedDevices

getAllManagedDevices returns a list of SBCDetails for all managed devices.

public ArrayList<SBCDetails> getAllManagedDevices() throws AcmeDeviceWSFault, AcmeAdminWSFault;

Specified by

getAllManagedDevices in DeviceMgmt interface

Input Parameters

None

Output Parameters

ArrayList<SBCDetails>: a List of SBCDetails object

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getAllManagedDeviceTargetNames

getAllManagedDeviceTargetNames returns a list of the names of all managed devices.

public ArrayList<String> getAllManagedDeviceTargetNames() throws AcmeDeviceWSFault, AcmeAdminWSFault;

Specified by

getAllManagedDeviceTargetNames in the DeviceMgmtIF

Input Parameters

- None

Output Parameters

ArrayList< String >: a List of String

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getNNCDetails

getNNCDetails returns an NNCDetails data structure for the NNC server that contains software version, addressing, and cluster information.

public NNCDetails getNNCDetails() throws AcmeDeviceWSFault, AcmeAdminWSFault;

Specified by

getNNCDetails in DeviceMgmtIF interface.

Input Parameters

- None

Output Parameters

NNCDetails object

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getTopLevelElementCount

getTopLevelElementCountreturns a count of all top-level configuration elements. To obtain the element count, it sums the local configuration copy and local configuration change values.

public ArrayList<IntegrityCheckResult> getTopLevelElementCount(String targetName) throws AcmeDeviceWSFault, AcmeAdminWSFault

Specified By

getTopLevelElementCount in interface DeviceMgmtIF

Input Parameters

- targetName- - device name

Output Parameters

An ArrayList of IntegrityCheckResult data structures

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getAllAssociatedDevicesInEMSLicense

> **Note:**
>
> This API is deprecated. Use the getAllAssociatedDevicesInElementManager API instead, which returns an ArrayList<String> with no input parameters and throws AcmeAdminWSFault and AcmeDeviceWSFault exceptions.

addDeviceToEMSLicense

> **Note:**
>
> This API is deprecated. Use the WSConfigResult associateDeviceToElementManager(@WebParam(name = "targetName") String targetName), which throws throws AcmeAdminWSFault, AcmeDeviceWSFault;.

removeDeviceFromEMSLicense

This API is deprecated. Use the WSConfigResult disassociateDeviceFromElementManager(@WebParam(name = "targetName") String targetName) API instead. This API throws AcmeAdminWSFault, AcmeDeviceWSFault;.

4
Configuration Management Level

getPrimaryKeyByElementType

getPrimaryKeyByElementType returns a list of PrimaryKey information for a given element type.

```
public java.util.ArrayList<java.lang.String>
getPrimaryKeyByElementType(java.lang.String targetDevice,
java.lang.String elementType)throws
com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault,
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

Input Parameters

- elementType: element type information
  For a sub-element, the elementType references the full path: for example, to obtain the primary key value for an elementRule, use the expression sipManipulation/headerRule/elementRule.

Output Parameters

An ArrayList of String primary key information, which will include path expression inside the string.

Throws

```
com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

getTopLevelConfigElementTypeNames

getTopLevelConfigElementTypeNames returns a list of top-level configuration element names associated with a specific SBC

```
public java.util.ArrayList<java.lang.String>
getTopLevelConfigElementTypeNames(java.lang.String targetName) throws
com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault,
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

Input Parameters

- targetName: target device information, which is the target name

Output Parameters

An ArrayList of top configuration element names.

Throws

```
com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

getSubElementTypesByElementType

getSubElementTypesByElementTypes returns a list of sub element types for the given elementType.

```
public ArrayList<String> getSubElementTypesByElementType(String
targetName, String elementType) throws AcmeConfigWSFault,
AcmeAdminWSFault
```

Input Parameters

- targetName: target device information, which is the target name
- elementType: element type. For example, sipInterface

Output Parameters

A list of String (sub element types) for the given element type.

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getRequiredSubElementTypesByElementType

getRequiredSubElementTypesByElementType returns a list of required sub element types for the given elementType.

```
public ArrayList<String> getSubElementTypesByElementType(String
targetName, String elementType) throws AcmeConfigWSFault,
AcmeAdminWSFault
```

Input Parameters

- targetName: target device information, which is the target name
- elementType: element type. For example, sipInterface

Output Parameters

Returns a list of required sub element types for the given element type.

Throws

```
com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

getAllSupportedAttributeInfoByElementType

getAllSupportedAttributeInfoByElementType returns a list of WSConfigAttributeMetaData information for the given elementType.

```
public ArrayList<WSConfigAttributeMetaData>
getAllSupportedAttributeInfoByElementType(String targetName, String
elementType) throws AcmeConfigWSFault, AcmeAdminWSFault
```

Input Parameters

- targetName: target device information, which is the target name
- elementType: element type. For example, sipInterface

Output Parameters

Returns a list of WSConfigAttribute information for the given elementType.

Throws

```
com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault
```

deleteConfigElement

deleteConfigElement deletes a specified configuration element; any existing child elements of the element are also deleted.

public com.acmepacket.ems.ws.service.userobjects.WSConfigResult deleteConfigElement(java.lang.String targetDevice, com.acmepacket.ems.ws.service.userobjects.WSConfigElement wsConfigElement)throws AcmeConfigWSFault, AcmeAdminWSFault

Input Parameters

- targetName: target device information, which is the target name
- wsConfigElement: wsConfigElement information

Output Parameters

WSConfigResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

updateConfigElement

updateConfigElement performs an incremental update of a single specified top-level WSConfigElement, or a single, specified sub-element. The user application does not need to provide a complete WSConfigElement; it needs to provide only the primaryKeys required to identify the target configuration element instance, and the attribute/value pairs that require update.

This Oracle Communications Session Delivery Manager SOAP API release does not provide an API to update sub-elements; as a result, updateConfigElement is used to update both top-level and sub-elements. However, users cannot use updatConfigElement to add or delete sub-elements fom an existing configuration element. Use addSubElement to add a sub-element, and deleteSubElement to delete a sub-element.

When updating a sub-element, users must provide an unambiguous path to the single target sub-element that requires update. The path consists of the ACP top-level identifier, followed by one or more sub-element types. At each path level, primaryKeys (such as ACLI object names) must be supplied to ensure unambiguous element identification. For example, the following path

sipManipulation(primaryKeys)/headerRule(primaryKeys)/elementRule(name=”rule1”)

identifies a SIP element rule to be updated.

public com.acmepacket.ems.ws.service.userobjects.WSConfigResult updateConfigElement(java.lang.String targetDevice, com.acmepacket.ems.ws.service.userobjects.WSConfigElement wsConfigElement) throws com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetDevice - - the target name
- wsConfigElement - - contains primarykey attributes to identify the target Configuriation Element, and additional attributes which require update to new values

Output Parameters

WSConfigResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getConfigElement

getConfigElement gets a specified configuration element from the configuration database.

public com.acmepacket.ems.ws.service.userobjects.WSConfigElement getConfigElement(java.lang.String targetDevice, com.acmepacket.ems.ws.service.userobjects.WSConfigElement wsConfigElement) throws com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetDevice - - target name information
- wsConfigElement- - WSConfigElement you need to supply only the primary key attributes on this wsConfigElement.

Output Parameters

WSConfigElement data structure describing the requested configuration element

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getAllConfigElements

getAllConfigElements gets a arrayList of all configuration elements from the configuration database.

public ArrayList<WSConfigElement> getAllConfigElement String targetName,,String elementType) throws com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetDevice - - target device information, which is the target name
- elementType---element type information, such as sipInterface.

Output Parameters

a list of WSConfigElements

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

applyBatch

applyBatch initiates a database batch operation; each individual requested operation is described by a wsBatch data structure.

public com.acmepacket.ems.ws.service.userobjects.WSConfigResult applyBatch(java.lang.String targetDevice, com.acmepacket.ems.ws.service.userobjects.WSBatch wsBatch)throws com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetDevice - - target device information
- wsBatch - - wsBatch data structure

Output Parameters

WSConfigResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

addConfigElement

addConfigElement adds a specified configuration element to the configuration database; sub-elements, if present, are also added to the database.

public com.acmepacket.ems.ws.service.userobjects.WSConfigResult addConfigElement(java.lang.String targetDevice, com.acmepacket.ems.ws.service.userobjects.WSConfigElement wsConfigElement) throws com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetDevice - - target name information
- wsConfigElement - - configuration element to be added to database

Output Parameters

WSConfigResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

replace

replace replaces an existing configuration element in the configuration database; the user must define the replacement configuration element in its entirety, to include sub-elements if any exist.

public com.acmepacket.ems.ws.service.userobjects.WSConfigResult replace(java.lang.String targetDevice, com.acmepacket.ems.ws.service.userobjects.WSConfigElement wsConfigElement) throws com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault, com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

Input Parameters

- targetDevice - - target name information
- wsConfigElement - - configuration element to be replaced

Output Parameters

WSConfigResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

addSubElement

addSubElement adds a new sub-element to a specified top-level configuration element.

When adding a sub-element, users must provide an unambiguous path to the target sub-element to be added. The path consists of the ACP top-level identifier, followed by one or more followed by one or more sub-element types. At each path level, primaryKeys (such as ACLI object names) must be supplied to ensure unambiguous element identification. For example, the following path

sipManipulation(primaryKeys)/headerRule(primaryKeys)/elementRule(name=”rule2”)

identifies a SIP element rule to be added.

public WSConfigResult addSubElement(String targetName, WSConfigElement parent, WSConfigElement child) throws AcmeConfigWSFault, AcmeAdminWSFault

Input Parameters

- targetDevice - - target name information

- parent - - the parent configuration element
- child - - the child sub-element to be added

Output Parameters

WSConfigResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

deleteSubElement

deleteSubElement deletes an existing sub-element from a specified top-level configuration element.

When deleting a sub-element, users must provide an unambiguous path to the target sub-element to be deleted. The path consists of the ACP top-level identifier, followed by one or more followed by one or more sub-element types. At each path level, primaryKeys (such as ACLI object names) must be supplied to ensure unambiguous element identification. For example, the following path

sipManipulation(primaryKeys)/headerRule(primaryKeys)/elementRule(name=”rule2”)

identifies a SIP element rule to be deleted.

public WSConfigResult addSubElement(String targetName, WSConfigElement parent, WSConfigElement child) throws AcmeConfigWSFault, AcmeAdminWSFault;

Input Parameters

- targetDevice - - target name information
- parent - - the parent configuration element
- child - - the child sub-element to be deleted

Output Parameters

WSConfigResult

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getConfigElementMetaData

getConfigElementMetaData returns a configuration element’s metadata to include its attributes.

public WSConfigElementMetaData getConfigElementMetaData(String targetName, String elementType) throws AcmeConfigWSFault, AcmeAdminWSFault

Input Parameters

- targetName - - target device information
- elementType – The type of the element for which the metadata to be returned

Output Parameters

WSConfigElementMetaData

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getConfigAttributeMetaData

getConfigAttributeMetaData returns metadata. for a specified attribute of a specified configuration element.

public WSConfigAttributeMetaData getConfigAttributeMetaData(String targetName, String elementType, String attributeName) throws AcmeConfigWSFault, AcmeAdminWSFault

Input Parameters

- targetName: target device information
- elementType: type of the element for which the metadata to be returned
- attributeName: name of the attribute

Output Parameters

WSConfigElementMetaData

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

getValuesForReferenceAttribute

getValuesForReferenceAttribute returns the values for a specified reference attribute.

public ArrayList<String> getValuesForReferenceAttribute(String targetName, String elementType, String attributeName) throws AcmeAdminWSFault, AcmeConfigWSFault

Input Parameters

- targetName: target device information

- elementType: type of the element for which the metadata to be returned
- attributeName: The name of the attribute

Output Parameters

ArrayList<String>

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

newConfigElement

newConfigElement creates a new default instance of a specified configuration element.

public WSConfigElement newConfigElement(String targetName, String elementType) throws AcmeConfigWSFault, AcmeAdminWSFault

Input Parameters

- targetName - - target name information
- elementType – The type of the element to be returned

Output Parameters

WSConfigElement

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

encryptedPassword

encryptedPassword encrypts a specified user password.

public String encryptedPassword(string configurationPasswordInfo, String inputPassword) throws AcmeConfigWSFault, AcmeAdminWSFault

Input Parameters

- configurationPasswordInfo - - an SBC constant
- inputPassword – the plaintext password to be encrypted

Output Parameters

a string containing the encrypted inputPassword

Throws

com.acmepacket.ems.ws.service.fault.AcmeConfigWSFault
com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

deleteUserChanges

The deleteUserChanges API is used to delete any changes that a logged-in user made to a managed device.

Input Parameters

- targetName—The target name of the device on which the logged-in user made changes.

Output Parameters

- WSDeviceResult—The name of the result of deleting changes that a logged-in user made to a managed device.

Throws

com.acmepacket.ems.ws.service.fault.AcmeDeviceWSFault

com.acmepacket.ems.ws.service.fault.AcmeAdminWSFault

A

Meta Data Tables

The tables listed in this section list the SOAP attributes and the sub-elements for the following tables:

- ikeSanInfo
- spdConfig
- networkInterfaceId
- spdFineGrained
- sipInterface
- sipPort
- addSdpProfilesInMsg
- mediaProfile

Table Name - ikeSanInfo

This table lists the the field lengths for the fields in the table ikeSanInfo.

For the fields listed under the Valid Values column, you can consider the longest value listed, but it is recommended that you know the max length. For the fields listed with no valid values, you will need to know the max length.

Table A-1 ikeSanInfo

SOAP Attributes/ Subelements	ACLI media-manager- >realm-config	Default Values	Valid Values	Attribute length
mode	ipsec-mode	tunnel	transport, tunnel	max-length = 9
tunnelSrcIP	tunnel-local-addr			max-length = 15
lastModifiedDate	last-modified-date			max-length = 19
proto	security-protocol	esp-auth	esp, ah, esp-auth, esp-null	max-length = 8
lastModifiedBy	last-modified-by			max-length = 52
id	name			1-128
tunnelDstIP	tunnel-remote-addr	*		max-length = 15
authAlgo	auth-algo	sha2-512	sha1, sha2-384, xcbc, sha2-512, sha2-256, any, md5	max-length = 8
encryAlgo	encryption-algo	aes	aes-ctr, null, 3des, any, aes	max-length = 7

> **Note:**
>
> The information provided in this table is valid for SBC 8.4.0

Security-policy - Table Name - spdConfig

This table lists the the field lengths for the fields in the table spdConfig.

For the fields listed under the Valid Values column, you can consider the longest value listed, but it is recommended that you know the max length. For the fields listed with no valid values, you will need to know the max length.

Table A-2 spdConfig

SOAP Attributes/ Sub-elements	ACLI media-manager->realm-config	Default Values	Valid Values	Attribute length
ikeSaInfoName	ike-sainfo-name			1-128
srcPort	local-port-match	0	0 - 65535	-
dstPortMax	remote-port-match-max	65535	0 - 65535	-
protocol	trans-protocol-match	ALL	TCP, UDP, ALL, IPV6-ICMP, SCTP, ICMP	max-length = 9
dstPort	remote-port-match	0	0 - 65535	-
options	options			No length restriction
action	action	ipsec	allow, discard, ipsec, srtcp, srtp	max-length = 7
direction	direction	both	in, out, both	max-length = 4
lastModifiedDate	last-modified-date			max-length = 19
lastModifiedBy	last-modified-by			max-length = 52
dstIPMask	remote-ip-mask	255.255.255.255		max-length = 15
priority	priority	0	0 - 3071	-
dstIPAddr	remote-ip-addr-match			max-length = 15
name	name			1-128
srcIPAddr	local-ip-addr-match			max-length = 15
srcPortMax	local-port-match-max	65535	0 - 65535	-
srcIPMask	local-ip-mask	255.255.255.255		max-length = 15

> **Note:**
>
> The information provided in this table is valid for SBC 8.4.0

Security-policy - Table Name - networkInterfaceId

This table lists the the field lengths for the fields in the table spdConfig/networkInterfaceId which is a sub-element of security-policy.

For the fields listed under the Valid Values column, you can consider the longest value listed, but it is recommended that you know the max length. For the fields listed with no valid values, you will need to know the max length.

Table A-3 spdConfig/networkInterfaceId

SOAP Attributes/ Subelements	ACLI media-manager- >realm-config	Default Values	Valid Values	Attribute length
subPortId	subPortId	0	0	-
name	name			1-128
family	family		4,5,6	-

> **Note:**
>
> The information provided in this table is valid for SBC 8.4.0

Security-policy - Table Name - spdFineGrained

This table lists the the field lengths for the fields in the table spdFineGrained.

For the fields listed under the Valid Values column, you can consider the longest value listed, but it is recommended that you know the max length. For the fields listed with no valid values, you will need to know the max length.

Table A-4 spdFineGrained

SOAP Attributes/ Subelements	ACLI media-manager- >realm-config	Default Values	Valid Values	Attribute Length
valid	valid	enabled	enabled, disabled	max-length = 8
srcIP	local-ip-mask	255.255.255.255		max-length = 15
protocol	trans-protocol-mask	0	0 - 65535	-
dstPort	remote-port-mask	0	0 - 65535	-
vlanID	vlan-mask	0xFFF		max-length = 5
dstIP	remote-ip-mask			max-length = 15
srcPort	local-port-mask	0	0 - 65535	-

Table A-4 (Cont.) spdFineGrained

SOAP Attributes/ Subelements	ACLI media-manager- >realm-config	Default Values	Valid Values	Attribute Length
saLookupException	sa-lookup-exception	enabled	enabled, disabled	max-length = 8

> **Note:**
>
> The information provided in this table is valid for SBC 8.4.0

SIP Interface - Table Name - sipInterface

This table lists the the field lengths for the fields in the table sipInterface.

For the fields listed under the Valid Values column, you can consider the longest value listed, but it is recommended that you know the max length. For the fields listed with no valid values, you will need to know the max length.

Table A-5 sipInterface

SOAP Attributes/ Subelements	ACLI media-manager- >realm-config	Default Values	Valid Values	Attribute Length
add-sdp-invite	add-sdp-invite	disabled	reinvite, disabled, invite, both	max-length = 8
RealmID	realm-id			1-128
add-sdp-in-msg	add-sdp-in-msg			max-length = 6
anonymousPriority	anonymous-priority	none	Normal, non-urgent, emergency, none, urgent	max-length = 10
initialInvTransExpire	initial-inv-trans-expire	0	0 - 999999999	-
sipRecursionPolicy	sip-recursion-policy			1-128
fqdnDomain	uri-fqdn-domain			No string restriction
sipdynamicHnt	sip-dynamic-hnt		enabled, disabled	max-length = 8
atcfIcsiMatch	atcf-icsi-match			No string restriction
s8hrProfileName	s8hr-profile			1-128
userAgentName	user-agent			No length restriction
smIcsiMatchForInvite	sm-icsi-match-for-invite			No length restriction
hmrString	manipulation-string			No length restriction

Table A-5 (Cont.) sipInterface

SOAP Attributes/ Subelements	ACLI media-manager->realm-config	Default Values	Valid Values	Attribute Length
options	options			No length restriction
operatorIdentifier	operator-identifier			min length = 1
sec-agree-pref	sec-agree-pref	ipsec3gpp	tls-ipsec3gpp, ipsec3gpp-tls, ipsec3gpp, tls	max-length = 13
state	state	enabled	enabled, disabled	max-length = 8
natmaxInterval	max-nat-interval	3600	0 - 4294967295	-
imsAkaFeature	sec-agree-feature	disabled	enabled, disabled	max-length = 8
tcpNatInterval	tcp-nat-interval	90	0 - 4294967295	-
stopRecurse	stop-recurse	401,407		max-length = 3
carriers	carriers			1-24
registrationCaching	registration-caching	disabled	enabled, disabled	max-length = 8
termTgrpMode	term-tgrp-mode	none	egress-uri, iptel, none	max-length = 10
pearlyMediaHeader	p-early-media-header	disabled	add, modify, disabled, support	max-length = 8
divInfoMappingMode	diversion-info-mapping-mode	none	hist2div, div2hist, force, none	max-length = 8
asymmetricPreconditionsMode	asymmetric-preconditions-mode	send-with-nodelay	send-with-nodelay, send-with-delay	max-length = 17
sipProfile	sip-profile			1-127
smIcsiMatchForMessage	sm-icsi-match-for-message			min-length = 11
inManipulationId	in-manipulationid		ACME_NAT_TO_FROM_IP	max-length =19
extPolicyServer	ext-policy-server			1-128
localresponseMap	local-response-map			1-128
splOptions	spl-options			No length restriction
responseMap	response-map			1-128
defaultLocationString	default-location-string			1-128
outManipulationId	out-manipulationid			max-length = 19
histToDivForCause380	hist-to-div-for-cause-380	inherit	inherit, disabled, enabled	max-length = 8
regInterval	registration-interval	3600	0 - 4294967295	-
natTestIncrement	nat-test-increment	30	0 - 4294967295	-

Table A-5 (Cont.) sipInterface

SOAP Attributes/ Subelements	ACLI media-manager->realm-config	Default Values	Valid Values	Attribute Length
trustMode	trust-mode	all	all, realm-prefix, agents-only, registered, none	max-length = 12
pearlyMediaDirection	p-early-media-direction			max-length = 8
imsFeature	sip-ims-feature	disabled	enabled, disabled	max-length = 8
redirectAct	redirect-action		Proxy, Recurse, Recurse-305-only	max-length = 16
RealmID	realm-id			1-128
isSecure	secured-network	disabled	enabled, disabled	max-length = 8
ccfAddress	ccf-address			No string restriction
constraintName	constraint-name			1-128
portMapStart	port-map-start	0	0- 0, 1025-65535	-
invite-expire	invite-expire	0	0 - 999999999	-
chargingVectorMode	charging-vector-mode	pass	pass, conditional-insert, insert, none, delete-and-respond, delete	max-length = 18
rfc2833-payload	rfc2833-payload	101	96 - 127	-
tcp-keepalive	tcp-keepalive	none	disabled, none, enabled	max-length = 8
send380Response	send-380-response			No string restriction
sessionRecordingServerTarget	session-recording-server			1-128
regMinExpire	min-reg-expire	300	0 - 999999999	-
portMapEnd	port-map-end	0	0 – 0, 1025 - 65535	-
sessionTimerProfile	session-timer-profile			1-128
serviceTag	service-tag			No string restriction
kpml2833IwfOnHairpin	kpml2833-iwf-on-hairpin	disabled	enabled, disabled	max-length = 8
chargingFuncAddrMode	charging-function-address-mode	pass	insert-reg-cache, pass, conditional-insert, insert, none, delete-and-respond, delete	max-length = 18
maxConnPerPeer	per-src-ip-max-incoming-conns	0	0 - 20000	-
enforcementProfile	enforcement-profile			1-128
proxyMode	proxy-mode		Stateless, Proxy, Record-Route, Redirect	max-length = 12

Table A-5 (Cont.) sipInterface

SOAP Attributes/ Subelements	ACLI media-manager->realm-config	Default Values	Valid Values	Attribute Length
sipRegisterKeepAlive	register-keep-alive	none	always, bnat, none	max-length = 6
ecfAddress	ecf-address			No string restriction
kpmlInterworking	kpml-interworking	disabled	disabled, enabled	max-length = 8
routeUnauthorizedCalls	route-unauthorized-calls			1-128
sipIsupProfile	sip-isup-profile			1-128
atcfFeature	sip-atcf-feature	disabled	disabled, enabled	max-length = 8
natIntervalIncrement	nat-int-increment	10	0 - 4294967295	-
sessionRecordingRequired	session-recording-required	disabled	disabled, enabled	max-length = 8
trans-expire	trans-expire	0	0 - 999999999	-
tunnelName	tunnel-name			1-128
msrpDelayEgressBye	msrp-delay-egress-bye	disabled	disabled, enabled	max-length = 8
natTraversal	nat-traversal	none	always, rport, none	max-length = 6
rfc2833-mode	rfc2833-mode	transparent	dual, transparent, preferred	max-length = 11
description	description			No string restriction
max-redirect-contacts	max-redirect-contacts	0	0 - 10	-
contactSip	contact-mode	none	maddr, strict-route, loose-route, none	max-length = 12
NetworkID	network-id			No string restriction
manipPattern	manipulation-pattern			No string restriction
subscribeRegEvent	subscribe-reg-event	disabled	disabled, enabled	max-length = 8
anonymousPriority	anonymous-priority	none	normal, non-urgent, emergency, none, urgent	max-length = 10
sessionMaxLifeLimit	session-max-life-limit	0	0 - 2073600	-
regCacheRoute	reg-cache-route	disabled	disabled, enabled	max-length = 8
isRouteReg	route-to-registrar	disabled	disabled, enabled	max-length = 8
telUri	teluri-scheme	disabled	disabled, enabled	max-length = 8
idleConnTimeout	inactive-conn-timeout	0	0 - 999999999	-

Table A-5 (Cont.) sipInterface

SOAP Attributes/ Subelements	ACLI media-manager->realm-config	Default Values	Valid Values	Attribute Length
npliProfileName	npli-profile			1-128
lastModifiedDate	last-modified-date			max-length = 19
lastModifiedBy	last-modified-by			max-length = 52
tcpConnDereg	tcp-conn-dereg	0	0 - 999999999	-
asymmetricPreconditions	asymmetric-preconditions	disabled	disabled, enabled	max-length = 8
implicitServiceRoute	implicit-service-route	disabled	replace, absent, disabled, strict, enabled	max-length = 8
pcscfRestoration	pcscf-restoration			No string restriction
natInterval	nat-interval	30	0 - 4294967295	-
add-sdp-invite	add-sdp-invite	disabled	reinvite, disabled, invite, both	max-length = 8
untrustedConnTimeout	untrusted-conn-timeout	**0**	0 - 999999999	-
maxConn	max-incoming-conns	**0**	0 - 20000	-
ldapPolicyServer	ldap-policy-server			1-128
rbtTrigger	ringback-trigger	**none**	refer, 180-force, 183-no-sdp, rbt-playback-on-header, 180-no-sdp, disabled, none, 183, 183-and-refer	max-length = 22
ringbackFile	ringback-file			No length restriction

Note:

The information provided in this table is valid for SBC 8.4.0

SIP Interface - Table Name - sipPort

This table lists the the field lengths for the fields in the table sipPort.

For the fields listed under the Valid Values column, you can consider the longest value listed, but it is recommended that you know the max length. For the fields listed with no valid values, you will need to know the max length.

Table A-6 sipPort

SOAP Attributes/ Subelements	ACLI media-manager- >realm-config	Default Values	Valid Values	Attribute Length
address	address			max-length = 15
transProtocol	transport-protocol	UDP	UDP, TCP, TLS, SCTP	max-length = 4
anonMode	allow-anonymous	all	all, realm-prefix, agents-only, registered, register-prefix	max-length = 15
port	port	5060	1 - 65535	-
imsAkaProfile	ims-aka-profile			No length restriction
sctpMultiHomeAddrs	multi-home-addrs			max-length = 15
tlsProfile	tls-profile			No length restriction

Note:

The information provided in this table is valid for SBC 8.4.0

SIP Interface - Table Name - addSdpProfilesInMsg

This table lists the the field lengths for the fields in the table sipInterface/ addSdpProfilesInMsg. This table is a sub-element of sip-interface.

For the fields listed under the Valid Values column, you can consider the longest value listed, but it is recommended that you know the max length. For the fields listed with no valid values, you will need to know the max length.

Table A-7 Table sipInterface/addSdpProfilesInMsg

SOAP Attributes/ Subelements	ACLI media-manager- >realm-config	Default Values	Valid Values	Attribute Length
name	name			1-128

Note:

The information provided in this table is valid for SBC 8.4.0

SIP Interface - Table Name - mediaProfile

This table lists the the field lengths for the fields in the table sipInterface/mediaProfile. This table is a sub-element of sip-interface called add-spd-profiles.

For the fields listed under the Valid Values column, you can consider the longest value listed, but it is recommended that you know the max length. For the fields listed with no valid values, you will need to know the max length.

Table A-8 sipInterface/mediaProfile

SOAP Attributes/ Subelements	ACLI media-manager->realm-config	Default Values	Valid Values	Attribute Length
name	name		PCMU, PCMA, G722, G723, G726-16, G726-24, G726-32, G726, G726-40, G728, G729, G729A, GSM, iLBC, G711FB, H261, H263, T.38, telephone-event, AMR, EVRC0, DVI4, LPC, L16, QCELP, CN, MPA, CelB, nv, MPV, MP2T, opus, SILK	max-length = 15

Note:

The information provided in this table is valid for SBC 8.4.0

B

ACLI to ACP Mappings

Retrieve Element Metadata and Attributes

You can use the SOAP API to get element metadata and attribute information.

1. Add the device in Device Manager and load the device in Configuration Manager.
2. Use the ACP element type: **ConfigMgmtif.getConfigElementMetaData** with the string *targetName* and *elementType* to return all available metadata and attributes for the element type you choose.

> **Note:**
>
> The **generate-certificate-request** and **import-certificate** commands are not supported by the SOAP API.

Retrieving the ACLI to ACP Mapping

The ACLI to ACP mapping varies between models. To dynamically generate the ACLI to ACP mapping for your SBC version, use the getACLItoACPMapping API call.

The SBCs must already be added in Device Manager and loaded in Configuration Manager. If an SBC is not added in Device Manager, or added in Device Manager but not loaded in Configuration Manager, this procedure returns the error message:

```
The target device names added to OC SDM are: [null]
```

1. Unzip the CXFClientNNCMain.zip included as part of the Oracle Session Delivery Manager download.
2. In the CXFClientNNCMain\bin\build.bat file, set the following variable:
   - *JAVA_HOME*—The path to your local JDK installation
3. In the CXFClientNNCMain\bin\run.bat file, set the following variables:
   - *JAVA_HOME*—The path to your local JDK installation
   - *SERVER_NAME*—The host name of your Oracle Session Delivery Manager server.
4. Also in the CXFClientNNCMain\bin\run.bat file, change `sampleSource.GenericClient` to `sampleSource.ClientExample`.
   - If using https, change the `sampleSource.GenericClient` in line 15.

> **Note:**
>
> If using https, set values for the TRUST_STORE and TRUST_STORE_PASSWORD variables.

- If using http, change the `sampleSource.GenericClient` in line 20.

```
:http
"%JAVA_HOME%\bin\java"  -classpath .;%CLASSPATH%  -
DServerName=%SERVER_NAME% -DServerPort=%SERVER_PORT%
sampleSource.ClientExample
```

5. In the CXFClientNNCMain\sampleSource\ClientExample.java file, under the Class Variables section, set the following private static variables:
   - *serverName*—The host name or IP address of your Oracle Session Delivery Manager server.
   - *serverPort*—The port of your Oracle Session Delivery Manager server
   - *soapUser*—The administrator's user name.
   - *soapUserPwd*—The administrator's password.
   - *targetDevice.*—The target name of the SBC.

   > **Note:**
   >
   > To find the target name from within the Oracle Session Delivery Manager GUI, click **Configuration Manager**, and then **Devices**, and then **Expand All**. The Target Name column contains the value for the *targetDevice* variable.

   For example:

   ```
   private static String serverName="1.2.3.4";
   private static String serverPort="8080";
   private static String soapUser="admin_user";
   private static String soapUserPwd="admin_password";
   private static String targetDevice = "sbc720";
   ```

6. In the runScenarios() function, uncomment the getACLItoACPMapping API call.

   > **Note:**
   >
   > Because the getACLItoACPMapping call needs to know the devices managed by the Oracle Session Delivery Manager, the runScenario2 call must also be uncommented.

```
private void runScenarios() {
    try {
        //runScenario1();            // Summary view SOAP user
```

```
runScenario2();              // Get managed devices
//runScenario3();            // Get top level element names
//runScenario4();            // Create Top level element
getACLItoACPMapping();       // Return a list of ACLI to ACP name
                                mapping for Top-level Elements
```

7. From the Command Prompt, re-build and run the SOAP client.

```
C:\CXFClientNNCMain\bin>build.bat
Note: ..\sampleSource\ClientExample.java uses unchecked or unsafe
operations.
Note: Recompile with -Xlint:unchecked for details.

C:\CXFClientNNCMain\bin>run.bat
```

The ACLI to ACP mapping is displayed.

```
The target device names added to NNC are : [sbc720]
[
 Name : media-manager->codec-policy Value : codecPolicy,
 Name : media-manager->dns-config Value : dnsConfig,
 Name : media-manager->dnsalg-constraints Value : dnsAlgConstraints,
 Name : media-manager->ext-policy-server Value : extBwManager,
 . . .
```

Physical Interface

The following table lists SOAP attributes and sub-elements for the physical interface.

SOAP Attributes/ Sub-elements	ACLI system->phy-interface	Default Values	Valid Values	SBC Version
acliObjectName *# admin	name admin-state	enabled 50	24 characters enabled/disabled	4.0.0 and above
operationType #	operation-type		maintenance or media	
port #	port		0-3	
slot #	slot		0-1	
ae_en	auto-negotiation		enabled/disabled	
duplex	duplex-mode		full or half	
speed	speed		100 or 10	
virtualMac	virtual-mac		empty or hh:hh:hh:hh:hh:hh	
wancomHealthScore	wancom-health-score		0-100	
overloadProtection AlarmThreshold	overload-protection alarm-threshold	disabled minor	enabled, disabled minor, major, critical	6.2.0 and above
severity*#	severity	0	0-100	
value	value			

Network Interface

The following table lists SOAP attributes and sub-elements for the network interface.

SOAP Attributes/Sub-elements	ACLI system->network-interface	Default Values	Valid Values	SBC Version
acliObjectName * subPortId *#	name sub-port-id	<phy> disabled	<phy> 0-4095	4.0.0 and above
hostname	hostname	0	0-255 chars	
ipAddress	ip-address	0	Ipv4	
utilityAddress	pri-utility-addr	1	Ipv4	
secondUtilityAddress	sec-utility-addr	0	Ipv4	
netmask	netmask		Ipv4	
gateway	gateway		Ipv4	
gatewaySec	sec-gateway		Ipv4	
NetworkInterfaceGWHeartbeat	gw-heartbeat		enabled/disabled	
state #	state		0-65535	
timeout	heartbeat		0-65535	
retrycount	retry-count		1-65535	
retryTimeout	retry-timeout		0-100	
healthDec	health-score		Ipv4	
domNameServer	dns-ip-primary		Ipv4	
domNameServerB1	dns-ip-backup1		Ipv4	
domNameServerB2	dns-ip-backup2		list of IPs	
defDomainName	dns-domain		ipv4	
HipIpList	hip-ip-list		empty or combo of (ftp, icmp, snmp, telnet)	
ip *#	ftp-address		ftp HIP	
protocolParameters	icmp-address		icmp HIP	
ftpAddress	snmp-address		snmp HIP	
icmpAddress	telnet-address		telnet HIP	
snmpAddress				
telnetAddress				
dnsTimeout	dns-timeout	11	0-4294967295	
description	description		255 chars	5.0.0 and above
IcmpipList ip *#	icmp-address		HIP	4.1.4; 5.1.0 and above

SOAP Attributes/Sub-elements	ACLI system->network-interface	Default Values	Valid Values	SBC Version
hostname ipAddress utilityAddress secondUtilityAddress netmask gateway gatewaySec domNameServer domNameServerB1 domNameServerB2 HipIpList ip *# protocolParameters IcmpIpList ip *#	hostname ip-address pri-utility-addr sec-utility-addr netmask gateway sec-gateway dns-ip-primary dns-ip-backup1 dns-ip-backup2 hip-ip-list icmp-address		0-255 chars, ipv4, ipv6 Ipv4, ipv6, ipv6/prefix Ipv4, ipv6 Ipv4, ipv6 Ipv4, not allowed for ipv6 Ipv4, ipv6 Ipv4, ipv6 Ipv4, ipv6 Ipv4, ipv6 Ipv4, ipv6 list of IPs ipv4, ipv6 empty or combo of (ftp, icmp, snmp, telnet) list of ipv4, ipv6	CX6.2.0 and above

Realm

The following table lists SOAP attributes and sub-elements for the realm.

SOAP Attributes/Sub-elements	ACLI media-manager->realm-config	Default Values	Valid Values	SBC Version
id *# addrPrefix	identifier addr-prefix	0.0.0.0 0	24 characters 0.0.0.0 or ipv4 or ipv4/mask	4.0.0 and above
parent	parent-realm	disabled	empty or <realm>	
acliObjectName *#	max-bandwidth	enabled	0-999999999	
subPortId *#	mm-in-realm	disabled	enabled/disabled	
maxBandwidth	mm-in-network	disabled	enabled/disabled	
mrInRealm	msm-release	none	enabled/disabled	
mrInNetwork	qos-enable	0	enabled/disabled	
isMSMRelease	media-policy	0	empty or <QoS marking profile>	
qosEnable	in-translationid	0	empty or <trans-profile>	
mediaPolicy	outtranslationId	30	empty or <realm>	
intranslationid	dns-realm		empty or <cls-profile>	
outtranslationid	class-profile		none, low, medium, high	
dnsRealm	access-control-trust-level		0-999999999	
classProfile	average-rate-limit		0-999999999	
trustLevel	invalid-signal-threshold		0-999999999	
rateLimit	maximum-signal-threshold		0-999999999	
errMsgThreshold	deny-period			
maxMsgThreshold				
denyTimer				
RealmNetworkInterfaceId	network-interfaces		<phy:port-id> <ip_version> or lo0:0:4	Before 6.4.0
RealmNetworkInterfaceId	network-interfaces		<phy:port-id>, <ip_version>, lo0:0:4, or lo0:0:6	6.4.0 or later
symmetricLatching	symmetric-latching	disabled	enabled/disabled	
paiStrip	pai-strip	disabled	enabled/disabled	
trunkContext bwManager	trunk-context ext-policy-svr	0	empty or <pol-server>	
inManipulationId	in-manipulationid		empty or <sip-manipulation>	
outManipilationId	out-manipulationid			
options	options		list of options separated by comma	
maxMsgThresholdUntrusted	untrusted-signal-threshold		0-999999999	
mmInSystem restrictedLatching	mm-in-system restricted-latching	enabled none	enabled/disabled none, sdp, peer-ip	4.0.1 and above
restrictionMask	restriction-mask	32	1-32	

SOAP Attributes/Sub-elements	ACLI media-manager->realm-config	Default Values	Valid Values	SBC Version
mmSameIp earlyMediaAllow RealmAdditionalPrefixes prefix *#	mm-same-ip early-media-allow additional-prefixes	enabled	enabled/disabled empty, none, reverse, or both list of ipv4/mask ipv4/mask	
acctEnable	accounting-enable	enabled	enabled, disabled	4.1.0 and above
netMgmtCtrl userCacMode userCacBandwidth userCacSessions delayedMediaUpdate nonMmBwCAC codecPolicy codePolicyInRealm	net-management-control user-cac-mode user-cac-bandwidth user-cac-sessions delay-media-update bw-cac-non-mm codec-policy codec-manio-in-realm	disabled none 0 0 disabled disabled disabled	enabled or disabled none, aor, ip 0-999999999 0-999999999 enabled/disabled enabled/disabled empty or <codec-policy> enabled/disabled	4.1.1 and above
generateUDPChecksum enforcementProfile	generate-udp-checksum enforcement-profile	disabled	emoty or disabled empty or <enforcement-profile>	4.1.4; 5.1.0 and above
monthlyMinutes constraintName	monthly-minutes constraint-name	0	0-71582788 empty or <session-constraint>	4.1.4 and 5.1.1
referCallTransfer description	refer-call-transfer description	disabled	enabled, disabled	5.1.1 and above
callRecordingServerId	call-recording-server-id		empty, defined call recording server	6.0.0 and above

SOAP Attributes/Sub-elements	ACLI media-manager->realm-config	Default Values	Valid Values	SBC Version
hmrString maxPriorityBandwidth fallbackBandwidth icmpDetectMultip icmpAdvInterval icmpTargetIp MatchMediaProfile acliObjectName *# natTrustThreshold stunEnable stunServerIp stunServerPort stunChangedIp stunChangedPort qosConstraintName	manipulation-string max-priority-bandwidth fallback-bandwidth icmp-detect-multiplier icmp-advertisement-interval icmp-target-ip match-media-profiles nat-trust-threshold stun-enable stun-server-ip stun-server-port stun-changed-ip stun-changed-port qos-constraint	0 0 0 0 0 disabled 0.0.0.0 3478 0.0.0.0 3479	0-999999999 0-999999999 0-999999999 0-999999999 ipv4 list of <media-profile>, <media-profile>::, <media-profile>::<subname>, *, *::, *::<subname> 0-65535 enabled, disabled ipv4 1025-65535 ipv4 1025-65535 empty or <qos constraint>	6.1.0 and above
sipProfile sipIsupProfile referCallTransfer dynReferTerm cacFailThreshold untrustedCacFailThreshold manipPattern	sip-profile sip-isup-profile refer-call-transfer dyn-refer-term cac-failure-threshold untrust-cac-failure-threshold manipulation-pattern	disabled disabled 0 0	empty or <sip-profile> empty or <sip-isup-profile> disabled, enabled, dynamic enabled, disabled 0-999999999 0-999999999	6.2.0 and above
mediaSecPolicy addrPrefix xnqState hairpinId	media-sec-policy addr-prefix xnq-state hairpin-id	xnq-unknown	empty or <media-sec-policy> ipv4 or ipv4/mask, ipv6, ipv6/mask xnq-unknown, xnq-potential, xnq-remove 0-65535	CX6.2.0 and above

Realm Media Address

The following table lists SOAP attributes and sub-elements for the realm media address.ip-

SOAP Attributes/ Sub-elements	ACLI media-manager- >steering-pool	Default Values	Valid Values	SBC Version
ipAddress *# startPort *# endPort # realmID RealmNetworkInterfaceId acliObjectName subPortId	ip-address start-port end-port realm-id network-interface	<realm>	Ipv4 1025-65535 1025-65535, endPort > startPort <realm> empty or <phy:port-id>	4.0.0 and above
ipAddress *#	ip-address		ipv4, ipv6	CX6.2.0and above

Surrogate Agent

The following table lists SOAP attributes and sub-elements for the surrogate agent.

SOAP Attributes/ Sub-elements	ACLI session-router- >surrogate-agent	Default Values	Valid Values	SBC Version
registerHost *# registerUser *# state realmID * description customerHost customerRoute # contactHost # contactUser # password expires replaceContact routeToRegistrar count authUser options	register-host register-user state realm-id description customer-host customer-next-hop register-contact-host register-contact-user password register-expires replace-contact route-to-registrar aor-count auth-user options	enabled <realm> 600000 disabled enabled 1	Ipve or hostname enabled/disabled <realm> Ipv4 or hostname SAG:<sag> or <sa> or ipv4 or hostname Ipv4 or hostname 0-999999999 enabled/disabled enabled/disabled 0-999999999 list of comma separated options	4.0.1 and above
maxRegisterAttempts registerRetryTime countStart	max-register-attempts register-retry-time count-start	3 300 1	0-10 30-3600 0-999999999	4.1.4; 5.1.0 and above

SIP Interface

The following table lists SOAP attributes and sub-elements for the SIP interface.

SOAP Attributes/Sub-elements	ACLI session-router->sip-interface	Default Values	Valid Values	SBC Version
state	state	enabled	enabled/disabled	4.0.0 and above
RealmID *	realm-id	<realm>	<realm>	
trustMode	trust-mode	all	all, agents-only, relam-prefix, registered	
SIPConfiguration SIPPort	sip-port	5060		
address *#	address	UDP	ipv4	
port *#	port	all	1025-65535	
transProtocol *#	transport-protocol	none	UDP or TCP	
anonMode	allow-anonymous	disabled	all, agents-only, realm-prefix, registered, register-prefix	
proxyMode	proxy-mode	none		
redirectAct	redirect-action	30		
contactSip	contact-mode	300		
telUri	teluri-scheme	3600	empty, proxy, redirect, record-route, stateless	
fqdnDomain	uri-fqdn-domain	disabled		
natTraversal	nat-traversal	disabled	empty, proxy, recurse	
natInterval	nat-interval			
regMinExpire	min-reg-expire		none, maddr, strict, loose	
regInterval	registration-interval		enabled, disabled	
registrationCaching	registration-caching		none, always, rport	
isRouteReg	route-to-registrar		0-999999999	
SIPConfiguration Carriers	carriers		1-999999999	
acliObjectName *#	options		0-999999999	
options			enabled/disabled	
			enabled/disabled	
			list of carriers	
			list of options seperated by comma	
natmaxInterval	max-nat-interval	3600	enabled, disabled	
natIntervalIncrement	nat-int-increment	10		
natTestIncrement	nat-test-increment	30		
sipdynamicHnt	sip-dynamic-hnt	disabled		
stopRecurse	stop-recurse	401,407	list of response codes, 300-599 seperated by comma	
portMapStart	port-map-start	0	0, 1025-65535	
portMapEnd	port-map-end	0	0, 1025-65535, end>start	

SOAP Attributes/Sub-elements	ACLI session-router->sip-interface	Default Values	Valid Values	SBC Version
trustMode extPolicyServer	trust-mode ext-policy-server	disabled None	all, agents-only, relam-prefix, registered, none empty or <pol-server>	
defaultLocationString	default-location-string	None		
imsFeature	sip-ims-feature	pass	enable/disabled	
NetworkID	network-id	pass		
anonymousPriority	anonymous-priority		NONE (4.0.1), none (4.2), normal, non-urgent, urgent, emergency	
termTgrpMode	term-tgrp-mode			
chargingVectorMode	charging-vector-mode		none, iptel, egress-uri	
chargingFuncAddrMode	charging-function-address-mode		none, pass, delete, insert	
ecfAddress	ecf-address		none, pass, delete, insert	
ccfAddress	ccf-address			
operatorIdentifier	operator-identifier		Ipv4 or hostname	
inManipulationId	in-manipulationid		Ipv4 or hostname	
outManipulationId	out-manipulationid		empty or <sip-manipulation>	
implicitServiceRoute	implicit-service-route	disabled	strict, enabled, disabled	4.0.1 and above
tcpNatInterval isSecure	tcp-nat-interval secured-network	90 disabled	0-99999999 enabled, disabled	4.1.0 and above
rfc2833-mode	rfc2833-mode	transparent	transparent, preferred	
rfc2833-payload	rfc2833-payload	101	96-127	
maxConnPerPeer	per-src-ip-max-incoming-conns	0	0-20000	
maxConn		0	0-20000	
idleConnTimeout	max-incoming-conns	0	0-999999999	
SIPConfiguration SIPPort	inactive-conn-timeout		UDP, TCP, TLS	
transProtocol	sip-port		<tls-profile> if TLS specified	
tlsProfile	transport-protocol			
	tls-profile			
constraintName implicitServiceRoute	constraint-name implicit-service-route	disabled	empty or <session-constraint> strtict, enabled, disabled	4.0.1; 4.1.1 and above
responseMap localresponseMap	response-map local-response-map		empty or <sip-response-map>	4.1.1 and above

SOAP Attributes/Sub-elements	ACLI session-router->sip-interface	Default Values	Valid Values	SBC Version
trans-expire invite-expire	trans-expire invite-expire		0-999999999 0-999999999	
max-redirect-contacts	max-redirect-contacts		0-10	
rfc2833-mode	rfc2833-mode		transparent, preferred, dual	
untrustedConnTimeout	untrusted-conn-timeout	0	0-999999999	5.0.0 and above
tcp-keepalive chargingFuncAddrMode enforcementProfile	tcp-keepalive charging-function-address-mode enforcementProfile	none pass	none, disabled, enabled none, pass, delete, insert, delete-and-respond, insert-reg-cache empty or <enforcement profile>	4.1.4; 5.1.0 and above
add-sdp-invite SIPInterfaceMediaProfile	add-sdp-invite add-sdp-profile	disabled	disabled, invite, reinvite list of media profiles	4.1.4; 5.1.1 and above
referCallTransfer routeUnauthorizedCalls description	refer-call-transfer route-unauthorized-calls description	disabled	enabled, disabled empty, defined SA or SAG	5.1.1 and above
implicitServiceRoute	implicit-service-route	disabled	strict, enabled, disabled, absent, replace	6.0.0 and above
chargingVectorMode	charging-vector-mode	pass	none, pass, delete, insert, delete-and-respond	6.0.0M1 and above
imsAkaFeature imsAkaProfile hmrString SIPConfiguration SIPPort transProtocol	ims-aka-feature ims-aka-profile manipulation-string sip-port transport-protocol	disabled UDP	enabled, disabled <ims-aka-profile> or empty UDP, TCP, TLS, SCTP	6.1.0 and above
sipProfile sipIsupProfile manipPattern	sip-profile sip-isup-profile manipulation-pattern		empty or <sip-profile> empty or <sip-isup-profile>	6.2.0 and above
SIPConfiguration SIPPort address *#	sip-port address		ipv4, ipv6	CX6.2.0 and above

SIP NAT

The following table lists SOAP attributes and sub-elements for the SIP NAT.

SOAP Attributes/ Sub-elements	ACLI Session-router->sip-nat	Default Values	Valid Values	SBC Version
RealmID * ProxyAddress	realm-id ext-proxy-address	<realm> 5060	<realm> <0.0.0.0> or ipv4	4.0.0 and above
ProxyPort	ext-proxy-port	0	1025-65535	
ExternalAddress	ext-address	disabled	Ipv4	
HomeAddress	home-address	disabled	Ipv4	
HomeProxyAddress	home-proxy-address	-acme-	Ipv4	
		ACME-	1025-65535	
HomeProxyPort	home-proxy-port	none	enabled, disabled, forced	
RouteHomeProxy	route-home-proxy	list of nat headers: Call-ID Contact f From I Join m rRecord-Route Refer-To Replaces Replay-To Route t To v Via	empty, *, 0.0.0.0, ipv4/bitmask	
prefix	address-prefix		enabled/disabled	
TunnelRedirect	tunnel-redirect		<.com>	
UserNATTag	user-nat-tag		none, from-to, all	
HostNATTag	host-nat-tag		list of nat headers: Call-ID Contact f From I Join m r Record-Route Refer-To Replaces Replay-To Route t To v Via with values = NAT, fqdn-ip-ext, fqdn-ip-tgt, ip-ip-ext, ip-ip-tgt	
DomainSuffix	domain-suffix			
ParamMode	use-url-parameter			
ParamName	parameter-name			
SipNatHeaders	headers			
acliObjectName*#				

H.323 Stack

The following table lists SOAP attributes and sub-elements for the H.323 stack.

SOAP Attributes/Sub-elements	ACLI Session-router->h323->h323-stack	Default Values	Valid Values	SBC Version
acliObjectName *# state realm-id * assoc-stack local-ip ras-port q931-port H323AlternateTransport ipAddress *# q931-max-calls max-calls max-channels q931-start-port q931-number-ports dynamic-start-port dynamic-number-ports tcp-keeplive isgateway AnonMode filename H323TerminalAial e164 *# url *# ipAddress *# email *# h323-ID *# H323Prefixes e164 *# url *# ipAddress *# email *# h323-ID *#	name state realm-id assoc-stack local-ip ras-port q931-port alternate-transport q931-max-calls max-calls max-channels q931-start-port q931-number-ports dynamic-start-port dynamic-number-ports tcp-keepalive isgateway allow-anonymous filename terminal-alias prefixes	enabled <realm> 0.0.0.0 1719 1720 200 200 6 0 0 0 0 disabled enabled all	24 characters enabled/disabled <realm> empty or <h323-stack> empty or <HIP> 1025-65535 1025-65535 list of <ipv4:port> Ipv4:port >0 >0, must > q931-max-calls >0 0-65535 0, 1024, 2048, 4096, 8192, 16384, 32768 0-65535 0, 1024, 2048, 4096, 8192, 16384, 32768 enabled/disabled enabled/disabled all, agents-only, realm-prefix list of e164, url, h323-ID, email, ipAddress list of e164, url, h323-ID, email, ipAddress for gateway only	4.0.0 and above

SOAP Attributes/Sub-elements	ACLI Session-router->h323->h323-stack	Default Values	Valid Values	SBC Version
registration-ttl processRegistration proxy-mode h245-stage h245-tunneling stack-options auto-gk-discovery multicast gatekeeper gk-identifier callStartFast callStartSlow H323MediaProfile acliObjectName *# fs-in-first-msg	registration-ttl process-registration proxy-mode h245-stage h245-tunneling options auto-gk-discovery multicast gatekeeper gk-identifier call-start-fast call-start-slow media-profiles fs-in-first-msg	120 disabled connect disabled disabled enabled disabled disabled	>0 for gateway only enabled/disabled for gatekeeper only NONE, H225, H245 CONNECT, SETUP, ALERTING, CALL PROCEEDING, DYNAMIC, FACILITY, SETUP or CONNECT, NONE enabled/disabled list of options seperated by comma enabled, disabled ipAddress=ipv4:port for gateway only ipAddress=ipv4:port enabled/disabled enabled/disabled, each time only fast or only slow enabled list of media-profiles enabled/disabled	
rfc2833-mode	rfc2833-mode	transparent	transparent, preferred	4.1.0 and above
description	description			5.1.1 and above
H323StackAlarmThreshold severity*# value	alarm-threshold severity value	minor 0	minor, major, critical 0-100	6.2.0 and above

MGCP Config

The following table lists SOAP attributes and sub-elements for the MGCP config.

SOAP Attributes/Sub-elements	ACLI Session-router->mgcp-config	Default Values	Valid Values	SBC Version
realmPrivate * addressPrivate *#	pivate-realm private-address	<realm> 2727	<realm> Ipv4	4.0.0 and above
portPrivate	private-port	LineUnit	1025-65535	
mode	mode	256	Host, LineUnit, LinePrefix, FQDN, FQDN2, OnlyHost	
divisor	divisor	disabled		
unitPrefix	unit-prefix	disabled		
dnsAuthentication	dns-authentication	0	256, 65536, 16777216, 4294967295enabled/disabled	
dnsTranslation	dns-translation	disabled		
natTraversal	nat-traversal	0		
auditInterval	audit-interval	0.0.0.0		
options	options	2427	empty or <trans-pfl>	
caRedundancy	ca-redundancy	0<realm>	enabled/disabled	
caPingMethod	ca-ping-method	0.0.0.0	list of options	
caPingInterval	ca-ping-interval	2727	enabled/disabled	
hostGWPublic	public-gw-host		NTFY 1 ping@host	
addrGWPublic	public-gw-address		Ipv4/mask	
portGWPublic	public-gw-port		1025-65535	
portGWPublic2realmPublic	second-public-gw-portpublic-realm		0, 1025-65535<realm>	
pubCAHost	public-ca-host		Ipv4	
addrCAPublic	public-ca-address		1025-65535	
portCAPublic	public-ca-port			
portALG	alg-port	2427	1025-65535	4.1.4; 5.1.1 and below
MGCPConfigIpAddresses Addr *#	ca-failover-ip-addresses		List of ipv4 Ipv4	4.0.1 and above
rsipFailures	rsip-failures	500-509 511-519 522-599	500-599	5.1.0 and above
portMapStart portMapEnd	port-map-start port-map-end	0 0	0 or 1025-65535 0 or 1025-65535	5.1.1
caPingRetries	ca-ping-retries	0	0-4294967295	SC6.1.0M1

DNS Config

The following table lists SOAP attributes and sub-elements for the DNS config.

SOAP Attributes/ Sub-elements	ACLI media-manager->dns-config	Default Values	Valid Values	SBC Version
clientrealmID *# description ClientIpList IPAddress *# ServerDNSAttributes serverRealmID *# ServerDnsDomainSuffix acliObjectName * # ServerDnsAddressList IPAddress * # sourceAddress *# sourcePort *# transactionTimeout ServerDNSAddressTranslation serverprefix *# clientprefix *#	client-realm description client-address-list server-dns-attributes serverrealmID domain-suffix server-address-list source-address source-port transaction-timeout address-translation server-prefix client-prefix	<realm> 53 10	<realm> Ipv4 <realm> domain ipv4 ipv4 0-65535 0-999999999 ipv4/mask ipv4/mask	4.0.0 and above

Session Agent

The following table lists SOAP attributes and sub-elements for the session agent.

SOAP Attributes/Sub-elements	ACLI session-router->session-agent	Default Values	Valid Values	SBC Version
hostname *# ipAddress #	hostname ip-address	5060 enabled	FQDN or ipv4 0.0.0.0 or Ipv4	4.0.0 and above
port	port	UDP	0, 1025-65535	
state	state	disabled	enabled/disabled	
appProtocol #	app-protocol	disabled	SIP or H323	
appType	app-type	0	H323-GK or H323-GW for H323 only	
transMethod	transport-method	0		
realmID	realm-id	0	UDP, UDP+TCP, dynamicTCP, staticTCP	
description	description	0		
options	options	0		
SessionAgentMediaProfile	media-profiles	0	empty or <realm>	
	carriers	0	list of comma seperated options	
acliObjectName *#	allow-next-hop-ip	0		
SessionAgentCarriers	in-translationid	0	List of <media-profiles> for H323 only	
acliObjectName *#	outtranslationId			
allowNextHop	constraints		<media-profile>	
inTranslationId	max-sessions		List of carriers	
outTranslationId	max-outbound-sessions		<carrier-code>	
useConstraints	max-burst-rate		enabled/disabled	
maxNumSessions	max-sustain-rate		empty or <translation-profile>	
maxOutbSessions	time-to-resume		enabled/disabled	
maxBurstRate	ttr-no-response		0-999999999	
maxSustainedRate	in-service-period		0-999999999	
timeToResume	burst-rate-window		0-999999999	
noResponseTo	sustain-rate-window		0-999999999	
inServicePeriod			0-999999999	
burstWindow			0-999999999	
sustainedWindow			0-999999999	

SOAP Attributes/Sub-elements	ACLI session-router->session-agent	Default Values	Valid Values	SBC Version
trustMe proxyMode redirectAct allocMedia responseMap looseRouter inclCarrierAs pingMethod pingInterval	trust-me proxy-mode redirect-action send-media-session response-map loose-routing req-uri-carrier-mode ping-method ping-interval	enabled enabled disabled None 0	enabled/disabled empty, proxy, redirect, record-route empty, proxy, recurse enabled/disabled empty or <sip-response-code-profile> enabled, disabled None, URI-param, Prefix INFO, OPTIONS 0-999999999	4.0.0 and above (for SIP only)
localresponseMap pingToUserPart pingFromUserPart RequesturiHeader acliObjectName *# stopRecurse	local-response-map ping-to-user-part ping-from-user-part request-uri-headers stop-recurse		empty or <sip-response-code-profile> list of headers list of response codes, 300-599	
trustMeForLI	li-trust-me	disabled	enabled/disabled	
assertedID SessionAgentTrunkGroup acliObjectName *# inManipulationId outManipulationId maxRegisterSustainedRate	p-asserted-id trunk-group in-manipulationid out-manipulationid max-register-sustain-rate	0	sip:name@acme.com or tel:+1234 list of trunk groups or group:context empty or <sip-manipulation> 0-999999999	
earlyMediaAllow invalidateRegistrations	early-media-allow invalidate-registrations	disabled	empty, none, reverse, both enabled/disabled	4.0.1 and above (for SIP only)
minSeizure minAnswerSeizureRatio	min-seizures min-asr	5 0	1-999999999 0-100	4.0.1 and above
rfc2833-mode rfc2833-payload	rfc2833-mode rfc2833-payload	none 0	none, transparent, preferred 0, 96-127	4.1.0 and above for H323

SOAP Attributes/Sub-elements	ACLI session-router->session-agent	Default Values	Valid Values	SBC Version
maxInbSessions maxInbBurstRate maxOutbBurstRate maxInbSustainedRate maxOutbSustainedRate	max-inbound-sessions max-inbounds-burst-rate max-outbound-burst-rate max-outbound-sustain-rate	0 0 0 0 0	0-999999999 0-999999999 0-999999999 0-999999999 0-999999999	4.0.1; 4.1.1 and above
codecPolicy inServiceCodes outServicecodes	codec-policy in-service-response-codes out-service-response-codes		empty or <codec-policy> list of comma-separated response codes, 200-699	4.1.1 and above (for SIP only)
rfc2833-mode rfc2833-payload	rfc2833-mod rfc2833-payload	None 0	none, transparent, preferred, dual 0, 96-127	
reuse-connections tcp-keepalive tcp-reconn-Interval enforcementProfile	reuse-connections tcp-keepalive tcp-reconn-interval enforcement-profile	NONE none 0	NONE, TCP none, disabled, enabled 0, 2-300 empty or <enforcement-profile>	4.1.4; 5.1.0 and above (for SIP only)
maxRegisterBurstRate registerBurstWindow	max-register-burst-rate register-burst-window	0 0	0-999999999 0-999999999	4.1.4, 5.1.1 and above (for SIP only)
referCallTransferpingSendMode egressRealmID	refer-call-transferping-send-mode egress-realm-id	disabled keep-alive	enabled, disabled keep-alive, continuous empty or <realm>	5.1.1 and above (for SIP only)
SessionAgentRateConstraints method maxInBurstRate maxOutBurstRate maxInSustainedRate maxOutSustainedRate	rate-constraints method max-inbound-burst-rate max-outbound-burst-rate max-inbound-sustain-rate max-outbound-sustain-rate		INVITE, ACK, BYE, REGISTER, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, NOTIFY, REFER, UPDATE, MESSAGE, PUBLISH 0-999999999 0-999999999 0-999999999 0-999999999	5.1.1 and above

SOAP Attributes/Sub-elements	ACLI session-router->session-agent	Default Values	Valid Values	SBC Version
hmrString transMethod reuse-connections	manipulation-string transport-method reuse-connections	UDP NONE	UDP, UDP+TCP, dynamicTCP, staticTCP, dynamicTLS, staticTLS, staticSCTP, NONE, TCP, SCTP	6.1.0 and above (for SIP only)
pingAllAddresses sipProfile sipIsupProfile manipPattern referCallTransfer	ping-all-addresses sip-profile sip-isup-profile manipulation-pattern refer-call-transfer	disabled disabled	enabled, disabled empty or <sip-profile> empty or <sip-isup-profile> disabled, enabled, dynamic	6.2.0 above (for SIP only)
hostname *# ipAddress	hostname ip-address		fqdn, ipv4, ipv6 ipv4, ipv6	CX6.2.0 and above

Session Agent Group

The following table lists SOAP attributes and sub-elements for the session agent group.

SOAP Attributes/ Sub-elements	ACLI session-router->session-agent-group	Default Values	Valid Values	SBC Version
acliObjectName *# description	group-name description	enabled SIP	enabled/disabled SIP or H323	4.0.0 and above
state protocol # strategy SessionAgentGroupSipDest hostname *#	state app-protocol strategy dest	hunt	hunt, roundrobin, leastbusy, propdist, lowsusrate list of session-agents <sa name>	
SessionAgentGroupTrunkGroup acliObjectName *#	trunk-group		List of trunk groups or group:context <trk> or <trk>:<contxt>	4.0.0 and above (for SIP only)
sagRecurse stopRecurse	sag-recursion stop-sag-recursion	disabled 410, 407	enabled, disabled list of comma-separated response codes, 300-599	4.1.1 and above (for SIP only)

Local Policy

The following table lists SOAP attributes and sub-elements for local policy.

SOAP Attributes/Sub-elements	ACLI Session-router->local-policy	Default Values	Valid Values	SBC Version
routeName * LocalPolicyFrom # addr *# LocalPolicyTo # addr *# LocalPolicySourceRealm # acliObjectName *# activateTime deactivateTime state anonymousPriority LocalPolicyAttribute policyName * state startTime endTime dow cost LocalPolicyMediaProfiles acliObjectName *# carrierName nextHop # destRealm # appProtocol replace	from-address to-address source-realm activate-time deactivate-time state policy-priority policy-attribute state start-time end-time days-of-week cost media-profiles carrier next-hop realm app-protocol replace-uri	* * * enabled none enabled 0000 2400 U-S 0 SIP enabled	Route0, Route1…… +number, number, *, fqdn, ipv4 or 0.0.0.0 same * or <realm> yyyy-mm-dd-hh:mm:ss yyyy-mm-dd hh:mm:ss enabled/disabled none, normal, non-urgent, urgent, emergency RP0, RP1….. enabled, disabled 0000-2400 0000-2400 M, T, W, R, F, S, U, H or any combination 0-999999999 list of media-profiles <media-profile> <carrier-code> SAG:<sag>, <sa>, ipAddress, FQDN empty or <realm> SIP or H323 enabled/disabled	4.0.0 and above

SOAP Attributes/Sub-elements	ACLI Session-router->local-policy	Default Values	Valid Values	SBC Version
LocalPolicyAttribute startTime endTime dow cost LocalPolicyMediaProfiles acliObjectName *# carrierName nextHop # destRealm # appProtocol action isTermRoute replace	policy-attribute start-time end-time days-of-week cost media-profiles carrier next-hop realm app-protocol action terminate-recursion replace-uri	0000 0000 U-S 0 SIP none disabled	0000-2400 0000-2400 M, T, W, R, F, S, U, H or any combination 0-999999999 List of media-profiles <media-profile> <carrier> SAG:<sag>, <sa>, enum:<name> empty or <realm> SIP or H323 none, replace-uri, redirect enabled/disabled	4.0.1 and above
LocalPolicyFrom # addr *# LocalPolicyTo # addr *#	from-address to-address		also support 12*34, **** for number (potsstar)	4.0.1, 4.1.1 and above
LocalPolicyAttribute nextHop	policy-attribute next-hop		SAG:<sag>, <sa>, enum:<name>, lrt:<name>, enum:<name>;key=<value>, lrt:<name>;key=<value>, ipAddress, FQDN	4.1.1 and above
LocalPolicyAttribute nextHop	policy-attribute next-hop		SAG:<sag>, <sa>, enum:<name>, lrt:<name>, enum:<name>;key=<value>, lrt:<name>;key=<value>, ipAddress, FQDN, ldap:<name>	4.50 and 4.5.1
description	description			5.1.1 and above

SOAP Attributes/Sub-elements	ACLI Session-router->local-policy	Default Values	Valid Values	SBC Version
LocalPolicyAttribute methods LocalPolicyFrom # addr *# LocalPolicyTo # addr *#	policy-attribute methods from-address to-address		space seperated list of INVITE, REGISTER, PRACK, OPTIONS, INFO, SUBSCRIBE, NOTIFY, REFER, UPDATE, MESSAGE, PUBLISH also supports DS: 123#456*Ab (alpha-numeric-dtmf, a combination of A-D, a-d, 0-9, #, *) (potsstar)	6.1.0 and above
LocalPolicyFrom # addr *# LocalPolicyTo # addr *# LocalPolicyAttribute eLocStrLkup eLocStrMatch lookup nextKey	from-address to-address policy-attribute eloc-str-lkup eloc-str-match lookup next-key	* * disabled single	+number (e164), number(pots), num**num (potsstar), */fqdn/ipv4/0.0.0.0 (hostname), DS: [A-D][a-d][0-9]#*(potsstar), urn:service:[sos, sos.fire, sos.animal-control] (hostname) enabled, disabled 24 chars such as noc, lac, line-code single, multi $TO, $FROM, $PAI or any string	6.2.0 and above

SOAP Attributes/Sub-elements	ACLI Session-router->local-policy	Default Values	Valid Values	SBC Version
LocalPolicyFrom # addr *# LocalPolicyTo # addr *# LocalPolicyAttribute nextHop	from-address to-address policy-attribute next-hop	* *	+number (e164), number(pots), num**num (potsstar), */fqdn/ipv4/ipv6/0.0.0.0 (hostname), DS:[A-D][a-d][0-9]#*(potsstar), urn:service:[sos, sos.fire, sos.animal-control] (hostname) SAG:<sag>, <sa>, enum:<name>, lrt:<name>, enum:<name>;key=<cic|rn|value>, lrt:<name>;key=<cic|rn|value>, ipv4, ipv6, FQDN	CX6.2.0 and above

Network Management Control

The following table lists SOAP attributes and sub-elements for network management control.

SOAP Attributes/Sub-elements	ACLI Session-router->net-management-control	Default Values	Valid Values	SBC Version
acliObjectName *# state aclitype value treatment nextHop nextHopRealm nextHopProtocol statusCode causeCode gapRateMaxCount gapRateWindowSize DestinationId destinationId *#	name state type value treatment next-hop realm-next-hop protocol-next-hop status-code cause-code gap-rate-max-count gap-rate-window-size destination-identifier	enabled 0 0 0 503 63	24 characters enabled, disabled empty, gap-rate, gap-percent, priority -1, 0-100 for gap-percent, 0-2147483647 for gap-rate empty, reject, divert empty, hostname:port, ipv4:port, sa, SAG:sa empty, <realm> empty, SIP, H323 1-699 0-999999999 0-999999999 0-999999999 List of number(^as wildcard), prefix(^as wildcard), ipv4(^as wildcard) and fqdn	4.1.1 and above
rphFeature rphProfile rphPolicy	rph-feature rph-profile rph-policy		disabled or enabled empty or <rph-profile> empty or <rph-policy>	4.1.4
destinationId destinationId *#	destination-identifier		list of number, prefix, ipv4 or fqdn (^ as wildcard for digit), urn:service:(sos, sos.fire, sos.animal-control etc.)	6.2.0 and above

SIP Header Manipulation

The following table lists SOAP attributes and sub-elements for SIP header manipulation.

SOAP Attributes/ Subelements	ACLI session-router->sip-manipulation	Default Values	Valid Values	SBC Version
acliObjectName * # HeaderRule	name header-rule	none any	add, delete, manipulate, none empty or <value>	4.0.0 and above
acliObjectName * #	name	none		
action	action	any	any, request, reply	
matchValue	match-value		empty or comma separated strings	
msgType	msg-type			
methods	methods		header-value, header-param, uri-user, uri-host, uri-port, uri-param, uri-header, uri-user-param	
ElementRule	element-rule			
acliObjectName *#	name			
aclitype	type			
action	action		add, replace, delete-header, delete-element, none	
matchValueType	match-val-type			
matchValue	match-value		IP, FQDN, ANY	
newValue	new-value		empty or <255 characters>	
			empty or combination of $ORIGINAL, $LOCAL_IP, $REMOTE_IP, $REMOTE_VIA_HOST, $TRUNK_GROUP, $TRUNK_GROUP_CONTEXT, <any string>, +, -, +^, -^	

SOAP Attributes/ Subelements	ACLI session-router->sip-manipulation	Default Values	Valid Values	SBC Version
acliObjectName * # description	name description	none case-sensititive	255 characters 255 characters or @ status-line	4.1.1 and above
HeaderRule	header-rule	any	add, delete, manipulate, store, none	
acliObjectName * #	name	none	case-sensitive, case-insensitive, pattern-rule	
headerName #	header-name	ANY	empty or <reg-expr>	
action	action	case-sensitive	any, request, reply	
cmpType	comparison-type		empty or <reg-expr>	
matchValue	match-value		empty or comma-seperated strings	
msgType	msg-type		255 characters	
newValue	new-value		255 characters	
methods	methods		header-value, header-param-name, header-param, uri-display, uri-user, uri-user-param, uri-host, uri-port, uri-param-name, uri-param, uri-header-name, uri-header, status-code, reason-phrase,	
ElementRule	element-rule		add, replace, delete-header, delete-element, store, none	
acliObjectName *#	name		IP, FQDN, ANY	
paramName	parameter-name		case-sensitive, case-insensitive, pattern-rule	
aclitype	type		empty or <reg-expr-value>	
action	action		empty or <reg-expr-value> with pre0defined parameters:	
matchValueType	match-val-type		$ORIGINAL, $LOCAL_IP, $REMOTE_IP, $REMOTE_VIA_HOST, $TRUNK_GROUP, $TRUNK_	
cmpType	comparison-type			
matchValue	match-value			
newValue	new-value			

SOAP Attributes/ Subelements	ACLI session-router->sip-manipulation	Default Values	Valid Values	SBC Version
			GROUP_CONTEXT	
Header Rule action cmpType newValue ElementRule cmpType newValue action aclitype	header-rule action comparison-type new-value element-rule comparison-type new-value action type	none	add, delete, manipulate, store, none, sip-manip case-sensitive, case-insensitive, pattern-rule, boolean, refer-case-sensitive, refer-case-insensitive empty, <reg-expr>, or <sip-manipulation> case-sensitive, case-insensitive, pattern-rule, boolean, refer-case-sensitive, refer-case-insensitive empty or <reg-expr> with pre-defined parameters: $ORIGINAL, $LOCAL_IP, $LOCAL_PORT, $REMOTE_IP, $REMOTE_PORT, $REMOTE_VIA_HOST, $TRUNK_GROUP, $TRUNK_GROUP_CONTEXT add, replace, delete-header, delete-element, store, none, find-replace-all header-value, header-param-name, header-param, uri-display, uri-user, uri-user-param, uri-host, uri-port, uri-param-name, uri-param, uri-header-name, uri-header, statust-code, reason-phrase, mime	4.1.4; 5.1.1 and above

SOAP Attributes/ Subelements	ACLI session-router->sip-manipulation	Default Values	Valid Values	SBC Version
HeaderRule matchValue ElementRule aclitype matchValue	header-rule match-value element-rule type match-value		empty or <regular-expr> with $MANIP_STRING header-value, header-param-name, header-param, uri-display, uri-user, uri-user-param, uri-host, uri-port, uri-param-name, uri-param, uri-header-name, uri-header, status-code, reason-phrase, mime, uri-user-only, uri-phone-number-only empty or <regular-expr> with $MANIP_STRING	6.1.0 and above

SOAP Attributes/ Subelements	ACLI session-router->sip-manipulation	Default Values	Valid Values	SBC Version
HeaderRule acliObjectName * # action msgType matchValue newValue ElementRule action matchValue newValue	header-rule name action msg-type match-value new-value element-rule action match-value new-value	none any none	unique and ordered with mime-rule, mime-isup-rule add, delete, manipulate, store, none, sip-manip, find-replace-all, reject, log any, request, reply, out-of-dialog empty or <regular-expr> with $MANIP_STRING, $MANIP_PATTERN empty or <regular-expr> or <sip-manipulation> or ACME_NAT_TO_FROM_IP add, replace, delete-header, delete-element, store, none, find-replace-all, reject, log, sip-manip empty or <regular-expr> with $MANIP_STRING ($M_STRING), $MANIP_PATTERN empty or <sip-manipulation> or <reg-expr> with reserved words and operators: $ORIGINAL, $LOCAL_IP/PORT, $REMOTE_IP/PORT, $REMOTE_VIA_HOST, $TRUNK_GROUP ($T_GROUP), $TRUNK_GROUP_CONTEXT ($T_CONTEXT), $REPLY_IP/PORT, $TARGET_IP/PORT, $TO/FROM/CONTACT/RURI/PAI/PPI/	6.2.0 and above

SOAP Attributes/ Subelements	ACLI session-router->sip-manipulation	Default Values	Valid Values	SBC Version
			PCPID_USER/ PHONE/HOST/ PORT, $TIMESTAMP_UTC, $CALL_ID, &, |, ==, ~=, !=, <=, >=, <, >	
MimeRules acliObjectName * # contentType action cmpType msgType format methods matchValue newValue MimeHeaderRule acliObjectName *# mimeHeaderName # action cmpType matchValue newValue	mime-rule name content-type action comparison-type msg-type format methods match-value new-value mime-header-rule name mime-header-name action comparison-type match-value new-value	none case-sensitive any ascii-string none case-sensitive	unique and ordered with header-rule, mime-isup-rule 255 chars such as application/SDP, @preamble, @epilogue add, delete, manipulate, store, none, sip-manip, find-replace-all, reject, log case-sensitive, case-insensitive, pattern-rule, boolean, refer-case-sensitive, refer-case-insensitive any, request, reply, out-of-dialog ascii-string, hex-ascii, binary-ascii empty or comma seperated strings 255 chars 255 chars such as Content-Disposition add, replace, store, none, sip-manip, find-replace-all, reject, log case-sensitive, case-insensitive, pattern-rule, boolean, refer-case-sensitive, refer-case-insensitive	6.2.0 and above

SOAP Attributes/ Subelements	ACLI session-router->sip-manipulation	Default Values	Valid Values	SBC Version
MimeISUPRules acliObjectName * # contentType isupSpec isupMsgTypes action cmpType msgType methods matchValue newValue MimeHeaderRule MimeISUPParamRule acliObjectName *# parameterType parameterFormat action cmpType matchValue newValue	mime-isup-rule name content-type isup-spec isup-msg-types action comparison-type msg-type methods match-value new-value mime-header-rule isup-param-rule name type format action comparison-type match-value new-value	ansi-2000 none case-sensitive any 0 hex-ascii none case-sensitive	unique and ordered with header-rule, mime-isup-rule 255 chars such as application/ISUP ansi-2000, itu-99, gr-317, etsi-356 empty or comma seperated list of 1-255 add, delete, manipulate, store, none, sip-manip, find-replace-all, reject, log case-sensitive, case-insensitive, pattern-rule, boolean, refer-case-sensitive, refer-case-insensitive any, request, reply, out-of-dialog empty or comma seperated strings 255 chars 0-255 number-param, hex-ascii, binary-ascii, ascii-string, bcd add, replace, store, none, sip-manip, find-replace-all, reject, log case-sensitive, case-insensitive, pattern-rule, boolean, refer-case-sensitive, refer-case-insensitive	6.2.0 and above
splitHdrList joinHdrList	split-headers join-headers		comma seperated list of header names such as "Allowed,P-Asserted-Identity", "Diversion,Allow"	6.2.0M1

Session Constraints

The following table lists SOAP attributes and sub-elements for session constraints.

SOAP Attributes/Sub-elements	ACLI Session-router->session-constraints	Default Values	Valid Values	SBC Version
acliObjectname * #	name	disabled	24 characters	4.0.1; 4.1.1 above
useConstraints	state	0	enabled/disabled	
maxNumSessions	max-sessions	0	0-999999999	
maxInbSessions	max-inbound-sessions	0	0-999999999	
maxOutbSessions	max-outbound-sessions	0	0-999999999	
maxBurstRate	max-burst-rate	0	0-999999999	
maxInbBurstRate	max-inbound-burst-rate	0	0-999999999	
maxOutbBurstRate	max-outbound-burst-rate	0	0-999999999	
maxSustainedRate	max-sustain-rate	0	0-999999999	
maxInbSustainedRate	max-inbound-sustain-rate	5	0-999999999	
maxOutbSustainedRate	max-outbound-sustain-rate	0	1-999999999	
minSeizure	min-seizures	0	0-100	
minAnswerSeizureRatio	min-asr	0	0-999999999	
timeRoResume	time-to-resume	0	0-999999999	
noResponseTo	ttr-no-response	0	0-999999999	
inservicePeriod	in-service-period	0	0-999999999	
burstWindow	burst-rate-window		0-999999999	
sustainedWindow	sustain-rate-window			
SessionConstraintRateConstraints	method		INVITE, ACK, BYE, REGISTER, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, NOTIFY, REFER, UPDATE, MESSAGE, PUBLISH	5.1.1 and above
method	max-inbound-burst-rate		0-999999999	
maxInBurstRate	max-outbound-burst-rate		0-999999999	
maxOutBurstRate	sustain-rate-max-outbound		0-999999999	
maxInSustainedRate	max-outbound-sustain-rate		0-999999999	
maxOutSustainedRate				

Session Translation

The following table lists SOAP attributes and sub-elements for session translation.

SOAP Attributes/ Sub-elements	ACLI session-router->session-translation	Default Values	Valid Values	SBC Version
Id *# RuleCalling acliObjectName *# RuleCalled acliObjectName *#	id rules-calling rules-called		list of translation rules	4.0.0 and above

Translation Rules

The following table lists SOAP attributes and sub-elements for translation rules.

SOAP Attributes/ Sub-elements	ACLI session-router->translation-rule	Default Values	Valid Values	SBC Version
Id *# aclitype add_s add_indx del_s del_indx	id type add-string add-index delete-string delete-index	none 0 0	add, delete, replace, none <string> 0-999999999, $ for appending at the end @ as wild char or <string> 0-999999999	4.0.0 and above

RPH Profile

The following table lists the SOAP attributes and sub-elements for RPH profiles.

SOAP Attributes/ Sub-elements	ACLI session-router->rph-profile	Default Values	Valid Values	SBC Version
acliObjectName *# callTreatment mediaPolicy RValues rValue *#	name call-treatment media-policy r-values	accept	24 characters accept, reject, priority empty or <QoS marking profile> list or r-values such as ets.0 or wps.1, ets.1	4.1.4; 5.1.0 and above

RPH Policy

The following table lists the SOAP attributes and sub-elements for RPH policies.

SOAP Attributes/Sub-elements	ACLI session-router->rph-policy	Default Values	Valid Values	SBC Version
acliObjectName *# OverrideRValues rValue *# InsertRValues rValue *#	name override-r-values insert-r-values		24 characters One rValue	4.1.4; 5.1.0 and above

Host Routes

The following table lists the SOAP attributes and sub-elements for host routes.

SOAP Attributes/Sub-elements	ACLI system->host-route	Default Values	Valid Values	SBC Version
netAddress *# netmask gateway description	dest-network netmask gateway description		Ipv4 Ipv4	4.0.0 and above 5.1.1 and above
netAddress *# netmask gateway	dest-network netmask gateway		Ipv4, ipv6, ipv6/prefix Ipv4, not allowed for ipv6 Ipv4, ipv6	CX6.2.0 and above

SIP Local Map Entry

The following table lists the SOAP attributes and sub-elements for SIP local map entries.

SOAP Attributes/Sub-elements	ACLI session-router->local-response-map->entries	Default Values	Valid Values	SBC Version
localerror *# sipstatus cause sipreason causereason	local-error sip-status q850-cause sip-reason q850-reason	0	invalid-message, cpu-overload, media-released, media-not-allocated 100-699	4.0.0 and above

SOAP Attributes/Sub-elements	ACLI session-router->local-response-map->entries	Default Values	Valid Values	SBC Version
localerror *#	local-error		invalid-message, cpu-overload, media-released, media-not-allocated, enum-void-route	4.1.1 and above
localerror *#	local-error		invalid-message, cpu-overload, media-released, media-not-allocated, enum-void-route, monthly-minutes-exceed, next-hop-sa-oos, recv-sa-exc-constraints, revc-sip-int-exc-constraints, next-hop-sa-exc-constraints, next-hop-sip-int-exc-constraints, realm-bw-exc-poly-serv-reject, no-steering-pool-ports-available, allow-anonymous-rejection, sdp-address-mismatch,	4.1.4; 5.1.1 and above

SOAP Attributes/Sub-elements	ACLI session-router->local-response-map->entries	Default Values	Valid Values	SBC Version
localerror *# method registerResponseExpires	local-error method register-response-expires		invalid-message, cpu-overload, media-released, media-not-allocated, enum-void-route, monthly-minutes-exceed, next-hop-sa-oos, recv-sa-exc-constraints, revc-sip-int-exc-constraints, next-hop-sa-exc-constraints, next-hop-sip-int-exc-constraints, realm-bw-exc-poly-serv-reject, no-steering-pool-ports-available, allow-anonymous-rejection, sdp-address-mismatch, request-method-throttled empty, REGISTER 0-999999999	5.1.1 and above

Codec Policy

The following table lists the SOAP attributes and sub-elements for codec policies.

SOAP Attributes/Sub-elements	ACLI media manager->codec-policy	Default Values	Valid Values	SBC Version
acliObjectName *# CodecPolicyAllow acliObjectName *# CodecPolicyOrder acliObjectName *#	name allow-codecs order-codecs		list of *, <media profile>, PCMU, G726-32, G723, PCMA, G722, G726, G729, telephone-event with appending exception :no or :force same values as in list above, but order matters	4.1.1

Access Control

The following table lists the SOAP attributes and sub-elements for acess control.

SOAP Attributes/ Sub-elements	ACLI session-router->access-control	Default Values	Valid Values	SBC Version
inRealm * inSrc *# InDst *# appProtocol *# transProtocol *# access rateLimit trustLevel errMsgThreshold maxMsgThreshold denyTimer maxMsgThreshold Untrusted	realm-id source-address destination-address application-protocol transport-protocol access average-rate-limit trust-level invalid-signal-threshold maximum-signal-threshold deny-period untrusted-signal-threshold	0.0.0.0 0.0.0.0 all permit 0 none 0 0 30 0 or the same as average-rate-limit	<realm> Ipv4/mask:port/mask Ipv4/mask:port/mask for application-protocol, NONE NONE, SIP, MGCP TCP, UDP, all permit, deny 0-4294967295 none, low, medium, high 0-4294967295 0-4294967295 0-4294967295	4.0.0
reservedBandwidth	minimum-reserved-bandwidth	0	0-999999999	4.1.4; 5.1.1 and above
description	description		255 characters	5.1.1 and above
natTrustThreshold	nat-trust-threshold	0	0-65535	6.1.0 and above
cacFailThreshold untrustedCacFailThreshold	cac-fail-threshold untrusted-cac-failure-threshold	0 0	0-999999999 0-999999999	6.2.0 and above
inSrc *# inDst *#	source-address destination-address		ipAddress/mask:port/mask, ipAddress is either ipv4 or ipv6, mask is 32 for ipv4, 128 for ipv6	CX6.2.0 and above

Media Profile

The following table lists the SOAP attributes and sub-elements for media profile.

SOAP Attributes/Sub-elements	ACLI session-router->media-profile	Default Values	Valid Values	SBC Version
acliObjectName *# mediaType payloadType transport reqBandwidth framesPerPacket parameters	name media-type payload-type transport req-bandwidth frames-per-packet parameters	audio 0 RTP/AVP 0 0	24 characters audio, video, data, application, control RTP/AVP, UDP 0-999999999 0-256 space separated <name=value> pair	4.0.0 and above
avgRate	average-rate-limit	0	0-125000000	
peakRate maxBurstSize	peak-rate-limit max-burst-size	0 0	0-125000000 0-125000000	
mediaType sdpRateLimit sdpBandwidth	media-type sdp-rate-limit-headroom sdp-bandwidth	audio 0 disabled	audio, video, data, appkication, control, imate, text 0-100 enabled or disabled	4.1.1 and above
policeRate	police-rate	0	0-999999999	5.1.1 and above
subName	subname			6.1.0 and above

SIP Response Map

The following table lists the SOAP attributes and sub-elements for SIP response map.

SOAP Attributes/Sub-elements	ACLI session-router->sip-response-map	Default Values	Valid Values	SBC Version
acliObjectName *# SIPResponseMapEntry statusRcvd *# statusSend # reason	name entries recv-code xmit-code reason		100-699 100-699	4.0.0 and above
method registerResponseExpires	method register-response-expires	0	empty, REGISTER 0-999999999	5.1.1 and above

Diameter Director Agent

The following table lists the SOAP attributes and sub-elements for the DIAMETER Director agent.

SOAP Attributes/ Sub-elements	ACLI session-router->diameter-director-agent	Default Values	Valid Values	SBC Version
port constraintName	port constraint-name	3868 30	Valid port number 0-65535	DD1.0.0 and above
appProtocol	protocol	enabled	enabled or disabled	
watchDogTimer	watchdog-timer	TCP	TCP or SCTP	
state	state	outbound	FQDN or IP address diameter-manipulation rule	
transportProtocol	transport-protocol	0	Existing realm name	
responseMap	response-map	authentication	diameter-manipulation rule	
hostname	hostname		outbound, inbound, inbound-dynamic-ip	
inManipulationId	in-manip-ip		256-character string	
realmId	realm-id		IP address	
outManipulationId	out-manip-id		32-bit hexadecimal or 32-bit integer	
connectionMode	connection-mode		32-bit integer	
description	description		authentication or accounting	
options	options			
ipAddress	ipAddress			
diamDirApplication	diameter-director-applications			
appId	application-id			
vendorId	vendor-id			
appType	application-type			
tosValue	tos-value			DD1.0.0M1 and DD2.0.0M1

Diameter Director Configuration

The following table lists the SOAP attributes and sub-elements for the DIAMETER Director agent.

SOAP Attributes/Sub-elements	ACLI session-router->diameter-director-config	Default Values	Valid Values	SBC Version
redundancyPortllAction	redndancy-port load-limit-action	1999 reject	Valid port number reject or drop	DD1.0.0 and above
dynamicRouting	dynamic-routing	enabled	enabled or disabled	
state	state	enabled		
loadLimit	load-limit	85	enabled or disabled	
activeRedPort	active-redundancy-port	9000	0-100	
redNumTrans		50000	Valid port number	
llExpResultCode	red-max-transactions	3004	0-999999	
statefulPolicy			Valid result code	
llResultCode	load-limit-exp-result-code			
	stateful-policy			
	load-limit-result-code			
options	options			DD2.0.0 and above

Diameter Director Constraints

The following table lists the SOAP attributes and sub-elements for the DIAMETER Director constraints.

SOAP Attributes/ Sub-elements	ACLI session-router->diameter-director-constraints	Default Values	Valid Values	SBC Version
burstWindow	burst-rate-window	0	0-999999	DD1.0.0 and above
maxInbSustainedRAte	max-inbound-sustain-rate	0	0-999999	
maxOutbBurstRate	max-outbound-burst-rate	0	0-999999	
sustainedRate	sustain-rate-window	0	0-999999	
useConstraints	state	enabled	enabled or disabled	
maxBurstRate	max-burst-rate	0	0-999999	
maxInbBurstRate	max-inbound-burst-rate	0	0-999999	
maxOutbBurstRate	max-outbound-burst-rate	0	0-999999	
timeToResume	time-to-resume	0	0-999999	
name	name	3004	0-999999	
maxSustainedRate	max-sustained-rate	0	1000-6000	
lastModifiedBy	last-modified-by		0-999999	
resultCode	result-code		0-999999	
lastModifiedDate	last-modified-date		0-999999	
messageRateConstraints	message-rate-constraints		0-999999	
maxOutSustainedRate	max-outbound-sustain-rate			
maxInSustainedRate	max-inbound-sustain-rate			
maxInBurstRate	max-inbound-burst-rate			
command	command			
maxOutBurstRate	max-outbound-burst-rate			

Diameter Director Group

The following table lists the SOAP attributes and sub-elements for the DIAMETER Director group.

SOAP Attributes/Sub-elements	ACLI session-router->diameter-director-constraints	Default Values	Valid Values	SBC Version
groupName description lastModifiedBy state lastModifiedDate strategy inManipulationId outManipulationId recursiveRouting recursionTimeout doRecursion transactionTimeout resultCodes expResultCodes diamDirApplication appId vendorId appType destination seqno name	group-name description last-modified-by state last-modified-date strategy in-manip-id out-manip-id recursive-routing recursion-timeout do-recursion transaction-timeout result-codes exp-result-codes diameter-director-application application-id vendor-id application-type destinations seqno name	enabled hunt 100000 disabled 32000 0 authentication	256 character string enabled or disabled hunt diameter-manipulation rule diameter-manipulation rule 1-999999 enabled or disabled 1-999999 valid diameter result code 32-bit hexadecimal or 32-bit integer 32-bit integer authentication or accounting	DD1.0.0 and above

Diameter Director Interface

The following table lists the SOAP attributes and sub-elements for the DIAMETER Director interface.

SOAP Attributes/ Sub-elements	ACLI session-router->diameter-director-constraints	Default Values	Valid Values	SBC Version
constraintName outManipId state routingPolicy realmId suppVendorIds originHostId description originHostFormat lastModifiedBy lastModifiedDate inManipId sipPort port tlsProfile transProtocol address anonMode imsAkaProfile sctpMultiHomeAddrs diamDirApplication appId vendorId appType	constraint-name out-manip-id state routing-policy realm-id supported-vendor-ids origin-host-identifier description origin-host-format last-modified-by last-modified-date in-manip-id diameter-director-ports port tls-profile transport-protocol address allow-anonymous ims-aka-profile multi-home-addrs diameter-director-application application-id vendor-id application-type	enabled none 3868 TCP all 0 authentication	diameter director constraint diameter-manipulation rule disabled 256 character string 256 character string 256 character string none, identifier, identifier-with-realm diameter-manipulation rule number greater than 1023 TCP, SCTP IP address all, agents-only IP address 32-bit hexadecimal or integer 32-bit integer authentication, accounting	DD1.0.0 and above
tosValue	tos-value			DD1.0.0M1 and DD2.0.0M1

Diameter Manipulation

The following table lists the SOAP attributes and sub-elements for the DIAMETER manipulation.

SOAP Attributes/Sub-elements	ACLI session-router->diameter-director-constraints	Default Values	Valid Values	SBC Version
description name lastModifiedBy lastModifiedDate diameterManipRules seqno newValue avpCodeDescr name cmpType action matchValue avpCode msgType msgCmdCode avpType avpHeaderRule headerType newValue name action matchValue	description name last-modified-by last-modified-date diameter-manip-rules seqno new-value descr-avp-code name comparison-type action match-value avp-code msg-type msg-cmd-code avp-type avp-header-rule header-type new-value name action match-value	case-sensitive none 0 any 0 none none	256 character string 256 character string AVP header-rule 256 character string case-sensitive, canse-insensitive, pattern-rule, boolean none, add, delete, store, diameter-manip, group-manip, find-replace-all, replace AVP code any, request, reply diameter message code none, octet-string, octet-hex, integer32, unsignedint32, address, diameteruri, enumerated avp-flag or avp-vendor-id none, add, delete, replace	DD1.0.0 and above

C

Running a Legacy SOAP Client API

Users who have created client applications with now deprecated APIs can run these applications after completing the following procedure.

1. Extract NNC700WSlassic.zip (contained on the Oracle software distribution CD) to a folder on the client computer. This folder provides the [WSClassicClient_HOME}.
2. Move existing applications, created with the now deprecated provisioning APIs, to the {WSClassicClient_HOME}/sampleSouce folder.
3. Delete the directory that previously contained client applications.
4. Go to {WSClassicClient_HOME}/bin.
5. Edit run.bat, the file that allows you to run client application code, by changing the JAVA_HOME path variable to match the JDK installation path. In addition, edit the SERVER_NAME and SERVER_PORT variables to match the IP address and port number of the Oracle Communications Session Delivery Manager SOAP API Server.

   > **Note:**
   >
   > Client application code now requires JDK 1.6.0 or later; the latest update is recommended.

6. Edit build.bat by making the same change to the JAVA_HOME path variable.
7. The following Step, which imports one or more server certificates to a specific JAVA keystore, is required only if the client interface will run over HTTPS. This Step can be safely ignored if client/server transactions will take place over unsecured HTTP.
   a. Use FTP to move a copy of a Oracle Communications Session Delivery Manager SOAP API Server public certificate to the JAVA_HOME location on the client computer.
   b. The certificate is usually at opt/AcmePacket/NNC700/ssl/nncentral_server.cer on the Net-Net Central Server.
   c. Use the JAVA keytool utility to import the public certificate into a specified JAVA keystore. For example,

      ```
      keytool -import -keystore trustedCerts -alias NNC-01 -file nnC01.cer
      ```

      imports the certificate file, nnC01.cert, into the keystore named trustedCerts; the keystore file will be referenced by the NNC-01 alias.

      Note that you will be prompted for the keystore password before the import operation is initiated.

      For example:

      ```
      Owner: EMAILADDRESS=test@test.com, CN=172.30.10.120, OU=NmsCore,
      O=Acme Packet Inc., ST=Some-State, C=AU
      ```

```
Issuer: EMAILADDRESS=test@test.com, CN=172.30.10.120,
OU=NmsCore,
O=Acme Packet Inc., ST=Some-State, C=AU
Serial number: 8b4d53819b6dfff1
Valid from: Tue Nov 14 16:04:53 EST 2006 until: Sat Jan 31
16:04:53 EST
2015
Certificate fingerprints:
MD5: 98:DA:F6:04:A8:A0:CA:D4:33:83:2A:3F:CE:C3:FB:CD
SHA1:
F4:BB:72:7D:43:25:56:86:6A:70:55:27:63:96:D2:13:DF:89:B2:68
Trust this certificate? [no]: y
Certificate was added to keystore
```

d. Edit run.bat by changing the TRUST_STORE variable to match the location of the JAVA keystore that contains the public certificates of associated Oracle Communications Session Delivery Manager SOAP API Servers.

e. Edit run.bat by changing the TRUST_STORE_PASSWORD to match the password required to access the JAVA keystore containing the Oracle Communications Session Delivery Manager SOAP API Server certificates.

f. Use the JAVA keytool utility to conform the presence of the key in the keystore. For example,

```
keytool -list -v -keystore trustedCerts
```

provide a verbose display of the contents of the designated JAVA keystore, in this case, trustedCerts.

Note that you will be prompted for the keystore password before the keystore contents are displayed.

Repeat Steps 7a, 7b, and 7e to import additional Net-Net Central Server certificates to the same JAVA keystore.

8. If present, comment out the following code in your applications:

```
/* org.apache.axis.client.Stub yourStub = (Stub) emsLevelStub;//
add this line
yourStub._setProperty(org.apache.axis.MessageContext.HTTP_TRANSPORT_
VERSION,
org.apache.axis.transport.http.HTTPConstants.HEADER_PROTOCOL_V11);//
 add this line

//For the defect: SocketTimeoutException
org.apache.axis.client.Stub s = (Stub) networkLevelStub;
s.setTimeout(1800000);
//30 minutes, 30*60*1000

*/
```

9. Edit {WSClassicClient_HOME}/conf/client.properties by changing the value of the session_timeout_ms property to specify a session timeout value, expressed in milliseconds.

10. Use build.bat to compile the client application.
11. Use run.bat to run the client application.