



Audio Security Classification for Trunk User Calls

Feature Description

Release 21.0

Document Version 1.5

AudioSecurityClassificationForTrunkUserCallsFD-210

Market Request Number 189490

Feature Request Number 195363

BroadSoft® Guide

Copyright Notice

Copyright© 2014 BroadSoft, Inc.

All rights reserved.

Any technical documentation that is made available by BroadSoft, Inc. is proprietary and confidential and is considered the copyrighted work of BroadSoft, Inc.

This publication is for distribution under BroadSoft non-disclosure agreement only. No part of this publication may be duplicated without the express written permission of BroadSoft, Inc., 9737 Washingtonian Boulevard, Suite 350, Gaithersburg, MD 20878.

BroadSoft reserves the right to make changes without prior notice.

Trademarks

Any product names mentioned in this document may be trademarks or registered trademarks of BroadSoft or their respective companies and are hereby acknowledged.

This document is printed in the United States of America.

Document Revision History

Version	Reason for Change	Date
0.1 Draft	Created document.	July 22, 2014
0.2 Draft	Updated document in Provisioning Server section.	July 22, 2014
0.3 Draft	Added information on Execution Server (XS).	August 15, 2014
0.4 Draft	Updated document after the first Functional Specification (FS) review.	August 21, 2014
0.5 Draft	Updated document after the second FS review.	September 4, 2014
1.0 Approved	Approved document.	September 9, 2014
1.1	Added new parameter to the DNC header in section 6.3 SIP/MGCP Interface Impact .	October 3, 2014
1.2	Updated behavior changes on playing announcement in section 6.4.2.2 Call Recording .	October 22, 2014
1.3	Edited document.	October 24, 2014
1.4	Approved editing changes.	October 30, 2014
1.5	Finalized and published document.	November 4, 2014

Table of Contents

1	Feature Overview and Purpose	7
2	Detailed Feature Description.....	8
2.1	Two-Party Call	8
2.1.1	Security Classification Announcement Call Flow in Audio Call.....	9
2.1.2	Security Classification Announcement Call Flow in Video Call.....	11
2.2	Three-Way and N-Way Calls	13
2.3	Meet-Me Conference	14
2.4	Media Server Recovery.....	14
2.5	Execution Use Cases.....	14
2.5.1	Two-Party Audio Call with Two Trunk Group User.....	14
2.5.2	Two-Party Video Call with One Trunk Group User.....	14
2.5.3	Mid-Call Security Classification Level Changed	15
2.5.4	Call Transfer.....	15
2.5.5	N-Way Conference.....	15
2.5.6	Meet-Me Call.....	16
2.5.7	Shared Call Appearance – Bridging	17
2.6	Provisioning Steps.....	17
2.7	Client Interaction Use Cases	17
3	Provisioning Impacts.....	18
3.1	Configuration Data.....	18
3.1.1	System Security Classification Parameters	18
3.2	Centralized Configuration Data.....	18
3.3	Web Portal Impacts	18
3.3.1	General Description	18
3.3.2	Policy Impacts.....	18
3.3.3	Web Pages	18
3.3.4	Help Pages	19
3.4	CLI Impacts.....	19
3.5	Open Client Interface-Provisioning (OCI-P) Impact.....	19
3.5.1	Summary.....	19
3.5.2	Command Impacts.	19
3.5.3	Deprecated Commands	20
3.5.4	Reporting Impacts	20
3.6	Application Server Query User/Query Group Impacts	21
3.7	Application Server Enterprise Migration Tool Impacts	21
3.8	External Authentication Impacts	21
3.9	Application Server Portal API Impacts	21
3.10	Network Server Location API Impacts	21
3.11	NSSync API Impacts.....	21
3.12	Application Server Dump Impacts	21

3.13	BroadCloud Dump Impacts.....	21
3.14	Service Details and Licensing.....	21
3.15	Service License Reporting Impact.....	21
3.16	Call Detail Server SOAP Interface.....	21
3.17	Treatments.....	21
3.18	Media Announcements (Audio and Video)	21
3.19	BroadWorks Common Communication Transport Impacts	21
3.20	Device Management Impacts	21
4	Accounting Impacts.....	22
4.1	Summary of Changes	22
4.2	Generation of Accounting Records	22
4.3	Impact to Accounting Fields (CDR)	22
4.4	Original Called Reason and Redirection Reason	22
4.5	Related Call ID	22
4.6	Example	22
5	System Management Impacts.....	23
5.1	Performance Management Impacts	23
5.2	Fault Management Impacts	23
5.3	Scripts and Tools	23
5.4	EMS Integration Impacts	23
6	Execution/Call Processing Impacts.....	24
6.1	CAP Interface Impact	24
6.2	Xtended Services Interface (Xsi) Impact.....	24
6.2.1	Summary.....	24
6.2.2	Xsi-Actions Impacts	24
6.2.3	Xsi-Events Impacts.....	24
6.2.4	Xsi-MMTel Impacts.....	24
6.2.5	Schema Impacts.....	24
6.3	SIP/MGCP Interface Impact	24
6.3.1	Summary.....	24
6.3.2	SIP Header/MGCP Command	24
6.3.3	SIP Parameter/MGCP Signal/Event.....	25
6.4	Service Interactions	26
6.4.1	Service Precedence	26
6.4.2	Service Interactions	26
7	Client Application Impacts	28
7.1	OCI-P/CAP Impacts	28
7.2	Call Control Impacts	28
7.3	Window Impacts	28
8	Deployment/Operational Impacts	29
8.1	Configuration File Impacts	29
8.2	Installation Impacts.....	29

8.3	Upgrade Impacts	29
8.4	Rollback Impacts	29
8.5	Security Impacts	29
8.6	Scheduled Tasks	29
8.7	Third-Party Software.....	29
8.8	Server Logging Impacts	29
8.9	Client Application Impacts.....	29
8.9.1	Deployment Studio Impacts.....	29
8.9.2	Configuration Impacts	29
8.9.3	Host Application Impacts.....	29
8.9.4	Third-Party Integration Impacts.....	29
9	System Engineering Impacts	30
9.1	Processing Impacts	30
9.1.1	New Time-Outs.....	30
9.1.2	New Threads	30
9.2	Memory Impacts	30
9.3	Disk Usage Impacts	30
9.4	Port Usage Impacts.....	30
9.5	Hardware Impacts	30
9.6	Client Application Messaging Impacts.....	30
10	Service Patch Information	31
11	Restrictions and Limitations	32
	Acronyms and Abbreviations	33
	References	37

1 Feature Overview and Purpose

Applicable Telephony Application Server (TAS)
Application Server (AS)

The Audio Security Classification for Trunk User Calls feature enhances the Security Classification service for the trunk group user by playing the audio security classification announcement to notify the trunk group users of the current security classification level of the call.

2 Detailed Feature Description

This feature enhances the existing Visual Security Classification for Active Call feature in the *Visual Security Classification for Active Call Feature Description* [1] to play an announcement stating the security classification level of the call to the trunk group users whose devices are not capable of displaying the security call classification.

In general, this feature does not change the security classification level functionality provided by the Visual Security Classification for Active Call feature, which includes the computation of the security classification of the call and when or whether the notification (via SIP INFO message) of the security classification of the call is sent to the call participants.

However, note that prior to this feature, the trunk group users whose devices did not support the display of security call classification were automatically given the *Unclassified* level as their current classification level overriding their assigned classification levels. With this feature, the trunk group user's assigned classification level is now used in computing the security classification of the call in which the trunk group user is involved.

This feature focuses on providing the audio security classification announcement to the trunk group users whose devices are not capable of displaying the security call classification. The audio security classification announcement is played in lieu of the visual security classification notification INFO message when the call is answered and whenever the security classification level is changed during the call. The security classification announcements played to the trunk group users are the existing audio files that were uploaded during the time that the security classification levels are configured in the system, as described in the *Visual Security Classification for Active Call Feature Description* [1].

The security classification announcement is provided in both audio and video calls.

The feature only applies to the trunk group users who are assigned the Security Classification service or who belong to a group that is authorized with the Security Classification service. These trunk group users' devices do not support the *security-class* Info Package defined in the *Visual Security Classification for Active Call Feature Description* [1].

New system parameter, *playTrunkUserSecurityClassificationAnnouncement*, described in section 3.1.1 *System Security Classification Parameters* is introduced to activate this feature. The feature is deactivated by default.

The following subsections provide information on how the feature behaves when it is invoked.

2.1 Two-Party Call

The Audio Security Classification for Trunk User Calls feature operates independently on the originating and terminating sides of the call.

When a trunk group user originates or receives a call, the security classification announcement is played to the trunk group user after the call is answered. If both call participants are trunk group users, two security classification announcements are played, one for each trunk group user.

When a trunk group user is connected to a media Interactive Voice Response (IVR) triggered by other services, if the media IVR is played locally, the security classification announcement is suppressed. However, if the media IVR is played remotely, the local security classification announcement and the remote IVR announcement are played concurrently to this trunk group user. If the trunk group user is reconnected from the local

media IVR connection to a different party, the security classification announcement is played to the trunk group user.

2.1.1 Security Classification Announcement Call Flow in Audio Call

This section shows a call flow example for playing the security classification announcement to the call terminator. The call flow is similar for the call originator.

The call flow shows that:

- 1) After the call is answered, both participants are reconnected through the Media Server connections and the announcement is only played to the terminator.
- 2) After the announcement is completed, both originating and terminating parties are reconnected directly.

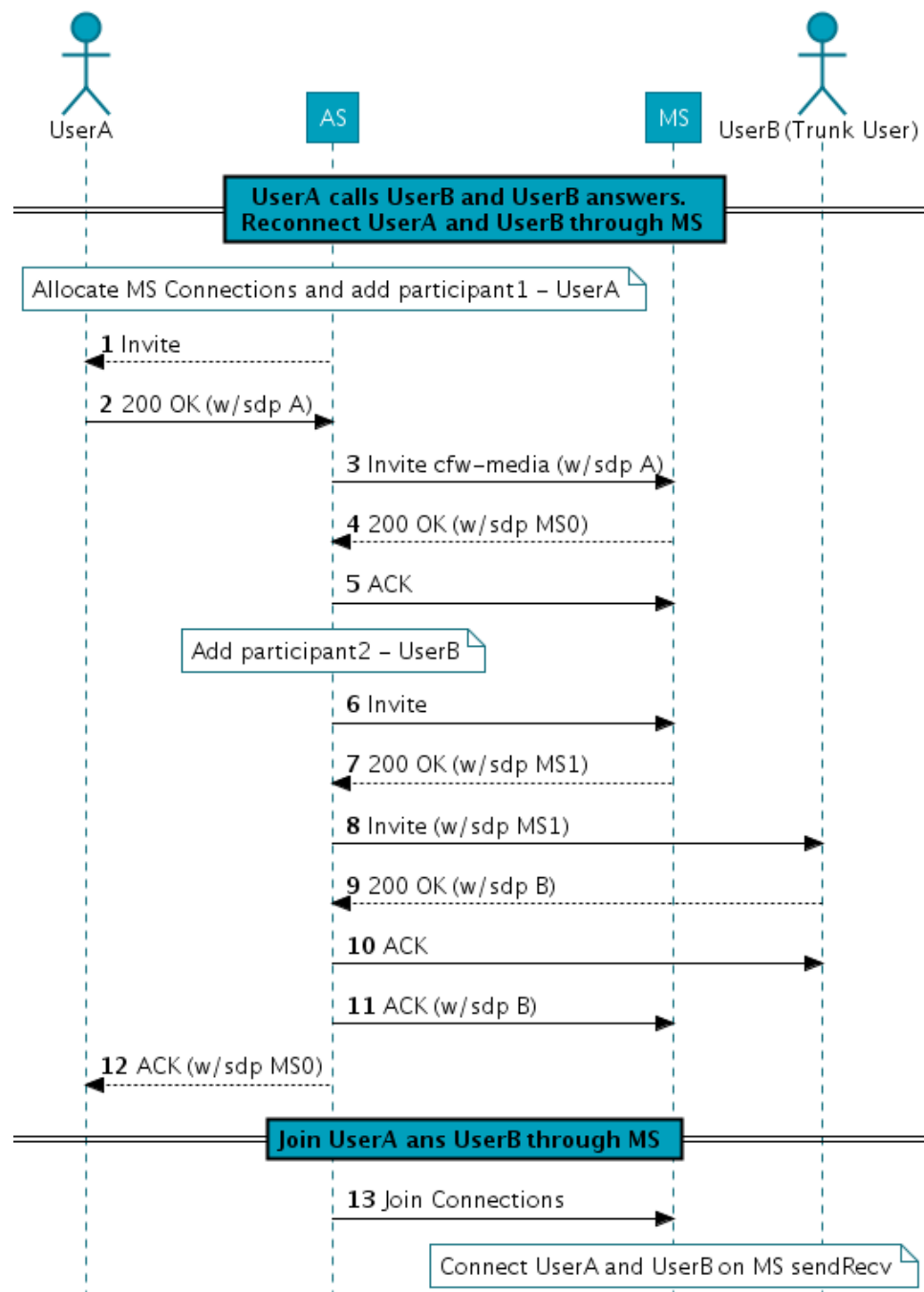


Figure 1 Call Flow for Playing Announcement in Audio Call (a) (audio call flow continues ...)

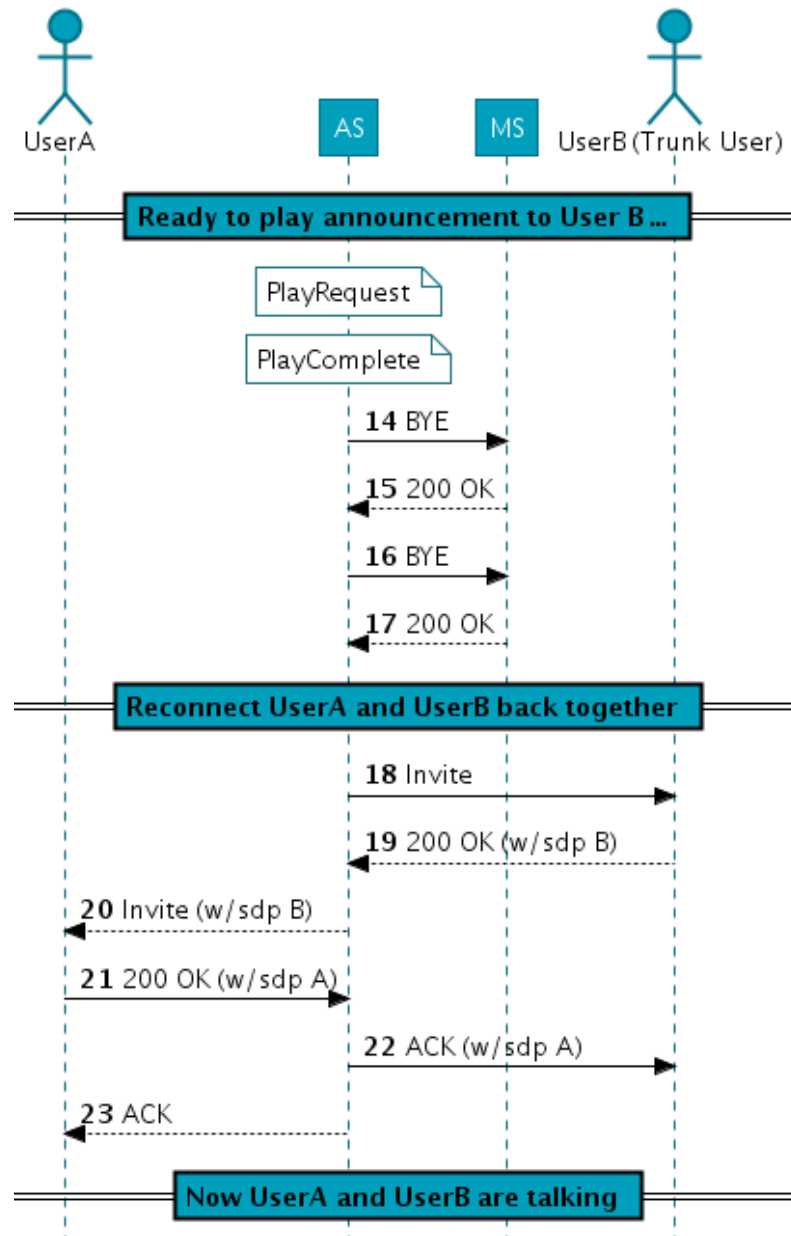


Figure 2 Call Flow for Playing Announcement in Audio Call (b) (... audio call flow continued)

2.1.2 Security Classification Announcement Call Flow in Video Call

The call flow is basically same as the one for audio call in section [2.1.1 Security Classification Announcement Call Flow in Audio Call](#), except that the video passthrough mechanism is used to set up the Media Server connections for playing the security classification announcement in the video call.

In the call flow:

- Each participant's video SDP is not passed to the Media Server.
- The SDP sent to each participant is manipulated by mixing the Media Server's audio SDP and the remote participant's video SDP.

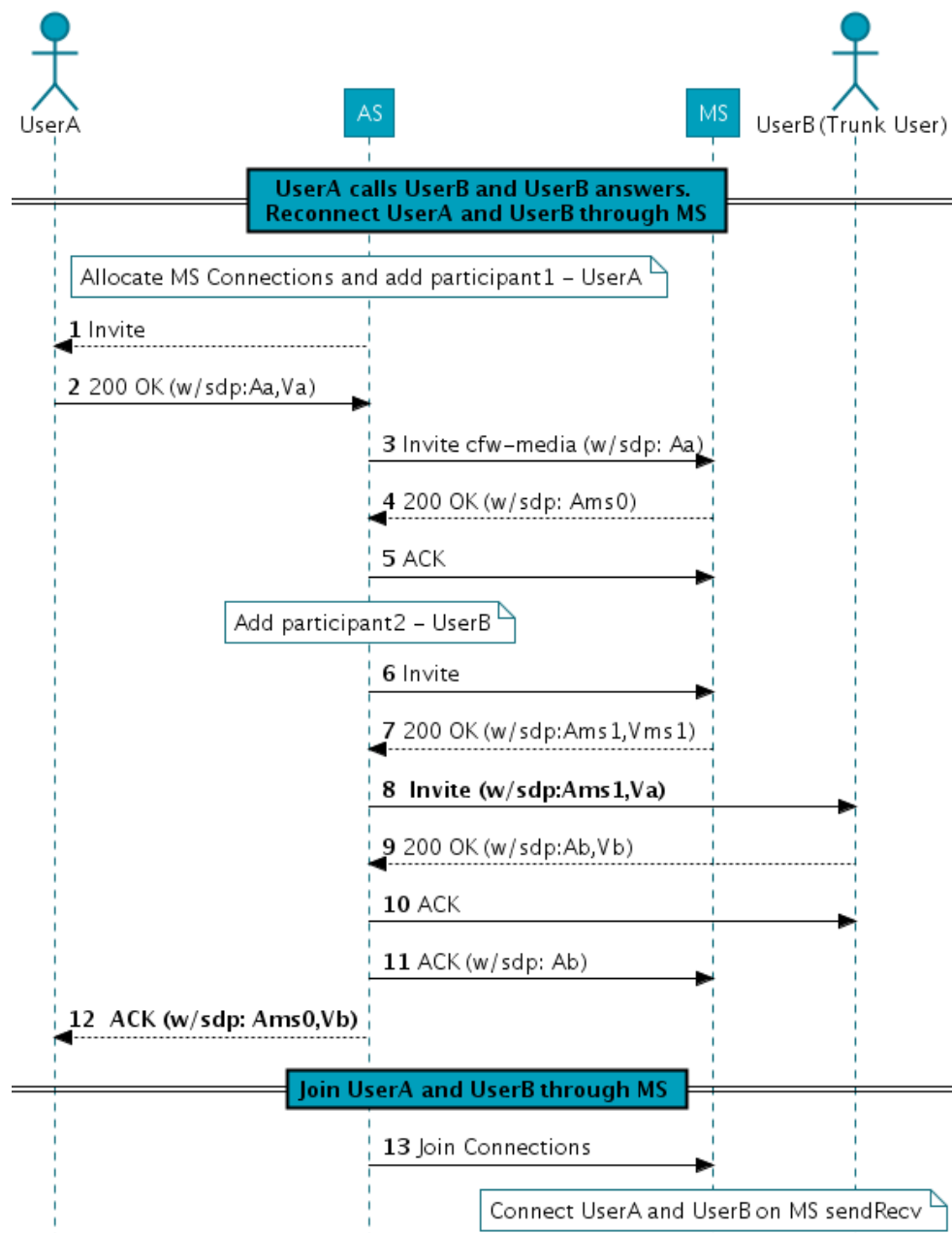


Figure 3 Call Flow for Playing Announcement in Video Call (a) (video call flow continues ...)

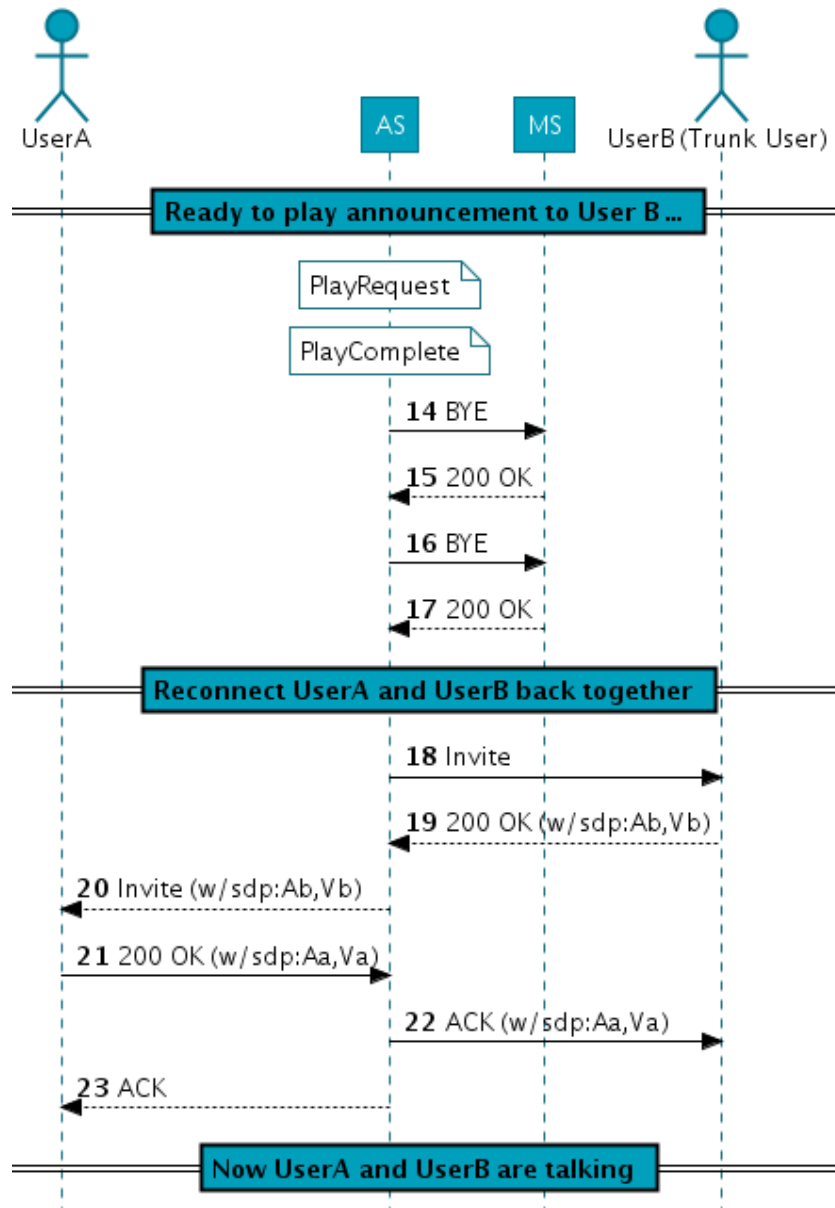


Figure 4 Call Flow for Playing Announcement in Video Call (b) (... video call flow continued)

2.2 Three-Way and N-Way Calls

When a trunk group user initiates a network conference, if the security classification level of the conference call is different from the level of the previous call, the security classification announcement is played by the conference service instance to the trunk group conference controller. Afterward, if the security classification level of the call is changed, the updated security classification announcement is played to the trunk group conference controller.

For a trunk group user participating in a conference that is controlled by a remote participant, this feature behaves as described in section [2.1 Two-Party Call](#).

2.3 Meet-Me Conference

When a trunk group user is connected to a Meet-Me conference within the enterprise, the audio security classification announcement introduced with this feature is suppressed since the Meet-Me Conference service described in the *Visual Security Classification for Active Call Feature Description* [1] already provides a security classification announcement to all users in the conference.

However, when a trunk group user is connected to a Meet-Me conference outside the enterprise, the trunk group user may hear two duplicated announcements concurrently, one from remote call half and played by the Meet-Me conference, another one from local call half and played by this feature.

2.4 Media Server Recovery

When a Media Server failure occurs while playing the security classification announcement, the trunk group user may hear an incomplete security classification announcement.

After the Media Server is recovered and back in service, the security classification announcement is played again to the trunk group user, whether or not the security classification level of the call is changed.

2.5 Execution Use Cases

In the use cases in the following subsections, it is assumed that all trunk group users are assigned the Security Classification service or belong to a group that is authorized with the Security Classification service and that the trunk group users' devices do not support the *security-class* Info Package.

2.5.1 Two-Party Audio Call with Two Trunk Group User

User A is a trunk group user and has the Security Classification service assigned with the security classification level set to "Top Secret".

User B is also a trunk group user who has the Security Classification service assigned with the security classification level set to "Secret".

- 1) User A calls User B and User B answers.
- 2) Both User A and User B hear the security classification announcement stating that the current call is *Secret*.

2.5.2 Two-Party Video Call with One Trunk Group User

User A is a trunk group user and has the Security Classification service assigned with the security classification level set to "Top Secret".

User B has the Security Classification service assigned and the security classification level is *Top Secret*.

Both User A's and User B's phone devices have the video enabled.

- 1) User A calls User B and User B answers. Both audio and video paths between User A and User B are connected.
- 2) User A hears the security classification announcement stating that the current call is *Top Secret*.

2.5.3 Mid-Call Security Classification Level Changed

User A is a trunk group user and has the Security Classification service assigned with the security classification level set to “Top Secret”.

User B has the Security Classification service assigned and the security classification level is *Top Secret*.

- 1) A call between User A and User B is established.
- 2) In mid-call, User A uses the Xsi-Actions to change the security classification level to *Unclassified*.
- 3) User A hears the security classification announcement stating that the current call is *Unclassified*.

2.5.4 Call Transfer

User A is a trunk group user and has the Security Classification service assigned with the security classification level set to “Top Secret”.

User B is also a trunk group user and has the Security Classification service assigned with the security classification level set to “Top Secret”.

User C does not have the Security Classification service assigned.

- 1) A call between User A and User B is established.
- 2) User B initiates a consultative transfer to User C.
- 3) When User C answers, User B hears the security classification announcement stating that the current call is *Unclassified*.
- 4) User B completes the call transfer and User A is connected to User C.
- 5) User A hears the security classification announcement stating that the current call is *Unclassified*.

2.5.5 N-Way Conference

User A is a trunk group user and has the Security Classification service assigned with the security classification level set to “Top Secret”.

User B is also a trunk group user and has the Security Classification service assigned with the security classification level set to “Top Secret”.

User C has the Security Classification service assigned with the security classification level set to “Secret”.

User D does not have the Security Classification service assigned.

- 1) User A is talking to User B. Both User A and User B have heard the security classification announcement stating that the current call is *Top Secret*.
- 2) User A puts User B on hold.
- 3) User A calls User C and User C answers.
- 4) Both User A and User C hear the security classification announcement stating that the current call is *Secret*.
- 5) User A uses the Call Manager client to establish a network conference among User A, User B, and User C.
- 6) The security classification level of the conference call is now *Secret*. Only User B hears the security classification announcement stating that the current call is *Secret*.

- 7) User A initiates another call to invite User D to the conference and User D answers.
- 8) User A hears the security classification announcement stating that the current call is *Unclassified*.
- 9) User A uses the Call Manager client to add User D to the conference bridge.
- 10) The security classification level of the conference call is now *Unclassified*. User B and User C hear the security classification announcement stating that the current call is *Unclassified*.
- 11) User D hangs up and leaves the conference.
- 12) All remaining, that is, User A, User B, and User C, hear the security classification announcement stating that the current call is *Secret*.

2.5.6 Meet-Me Call

User A is a trunk group user and has the Security Classification service assigned with the security classification level set to "Top Secret".

User B is also a trunk group user and has the Security Classification service assigned with the security classification level set to "Top Secret".

User C is a trunk group user and has the Security Classification service assigned with the security classification level set to "Top Secret".

User D does not have the Security Classification service assigned.

- 1) User A calls the Meet-Me conference and is connected to the Meet-Me greeting prompt asking User A to enter the conference ID.
- 2) User A hears the Meet-Me greeting prompts to enter a conference ID and the security classification announcement stating that the current call is *Unclassified* is played concurrently.
- 3) Now User A is connected to the Meet-Me conference bridge.
- 4) There is no security classification announcement played to User A since User A is the only participant of the Meet-Me conference.
- 5) User B calls the Meet-Me conference and User B hears the same announcement as User A in steps 1) and 2).
- 6) User B is added to the Meet-Me conference bridge and the security classification level of the Meet-Me conference is *Top Secret*.
- 7) Both User A and User B hear the security classification announcement stating that the current call is *Top Secret*.
- 8) User C dials seven digits (outside the enterprise dialing) to call the Meet-Me conference and User C hears the same announcement as User A in steps 1) and 2).
- 9) User C is added to the Meet-Me conference bridge and the security classification level of the Meet-Me conference is not changed.
- 10) User C hears two duplicate security classification announcements stating that the current call is *Top Secret*, which is played concurrently.
- 11) User D calls the Meet-Me conference and User D is prompted to enter the conference ID.
- 12) User D is added to the Meet-Me conference bridge and the security classification level of the Meet-Me conference is changed to *Unclassified*.

- 13) Both User A and User B hear one security classification announcement stating that the current call is *Unclassified*, while User C hears two duplicate security classification announcements stating that the current call is *Unclassified* (played concurrently).

2.5.7 Shared Call Appearance – Bridging

User A is a trunk group user who has the Security Classification service assigned and the security classification level is *Top Secret*.

User A is also assigned the Shared Call Appearance service and is configured with a Shared Call Appearance (SCA) location that supports the security classification display feature.

User B has the Security Classification service assigned and the security classification level is *Top Secret*.

- 1) User B calls User A and User A's SCA location answers.
- 2) The security classification level of the call is now *Top Secret*. However, there is no security classification announcement played to the SCA location because the SCA location is not a trunk group location.
- 3) From the primary location, User A dials feature access code (FAC) *15 to bridge with the SCA location.
- 4) User A's primary location is on the conference bridge with the SCA location.
- 5) Both User A's primary location and the SCA locations hear the security classification announcement stating that the current call is *Top Secret*.
- 6) User B uses the Xsi-Actions to change the security classification level to *Secret*.
- 7) The security classification level of the call is recomputed to *Secret*. The security classification announcement stating that the current call is *Secret* is played to the conference bridge between User A's primary location and the SCA locations. Both of User A's locations hear the announcement.

2.6 Provisioning Steps

To determine whether the trunk group user's security classification is played, set the *playTrunkUserSecurityClassificationAnnouncement* system-level parameter.

2.7 Client Interaction Use Cases

There is no impact.

3 Provisioning Impacts

3.1 Configuration Data

3.1.1 System Security Classification Parameters

Name	Field Type	Required?	Validation Values	Default Value
<i>playTrunkUserSecurityClassificationAnnouncement</i>	Boolean	Yes	true, false	false

3.2 Centralized Configuration Data

There is no impact.

3.3 Web Portal Impacts

3.3.1 General Description

A new configuration option is added to the *System → Security Classification* page. The *Play Trunk User Security Classification Announcement* check box indicates whether the security classification announcement is played.

3.3.2 Policy Impacts

There is no impact.

3.3.3 Web Pages

3.3.3.1 System Security Classification

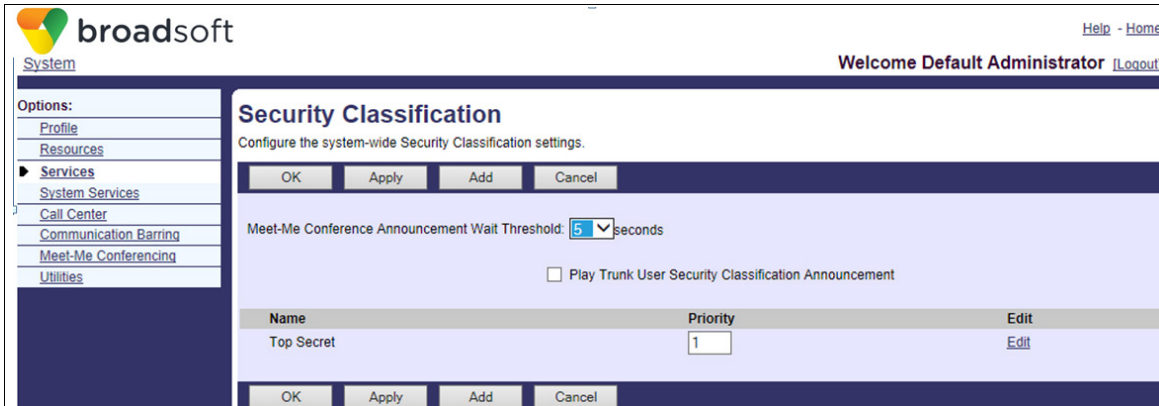


Figure 5 System Security Classification web page. New check box is added to enable/disable playing the trunk group user security classification announcement.

3.3.4 Help Pages

The help files in the following table are modified.

Level	Menu	Page Name (User Level)	User Type	Help Page Link
System	Services	<i>Security Classification</i>	SA	Help/en_US/SA/SASecurityClassifications.htm

3.4 CLI Impacts

There is no impact.

3.5 Open Client Interface-Provisioning (OCI-P) Impact

3.5.1 Summary

The following command has been added:

- SystemSecurityClassificationGetRequest21

The following command has been modified:

- SystemSecurityClassificationModifyRequest

The following command has been deprecated:

- SystemSecurityClassificationGetRequest

3.5.2 Command Impacts

3.5.2.1 SystemSecurityClassificationGetRequest21

Authorization level: System

XML Schema file: *OCISchemaServiceSecurityClassification.xsd*

```
<xs:complexType name="SystemSecurityClassificationGetRequest21">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <hssDataModeSupported>>false</hssDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Get the system Security Classification parameters.
      The response is either SystemSecurityClassificationGetResponse21 or
      ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SystemSecurityClassificationGetResponse21">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <hssDataModeSupported>>false</hssDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Response to the SystemSecurityClassificationGetRequest21.
      Contains a table with column headings:
```

```

        "Name", "Priority".
    </xs:documentation>
</xs:annotation>
<xs:complexContent>
    <xs:extension base="core:OCIDataResponse">
        <xs:sequence>
            <xs:element name="meetMeAnncThreshold"
type="SecurityClassificationMeetMeConferenceAnnouncementThresholdSeconds"/>
            <xs:element name="playTrunkUserSecurityClassificationAnnouncement"
type="xs:boolean"/>
            <xs:element name="SecurityClassificationTable" type="core:OCITable"/>
        </xs:sequence>
    </xs:extension>
</xs:complexContent>
</xs:complexType>

```

3.5.2.2 SystemSecurityClassificationModifyRequest

Authorization level: System

XML Schema file: *OCISchemaServiceSecurityClassification.xsd*

```

<xs:complexType name="SystemSecurityClassificationModifyRequest">
    <xs:annotation>
        <xs:appinfo>
            <asDataModeSupported>true</asDataModeSupported>
            <hssDataModeSupported>false</hssDataModeSupported>
        </xs:appinfo>
        <xs:documentation>
            Modify security classification parameters.
            The response is either a SuccessResponse or an ErrorResponse.
            NOTE: The security classifications must be specified in order of priority.
            The command fails if all the security classifications defined for the system are
            not provided.
        </xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="core:OCIRequest">
            <xs:sequence>
                <xs:element name="meetMeAnncThreshold"
type="SecurityClassificationMeetMeConferenceAnnouncementThresholdSeconds"
minOccurs="0"/>
                <xs:element name="playTrunkUserSecurityClassificationAnnouncement"
type="xs:boolean" minOccurs="0"/>
                <xs:element name="securityClassificationName"
type="SecurityClassificationName" minOccurs="0" maxOccurs="20"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>

```

3.5.3 Deprecated Commands

Command:	SystemSecurityClassificationGetRequest
Replaced By:	SystemSecurityClassificationGetRequest21
Behavior Impacts:	None

3.5.4 Reporting Impacts

There is no impact.

3.6 Application Server Query User/Query Group Impacts

There is no impact.

3.7 Application Server Enterprise Migration Tool Impacts

There is no impact.

3.8 External Authentication Impacts

There is no impact.

3.9 Application Server Portal API Impacts

There is no impact.

3.10 Network Server Location API Impacts

There is no impact.

3.11 NSSync API Impacts

There is no impact.

3.12 Application Server Dump Impacts

There is no impact.

3.13 BroadCloud Dump Impacts

There is no impact.

3.14 Service Details and Licensing

There is no impact. This feature enhances the existing Security Classification service.

3.15 Service License Reporting Impact

There is no impact.

3.16 Call Detail Server SOAP Interface

There is no impact.

3.17 Treatments

There is no impact.

3.18 Media Announcements (Audio and Video)

There is no impact.

3.19 BroadWorks Common Communication Transport Impacts

There is no impact.

3.20 Device Management Impacts

There is no impact.

4 Accounting Impacts

4.1 Summary of Changes

There is no impact.

4.2 Generation of Accounting Records

There is no impact.

4.3 Impact to Accounting Fields (CDR)

There is no impact.

4.4 Original Called Reason and Redirection Reason

There is no impact.

4.5 Related Call ID

There is no impact.

4.6 Example

There is no example.

5 System Management Impacts

5.1 Performance Management Impacts

There is no impact.

5.2 Fault Management Impacts

There is no impact.

5.3 Scripts and Tools

There is no impact.

5.4 EMS Integration Impacts

There is no impact.

6 Execution/Call Processing Impacts

6.1 CAP Interface Impact

There is no impact.

6.2 Xtended Services Interface (Xsi) Impact

6.2.1 Summary

There is no impact.

6.2.2 Xsi-Actions Impacts

There is no impact.

6.2.3 Xsi-Events Impacts

There is no impact.

6.2.4 Xsi-MMTel Impacts

There is no impact.

6.2.5 Schema Impacts

There is no impact.

6.3 SIP/MGCP Interface Impact

6.3.1 Summary

To avoid the glare conditions when both call halves are playing the audio security announcements at the same time, a new parameter, *sc-audio*, is introduced in the *X-BroadWorks-DNC* header to pass the local user's audio security capability to the remote party and avoid glare conditions as much as possible.

6.3.2 SIP Header/MGCP Command

X-BroadWorks-DNC header

DNC Header Parameter	Parameter Description
<i>sc-audio</i>	The user has the audio security capability enabled.

The new *sc-audio* parameter is passed along with another security parameter, *sc-user-class*, in the *X-BroadWorks-DNC* header when the user is a trunk group user and the audio security classification feature is enabled.

The terminator's call (half) receives the originator's audio security capability in the *sc-audio* parameter of the *X-BroadWorks-DNC* header (from the INVITE request message).

The terminator's audio security capability is forwarded to the originator's Application Server in the *sc-audio* parameter of the *X-BroadWorks-DNC* header (in the 200 OK response message).

The *sc-audio* parameter may be included in the 180 response and UPDATE request messages when the local user security classification information is forwarded to the remote party.

6.3.3 SIP Parameter/MGCP Signal/Event

The syntax of the new *X-BroadWorks-DNC sc-audio* parameter appears as follows.

```
X-BroadWorks-DNC = "X-BroadWorks-DNC" HCOLON (quoted-string SEMI enc
*(SEMI non-encrypted-dnc-param)) / *(SEMI dnc-param)
dnc-param = actual-identity | actual-privacy | colp-network-address |
network-address | redirection-reason | user-id | sc-userclass | sc-audio-
param | generic-param |
sc-audio-param = "sc-audio"
```

6.3.3.1 INVITE Between Peer Application Servers

The following message shows an INVITE between Application Servers. The originator's audio security capability is provided to the remote server in the *Distributed Network Call (DNC)* header.

```
INVITE sip:+19726981511@10.16.122.5:5060;user=phone SIP/2.0
Via:SIP/2.0/UDP 10.16.122.4;branch=z9hG4bKBroadWorks.16sknct-
10.16.122.5V5060-0-761705493-1015498782-1360880560168-
From:"Norma
South"<sip:9726981527@norma.rtx.broadsoft.com;user=phone>;tag=1015498782-
1360880560168-
To:<sip:+19726981511@10.16.122.5:5060;user=phone>
Call-ID:BW162240168140213-1143140263@10.16.122.4
CSeq:761705493 INVITE
Contact:<sip:10.16.122.4:5060>
P-Asserted-Identity:"Norma
South"<sip:9726981527@norma.rtx.broadsoft.com;user=phone>
Privacy:none
Allow:ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
X-BroadWorks-DNC:network-
address="sip:+19726981527@norma.rtx.broadsoft.com;user=phone";user-
id="south27@norma.rtx.broadsoft.com";sc-user-class="Top Secret";sc-audio
Accept:application/media_control+xml,application/sdp,application/x-
broadworks-call-center+xml,multipart/mixed
Supported:
Max-Forwards:10
Content-Type:application/sdp
Content-Length:211

v=0
o=BroadWorks 19 1 IN IP4 10.16.122.4
s=-
c=IN IP4 10.16.122.4
b=AS:1638
t=0 0
m=audio 5064 RTP/AVP 107 0 8 101
a=rtpmap:107 BV32/16000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

6.3.3.2 200 OK Between Application Servers

The following message shows the 200 OK response sent between Application Servers. The terminator's audio security capability is provided to the remote server in the *DNC* header.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.16.122.4;branch=z9hG4bKBroadWorks.16sknct-
10.16.122.5V5060-0-761705493-1015498782-1360880560168-
From: "Norma
South"<sip:9726981527@norma.rtx.broadsoft.com;user=phone>;tag=1015498782-
1360880560168-
To:<sip:+19726981511@10.16.122.5:5060;user=phone>;tag=716410562-
1360880560266
Call-ID: BW162240168140213-1143140263@10.16.122.4
CSeq: 761705493 INVITE
Supported:
Contact:<sip:10.16.122.5:5060>
X-BroadWorks-DNC: network-
address="sip:+19726981511@10.16.122.5;user=phone";user-
id="southmm@norma.rtx.broadsoft.com";sc-user-class="Secret";sc-audio
P-Asserted-Identity: "Meetme South"<sip:9726981511@10.16.122.5;user=phone>
Privacy: none
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
Accept: application/media_control+xml, application/sdp, application/x-
broadworks-call-center+xml, multipart/mixed
Content-Type: application/sdp
Content-Length: 194

v=0
o=BroadWorks 54 1 IN IP4 10.16.120.22
s=-
c=IN IP4 10.16.120.22
t=0 0
m=audio 12524 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

6.4 Service Interactions

6.4.1 Service Precedence

The Audio Security Classification service precedence is right after the Call Recording service for the terminating call half and it is after the Call Recording service and between the Emergency Call Timer service and the Call Forward Interrogation Feature Access Code service for the originating call half.

6.4.2 Service Interactions

In this section it is assumed that all trunk group users are assigned the Security Classification service or belong to a group that has the Security Classification service authorized. It is also assumed that the trunk group users' devices do not support the *security-class* Info Package.

6.4.2.1 Answer Confirmation

The security classification announcement is played to the trunk group users after the Answer Confirmation service accepts the call.

6.4.2.2 Call Recording

This feature reuses the media conference created by the Call Recording service to play the security classification announcement.

The security classification announcement and the call recording started announcement are played one after another to the trunk group user when the call is initially established, if the Call Recording service is enabled with the *Always* mode and the *Play Call Recording Start/Stop Announcement* option is enabled. The security classification announcement is played only to the local participant, except when the call recording is in the single-mode video, in which case the security classification announcement is played to both participants.

After the call is established, if the trunk group user changes their security classification level via Xsi-Actions or SIP interface, the security classification announcement is played to the trunk group user stating the updated classification level of the call.

6.4.2.3 Call Bridge

When the call bridge function is invoked, the security classification announcement is played to the bridge if there is any trunk group user location in the bridge. All locations bridged in the call hear the announcement.

6.4.2.4 Call Retrieve

When a trunk group user's primary location invokes the call retrieve function to retrieve the call on the secondary location, the security classification announcement is played to the trunk group user's primary location.

When a trunk group user's secondary location invokes the call retrieve function to retrieve the call on the primary location or other secondary location, the security classification announcement is not played if this secondary location is not a trunk group user.

6.4.2.5 Conference

For information, see section [2.2 Three-Way and N-Way Calls](#).

6.4.2.6 DTMF Transmission

This feature reuses the media conference created by the DTMF Transmission service to play the security classification announcement.

When a trunk group user actively connected on a call invokes an Xsi-Actions to send DTMF digits and when the trunk group user changes their security classification level while the DTMF digits are played, the security classification announcement is played to the trunk group user.

6.4.2.7 Push To Talk

This feature reuses the media conference created by the Push To Talk (PTT) service to play the security classification announcement.

In a Push To Talk call originating from or terminating to a trunk group user, the security classification announcement is played to the trunk group user after the call is answered.

7 Client Application Impacts

7.1 OCI-P/CAP Impacts

There is no impact.

7.2 Call Control Impacts

There is no impact.

7.3 Window Impacts

There is no impact.

8 Deployment/Operational Impacts

8.1 Configuration File Impacts

There is no impact.

8.2 Installation Impacts

The system security classification parameter defined in section [3.1.1 System Security Classification Parameters](#) is added with the default value.

8.3 Upgrade Impacts

On Application Server upgrade, the system security classification parameter defined in section [3.1.1 System Security Classification Parameters](#) is added with the default value.

8.4 Rollback Impacts

On Application Server rollback, the system security classification parameter defined in section [3.1.1 System Security Classification Parameters](#) is removed.

8.5 Security Impacts

There is no impact.

8.6 Scheduled Tasks

There is no impact.

8.7 Third-Party Software

There is no impact.

8.8 Server Logging Impacts

There is no impact.

8.9 Client Application Impacts

8.9.1 Deployment Studio Impacts

There is no impact.

8.9.2 Configuration Impacts

There is no impact.

8.9.3 Host Application Impacts

There is no impact.

8.9.4 Third-Party Integration Impacts

There is no impact.

9 System Engineering Impacts

9.1 Processing Impacts

When this feature is invoked, it creates the Media Server connections to play the security classification announcement to the trunk group user and reconnects the trunk group user back to the remote party after the announcement is completed. There are about 23 SIP messages exchanged between the Application Server, the Media Server, and the endpoint devices.

9.1.1 New Time-Outs

There is no impact.

9.1.2 New Threads

There is no impact.

9.2 Memory Impacts

There is no impact.

9.3 Disk Usage Impacts

There is no impact.

9.4 Port Usage Impacts

Two media ports are used to play the security classification announcement to a trunk group user.

9.5 Hardware Impacts

There is no impact.

9.6 Client Application Messaging Impacts

There is no impact.

10 Service Patch Information

This feature is not patched.

11 Restrictions and Limitations

There is no limitation.

Acronyms and Abbreviations

This section lists the acronyms and abbreviations found in this document. The acronyms and abbreviations are listed in alphabetical order along with their meanings.

AAC	Account/Authorization Code
ABNF	Augmented Backus-Naur Form
ACC	Advanced Call Control
ACD	Automatic Call Distribution
ACL	Access Control List
ACR	Anonymous Call Rejection
Admin	Administrator
AMS	Access Mediation Server
API	Application Programming Interface
AS	Application Server
AVP	Attribute Value Pair
BCCT	BroadWorks Common Communication Transport
BLF	Busy Lamp Field
BW	BroadWorks
CAP	Client Application Protocol
CBF	Communication Barring – Fixed
CCRS	Call Center Reporting Server
CDR	Call Detail Record
CDS	Call Detail Server
CFA	Call Forwarding Always
CFB	Call Forwarding Busy
CFNA	Call Forwarding No Answer
CFNR	Call Forwarding Not Reachable
CFS	Call Forwarding Selective
CLI	Command Line Interface
CLID	Calling Line ID
CNAM	Caller ID with NAME
CORBA	Common Object Request Broker Architecture
CPL	Call Processing Language
CPU	Central Processing Unit
CRS	Call Recording Server
CS	Conferencing Server

CSCF	Call Session Control Function
CSTA	Computer Supported Telecommunications Applications
CSV	Comma Separated Value
CTI	Computer Telephony Integration
CWT	Call Waiting Tone
dBm	The power ratio in decibel (dB) of the measured power referenced to one milliwatt (mW).
dBm0	The level of a signal as specified in dBm0, is the level of that signal (in dBm) as measured at the reference point of the network.
DBS	Database Server
DGC	Distributed Group Calls
DN	Directory Number
DNC	Distributed Network Calls
DND	Do Not Disturb
DPUBI	Directed Call Pickup with Barge-in
DTMF	Dual-Tone Multi-Frequency
EMS	Element Management System
EOCP	Enhanced Outgoing Calling Plan
EV	ExtraView
FAC	Feature Access Code
FD	Feature Description
FQDN	Fully Qualified Domain Name
FR	Feature Request
FS	Functional Specification
FTP	File Transfer Protocol
HCB	Hierarchical Communication Barring
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
Hz	Hertz
ICP	Incoming Calling Plan
IMAP	Internet Message Access Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IVR	Interactive Voice Response
LI	Lawful Intercept
LO	Local
LPS	Local Premium Service

LSSGR	LATA Switching Systems Generic Requirements
MB	Megabyte
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MOC	Microsoft Office Communications
MR	Market Request
MS	Media Server
NCOS	Network Class of Service
NE	Network Element
NS	Network Server
NSSync	Network Server Synchronization
OAM&P	Operations, Administration, Management, and Provisioning
OCI	Open Client Interface
OCI-C	Open Client Interface-Call Control
OCI-P	Open Client Interface-Provisioning
OCI-R	Open Client Interface-Reporting
OCP	Outgoing Calling Plan
OCS	Open Client Server
ODP	Outgoing Digit Plan
OID	Object Identifier
OOTB	Out-of-the-Blue
OS	Operating System
OSS	Operations Support System
PBX	Private Branch Exchange
PCV	P-Charging-Vector
PDF	Portable Document Format
PM	Performance Measurement
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
PTT	Push To Talk
PUI	Public User Identity
RAM	Random Access Memory
RFC	Request for Comments
RTP	Real-Time Transport Protocol
SAC	Session Admission Control
SBC	Session Border Controller

SCA	Shared Call Appearance
SCA	Selective Call Acceptance
SCR	Selective Call Rejection
SDR	Session Data Replication
SIP	Session Initiation Protocol
SMAP	Software Management Application Protocol
SMDI	Simplified Message Desk Interface
SMPP	Short Message Peer-to-Peer Protocol
SMS-C	Short Message Service Center
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SP	Service Patch
SRV	Service Locator
SSH	Secure Shell
TAS	Telephony Application Server
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TO	Toll
TPS	Toll Premium Services
TXNS	Transactions
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VMS	Voice Mail System
VoIP	Voice Over Internet Protocol
WebDAV	Web-based Distributed Authoring and Versioning
WS	Web Server
XML	eXtensible Markup Language
XS	Execution Server
XSD	XML Schema Definition
Xsi	Xtended Services Interface
Xsp	Xtended Services Platform

References

- [1] BroadSoft, Inc. 2014. *Visual Security Classification for Active Call Feature Description, Release 20.0*. Available from BroadSoft at xchange.broadsoft.com.