broadsoft

broadsoft broadworks

# Application Server

## Identity Guide

Release 21.0

Document Version 1

9737 Washingtonian Boulevard, Suite 350
Gaithersburg, MD 20878
Tel +1 301.977.9440

WWW.BROADSOFT.COM

# BroadSoft® Guide

## Copyright 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

| Release | Version | Reason for Change | Date | Author |
|---|---|---|---|---|
| 21.0 | 1 | Created document. | September 28, 2015 | Michael Boyle |
| 21.0 | 1 | Edited document. | October 9, 2015 | Joan Renaud |
| 21.0 | 1 | Made changes following review. | November 3, 2015 | Rod Hughes |
| 21.0 | 1 | Edited changes. | November 6, 2015 | Joan Renaud |
| 21.0 | 1 | Removed content that does not apply to this release. | November 10, 2015 | Rod Hughes |
| 21.0 | 1 | Edited changes and published document. | November 11, 2015 | Joan Renaud |

## Table of Contents

# 1 Summary of Changes

This section describes the changes to this document for each release and document version.

## 1.1 Changes for Release 21.0, Document Version 1

This document was created for Release 21.0.

# 2 Introduction

This document provides an overview of the identity-related configuration and handling on the Application Server.

Although this document is relevant to both trunking and non-trunking scenarios, Session Initiation Protocol (SIP) trunking has highly specialized identity handling that is not covered in this document. For the SIP trunking-specific identity-related configuration and handling, see the *BroadWorks SIP Trunking Solution Guide* [14].

# 3 Identity Types

There are a few different types of identities that are processed by the Application Server. The following subsections define these different identity types.

Note that all the identity types allow for both a name and an address, and for all the name is optional but the address is mandatory.

## 3.1 Presentation Identity

The presentation identity is an identity that is intended to be displayed on the receiving party's devices (such as a SIP device) and applications (such as an Xsi application). Unlike the asserted identity (see section *3.2 Asserted Identity)*, the presentation identity is not intended to always be a trusted, network-provided identity and can be user provided instead.

The presentation identity provides the receiving party with the remote party's name and address information, and allows the receiving party to identify who they are connected to. In addition, the presentation identity is used by many subscriber services such as Basic Call Logs, Enhanced Call Logs, Selective Call Rejection, and Voice Messaging.

For a BroadWorks subscriber, their presentation identity can be provided by various sources depending on the type of call and the subscriber's configuration. For example, the address may be an extension for group calls but a DN for external calls, and the name may be the subscriber's own name or a different value such as the group's name.

For a BroadWorks subscriber, their presentation identity is always considered available. For an external party, the presentation identity received, used, and sent by the Application Server for the party may be considered available or unavailable. Some subscriber screening services such as Selective Call Rejection have a setting to trigger when the presentation identity is unavailable. For details on how the Application Server detects and handles an unavailable presentation identity, see the *BroadWorks SIP Network Interface Interworking Guide* [3].

There are two different types of presentation identities. These are the calling identity and the connected identity.

### 3.1.1 Calling Identity

The calling identity is the presentation identity of the originating party that is provided to the terminating party at the start of the call.

### 3.1.2 Connected Identity

The connected identity is the presentation identity of the remote party that is provided to the receiving party in every scenario except the calling identity. For example, the presentation identity of the terminating party that is provided to the originating party is a connected identity, and any presentation identity that is provided to the terminating party after the start of the call is a connected identity.

## 3.2 Asserted Identity

The asserted identity is intended to be a trusted, network-provided identity. The asserted identity is only sent to trusted locations and is used by administrator services such as Communication Barring – Fixed, Hierarchical Communication Barring, and Outgoing Call Plan. The asserted identity is also used by many subscriber screening services such a Selective Call Rejection when the remote party is a known subscriber in the same group/enterprise.

For a BroadWorks subscriber, their asserted identity's address is always an E.164 number and may be either a DN for the subscriber or the group CLID for the subscriber's group. Their asserted identity's name is always the same as their presentation identity's name for external calls.

## 3.3 Redirecting Identity

The redirecting identity is the identity used by a party when a redirection (a call forwarding for example) occurs. The redirecting identity may be received by the Application Server for redirections that happened prior to the Application Server receiving the call, or may be added by the Application Server when the Application Server triggers a redirection.

For a BroadWorks subscriber, their redirecting identity is generally the same as their presentation identity for external calls and hence the redirecting identity's address is normally an E.164 number such as a DN.

## 3.4 Charge Identity

The charge identity is a trusted identity provided by the Application Server via the Charge Number service and is only sent on the SIP network interface.

The charge identity address for a BroadWorks subscriber is the charge number set via their Charge Number service. The charge identity name for a BroadWorks subscriber is always the same as their normal presentation identity name for external calls.

# 4 Privacy

Privacy can be indicated for the presentation identity, asserted identity, and redirecting identity in the incoming and outgoing messaging on the Application Server. Privacy is not normally indicated for the charge identity sent by the Application Server, but is when the charge identity is being sent via the *P-Asserted-Identity* header or the *Diversion* header per the SIP *chargeHeaderFormat* system parameter (see section *9 SIP System Parameters*).

For a BroadWorks subscriber, privacy can also be enabled or disabled via the Calling Line ID Delivery Blocking service for CLIR and the Connected Line Identification Restriction service for COLR.

For each party involved in a call on BroadWorks, there is a single privacy value in effect for the party that applies to both their presentation identity and asserted identity for the call. This privacy value impacts how BroadWorks services function. For example, Basic Call Logs and Enhanced Call Logs apply the privacy for the party to their presentation identity captured in the call logs, and some subscriber screening services such as Selective Call Rejection have a setting to trigger when privacy is in effect.

When a presentation identity or redirecting identity is sent to a non-trusted location, privacy is always applied to the identity as applicable.

When a calling identity is sent to a trusted location in an initial INVITE, privacy is only applied to the *From* header and only if the SIP *encryptFromHeader* system parameter is enabled (see section *9 SIP System Parameters*). Privacy is not applied to the connected identity, asserted identity, or redirecting identity sent to a trusted location.

For full details on SIP privacy handling, see the *BroadWorks SIP Network Interface Interworking Guide* [3] and the *BroadWorks SIP Access Interface Interworking Guide* [4].

# 5 Profile Identity Configuration

The group, department, and subscriber profile configuration on the Application Server contain various identity-related fields. The following subsections list the main identity-related fields in each of these profile types. For full details on these fields and their configuration, see the *BroadWorks Application Server Group Web Interface Administration Guide - Part 1* [6], the *BroadWorks Application Server Group Web Interface Administration Guide - Part 2* [7], and the *BroadWorks User Web Interface Administration Guide* [8].

## 5.1 Group Profile Identity Configuration

- Group Name – The Unicode name for the group.
- Calling Line ID Group Name – The ASCII name for the group.
- Calling Line ID Group Number – The group CLID for the group.
- Location Dialing Code.

## 5.2 Department Profile Identity Configuration

- Department Name – The Unicode name for the department.
- Department Calling Line ID Name – The ASCII name for the department.
- Department Calling Line ID Number – The department CLID for the department.

## 5.3 Subscriber Profile Identity Configuration

- Last Name – The Unicode last name for the subscriber.
- First Name – The Unicode first name for the subscriber.
- Calling Line ID Last Name – The ASCII last name for the subscriber.
- Calling Line ID First Name – The ASCII first name for the subscriber.
- Calling Line ID Phone Number – The configurable CLID for the subscriber.
- Phone Number – The primary DN for the subscriber.
- Extension – The primary extension for the subscriber.

# 6 Call Processing Policies

The Application Server provides many call processing policies that can be applied to subscribers. The call processing policies are grouped into functional categories and can be associated to a subscriber in either a hierarchical manner or via a Call Processing Policy Profile associated with the subscriber's Network Class of Service (NCOS).

The following subsections list the call processing policies in each category that are relevant to identity handling. For full details on the call processing policies and their configuration, see the *BroadWorks Call Processing Policies Guide* [1].

## 6.1 Calling Line ID Category

- Use group name for Calling Line Identity
- Allow Department Name Override
- External Calls
- Enterprise Calls
- Enterprise Group Calls
- Service Provider Group Calls
- Emergency Calls
- Allow Alternate Numbers for Redirecting Identity
- Allow Configurable CLID for Redirecting Identity
- Block Calling Name for External Calls

## 6.2 Translation and Routing Category

- Enforce Group Calling Line Identity Restriction
- Enforce Enterprise Calling Line Identity Restriction
- Override CLID Restriction For Private Call Category
- Use Enterprise CLID For Private Call Category

## 6.3 Dialable Caller ID Category

- Dialable Caller ID

# 7 Call Policies

In addition to the call processing policies listed in section *6 Call Processing Policies*, the Application Server provides a few call policies at the subscriber level. These call policies are separate from the call processing policies and are only configured at the subscriber level.

The following call policies are relevant to identity handling. For full details on the call policies and their configuration, see the *BroadWorks Call Processing Policies Guide* [1].

- Connected Line Identification Privacy on Redirected Calls
- Calling Line Identity for Redirected Calls

# 8 Services

The Application Server provides many services that can impact the identity information for a call. These include both services that can be assigned to a subscriber and virtual subscriber services.

The following services have identity-related interactions and hence are relevant to identity handling. For further details on these services and how they impact identity handling, see the *BroadWorks Service Guide* [10], the *BroadWorks Service Interaction Guide* [11], the solution guide for the service as referred to in the following list, and/or the Functional Description document for the service.

Note that the Dialable Caller ID and Phone List Lookup functionalities are similar to services but are controlled via call processing policies as described in section *6.3 Dialable Caller ID Category*.

- Alternate Numbers
- BroadWorks Anywhere – The only interaction is with the presentation identity for emergency calls from a BroadWorks Anywhere location.
- BroadWorks Mobility – See the *BroadWorks Mobility Guide* [16].
- Call Center – See the *BroadWorks Call Center Solution Guide* [15].
- Call Park – The only interactions are with the presentation identity for Call Park notifications and for Call Park Recall.
- Call Waiting – The only interaction is the presentation identity provided via SIP INFO to non-intelligent devices for Call Waiting calls.
- Calling Line ID Delivery Blocking – The CLIR service on the Application Server.
- Calling Line ID Blocking Override
- Calling Name Delivery – A CLIP service on the Application Server that only controls name delivery.
- Calling Name Retrieval
- Calling Number Delivery – A CLIP service on the Application Server that only controls number delivery.
- Charge Number
- City-Wide Centrex
- Connected Line Identification Presentation – The COLP service on the Application Server.
- Connected Line Identification Restriction – The COLR service on the Application Server.
- Executive
- External Calling Line ID Delivery – A CLIP service on the Application Server that controls name and number delivery for external calls.
- Flexible Seating Guest – The only interaction is with the presentation identity for emergency calls from a Flexible Seating Guest location.
- Group Paging
- Hoteling Guest – The only interaction is with the presentation identity for emergency calls from a Hoteling Guest location.

- Hunt Group
- Internal Calling Line ID Delivery – A CLIP service on the Application Server that controls name and number delivery for internal calls.
- Remote Office – The only interaction is with the presentation identity for emergency calls from a Remote Office location.
- Route List
- Route Point
- Trunk Group – See the *BroadWorks SIP Trunking Solution Guide* [14].
- Virtual On-Net Enterprise Extensions

# 9 SIP System Parameters

The Application Server provides many SIP system parameters that are used to configure how the SIP interface functions.

The following SIP system parameters found under the *Interfaces/SIP* level of the Application Server command line interface (CLI) are the main parameters relevant to identity handling. For full details on these SIP system parameters and their configuration, see the *BroadWorks Application Server Command Line Interface Administration Guide* [2], the *BroadWorks SIP Network Interface Interworking Guide* [3], and the *BroadWorks SIP Access Interface Interworking Guide* [4].

- encryptFromHeader
- useDomainForSubscriberAddress
- sendE164
- privacyVersion
- privacyEnforceScreening
- privateDialPlanOriginatorUsesExtension
- restrictedDisplayName
- callingPartyE164Normalization
- supportRFC3966PhoneContext
- includePrivacyUser
- useHistoryInfoHeaderOnNetworkSide
- chargeHeaderFormat
- sendCallerNameInfoForNetworkCalls
- disabledCLIDNumberValue
- networkSendIdentityInUpdateAndReInvite
- networkReceiveIdentityInUpdateAndReInvite
- enableTS29163Compliance
- redirectingAssertedIdentityPolicy
- useAssertedIdentityForPrivateCLID
- supportPrivacyNone
- redirectionHeaderPriority
- disableCOLPForRFC3323
- treatUnknownDisplayNameAsUnavailable
- includeHistoryInfoInResponse

# 10 Identity System Parameters and Other System-Level Configuration

In addition to the SIP system parameters listed in section *9 SIP System Parameters* and the system parameters associated with the call processing policies (see section *6 Call Processing Policies*), there are other identity-related system parameters on the Application Server.

The following system parameters are the main other system parameters relevant to identity handling. These system parameters are prefixed by their level under the Application Server CLI. For full details on these system parameters and their configuration, see the *BroadWorks Application Server Command Line Interface Administration Guide* [2].

- *Service/COLP/enforceUserServiceAssignment*
- *Service/SelectiveServices/screenPrivateNumber*
- *SubscriberMgmt/SystemConfig/CallProcessing/extendedCallingLineID*
- *SubscriberMgmt/SystemConfig/CallProcessing/honorCLIDBlockingForEmergencyCalls*
- *SubscriberMgmt/SystemConfig/CallProcessing/useUnicodeIdentityName*
- *SubscriberMgmt/SystemConfig/Provisioning/configurableCLIDNormalization*
- *System/CallP/CountryCodes/<countryCode>/enablePrefix*
- *System/CallP/CountryCodes/<countryCode>/prefix*
- *System/CallP/CountryCodes/<countryCode>/disableNationalPrefixForOffNetCalls*

The call types defined under the *System/CallP/CallTypes* level of the Application Server CLI control which digit patterns are considered to be emergency and repair calls. The identity handling for emergency and repair calls can be different from other calls, so this system call type configuration is loosely related to identity handling.

# 11 SIP Identity/Device Profile Type Policies

The Application Server provides policies for each SIP identity/device profile type that are used to configure how each specific SIP identity/device profile type behaves.

The following SIP identity/device profile type policies are the main policies relevant to identity handling. For full details on these SIP identity/device profile type policies and their configuration, see the *BroadWorks Application Server System Provider Web Interface Administration Guide* [5], the *BroadWorks Application Server Command Line Interface Administration Guide* [2], and the *BroadWorks SIP Access Interface Interworking Guide* [4].

- E164 Capable
- Trusted
- Use History-Info Header
- Support Identity In UPDATE and Re-INVITE
- Unscreened Presentation Identity Policy – This policy should generally be left at its default setting of “Profile Presentation Identity”. Only very specific scenarios should set the policy to use the unscreened presentation identity.

# 12 SIP Identity Headers

There are various SIP headers associated with the identity types defined in section *3 Identity Types*. The following subsections list the main SIP headers associated with these identity types for INVITE dialogs. For full details on these headers and their handling, see the *BroadWorks SIP Network Interface Interworking Guide* [3] and the *BroadWorks SIP Access Interface Interworking Guide* [4].

## 12.1 From

The Application Server always treats the *From* header as a presentation identity (see section *3.1.1 Calling Identity*). The Application Server does not support *RFC 4916* (see *Connected Identity in the Session Initiation Protocol (SIP), RFC 4916* [17]), so the *From* header is not allowed to change mid-dialog and is never treated as a connected identity.

## 12.2 P-Asserted-Identity

In an initial INVITE, the Application Server normally treats the *P-Asserted-Identity* header as either a presentation identity (see section *3.1.1 Calling Identity*) or as an asserted identity (see section *3.2 Asserted Identity*) depending on the Application Server's configuration and the call scenario. If the Application Server is in IMS mode or has TS 29.163 compliance enabled, then the initial INVITE's *P-Asserted-Identity* header is normally treated as an asserted identity. Otherwise, the initial INVITE's *P-Asserted-Identity* header is normally treated as a presentation identity.

When the SIP *chargeHeaderFormat* system parameter is set to "paiTelURI", the tel URI entry of the *P-Asserted-Identity* header sent by the Application Server in an initial INVITE contains a charge identity (see section *3.4 Charge Identity*) instead when applicable.

In subsequent *18x* and *200 OK* responses to INVITE's, in Re-INVITE requests, and in UPDATE requests, the Application Server always treats the *P-Asserted-Identity* header as a presentation identity (see *3.1.2 Connected Identity*).

## 12.3 P-Preferred-Identity

The Application Server treats a received *P-Preferred-Identity* header in largely the same manner as the *P-Asserted-Identity* header (see section *12.2 P-Asserted-Identity*). However, the Application Server does not support receiving the *P-Preferred-Identity* header in IMS mode, and never sends the *P-Preferred-Identity* header in IMS mode or standalone mode.

## 12.4 Remote-Party-ID

The Application Server treats the *Remote-Party-ID* header in largely the same manner as the *P-Asserted-Identity* header (see section *12.2 P-Asserted-Identity*). However, the Application Server does not support receiving the *Remote-Party-ID* header in IMS mode and never sends the *Remote-Party-ID* header in IMS mode.

## 12.5 Diversion

The Application Server normally treats a *Diversion* header entry as a redirecting identity (see section *3.3 Redirecting Identity*).

When the SIP *chargeHeaderFormat* system parameter is set to "diversionSip", a *Diversion* header entry sent by the Application Server contains a charge identity instead, when applicable (see section *3.4 Charge Identity*).

The *privacy* parameter for a *Diversion* header entry applies privacy to the redirecting identity for the entry. The *Privacy* header also applies privacy to redirecting identities as described in section *12.9 Privacy*.

## 12.6 History-Info

The Application Server treats a *History-Info* header entry as a redirecting identity (see section *3.3 Redirecting Identity*).

## 12.7 Charge

The Application Server treats the *Charge* header as a charge identity (see section *3.4 Charge Identity*). Note that the Application Server sends the *Charge* header when applicable but does not support receiving it.

## 12.8 P-Charge-Info

The Application Server treats the *P-Charge-Info* header as a charge identity (see section *3.4 Charge Identity*). Note that the Application Server sends the *P-Charge-Info* header when applicable but does not support receiving it.

## 12.9 Privacy

The Application Server uses the *Privacy* header to identity the privacy (CLIR/COLR) requested for the presentation identity in a SIP message. The *Privacy* header is also used to identify the privacy (CLIR) requested for the asserted identity in an initial INVITE.

The *Privacy* header also applies privacy to redirecting identities when the “history” value is present in the *Privacy* header. This includes when the *Privacy* header is escaped within a *History-Info* header entry.

## 12.10 RPID-Privacy

The Application Server treats the *RPID-Privacy* header in largely the same manner as the *Privacy* header (see section *12.9 Privacy*). However, the Application Server does not support receiving the *RPID-Privacy* header in IMS mode, and the *RPID-Privacy* header never applies to a redirecting identity.

## 12.11 Anonymity

The Application Server treats the *Anonymity* header in largely the same manner as the *Privacy* header (see section *12.9 Privacy*). However, the Application Server does not support receiving the *Anonymity* header in IMS mode, and the *Anonymity* header never applies to a redirecting identity.

# 13 IMS Mode

The Application Server can be deployed in IMS mode or in non-IMS mode (which is commonly referred to as standalone mode).

When deployed in IMS mode, the following IMS system parameters found under the *Interfaces/IMS* level of the Application Server CLI are relevant to identity handling:

- userPhoneErrorCorrection
- includeDirectoryNumberInPAI
- pServedUserSyntax
- enableOIPCompliance
- includeTrunkGroupPilotInPAITelURI

In addition to the SIP headers listed in section *12 SIP Identity Headers,* the following additional SIP headers are relevant to identity handling in IMS mode:

- *P-Served-User*
- *P-Served-User-Identity*

There are some differences in how the Application Server treats the SIP identity headers for IMS mode. Particularly notable is that the *P-Asserted-Identity* header the Application Server sends in an initial INVITE for a user includes both a SIP URI entry with the user's primary SIP URI (which is normally the user's primary SIP PUI) and a tel URI entry with an applicable DN for the user.

For full details of the IMS system parameters and SIP identity header handling in IMS mode, see the *BroadWorks AS Mode IP Multimedia Subsystem Solution Guide* [12] and the *BroadWorks AS Mode ISC Interface Specification* [13].

# 14 TS 29.163 Compliance

The Application Server can be configured with TS 29.163 (see the 3GPP TS 29.163 – *Interworking between the IP Multimedia (IM) Core Network (CN) Subsystem and Circuit Switched (CS) Network* [18]) compliance enabled or disabled via the SIP *enableTS29163Compliance* system parameter.

When TS 29.163 compliance is disabled in standalone mode, the Application Server does not support separate presentation and asserted identities for an initial INVITE. On the incoming side, a single identity is selected from the received presentation and asserted identity headers, and that identity is used as the received presentation identity. On the outgoing side, the presentation identity is included in both the *From* header and the *P-Asserted-Identity*/*Remote-Party-ID* header (if these headers are to be included at all).

When TS 29.163 compliance is enabled in standalone mode, the Application Server supports separate presentation and asserted identities. On the incoming side, the presentation identity and asserted identity headers are treated independently and both the presentation and asserted identity are kept. On the outgoing side, the presentation identity is included in the *From* header and the asserted identity is included in the *P-Asserted-Identity*/*Remote-Party-ID* header (if these headers are to be included at all).

In IMS mode, the Application Server supports separate presentation and asserted identities regardless of whether TS 29.163 compliance is enabled. However, whether TS 29.163 compliance is enabled does have impacts in IMS mode. For example, the IMS *includeDirectoryNumberInPAI* system parameter setting does not apply when TS 29.163 compliance is enabled (it is always treated as if set to “true”).

For full details on the TS 29.163 compliance interactions, see the *Calling Line Identity Compliance Enhancements Feature Description* [19].

# 15 Call Detail Record Fields

The Call Detail Record (CDR) generated by the Application Server for a call contains many different fields. The following CDR fields are the main fields that contain identity-related information. For full details on these and other CDR fields, see the *BroadWorks Accounting Call Detail Record Interface Specification* [9].

- userNumber
- groupNumber
- callingNumber
- callingPresentationIndicator
- calledNumber
- originalCalledNumber
- originalCalledPresentationIndicator
- originalCalledReason
- redirectingNumber
- redirectingPresentationIndicator
- redirectingReason
- otherPartyName
- otherPartyNamePresentationIndicator
- clidPermitted
- chargeNumber
- calledNumberContext
- callingNumberContext
- originalCalledNumberContext
- redirectingNumberContext
- calledAssertedIdentity
- calledAssertedPresentationIndicator
- configurableCLID
- namePermitted
- dialableCallingNumber
- callingPresentationNumber
- callingPresentationNumberContext
- callingAssertedNumber
- callingAssertedNumberContext
- calledPartyAddress

# 16 Configuration Examples

## 16.1 Presentation Identity Name

**Use the subscriber's name as the presentation identity name for all calls**

- Configure the name for the subscriber.
- Disable the *Use group name for Calling Line Identity* policy in effect for the subscriber.
- Make a call for the subscriber.

**Use the group's name as the presentation identity name for non-emergency external calls**

- Configure the name for the subscriber's group.
- Enable the *Use group name for Calling Line Identity* policy in effect for the subscriber.
- Make a non-emergency external call for the subscriber.

**Use the department's name as the presentation identity name for non-emergency external calls**

- Configure the name for the subscriber's department.
- Enable the *Use group name for Calling Line Identity* policy in effect for the subscriber.
- Enable the *Allow Department Name Override* policy in effect for the subscriber.
- Make a non-emergency external call for the subscriber.

**Block the subscriber's presentation identity name from being included for regular external calls**

- Enable the *Block Calling Name for External Calls* policy in effect for the subscriber.
- Make a regular (non-emergency, non-repair) external call for the subscriber.

## 16.2 Presentation Identity Address

**Use the subscriber's DN as the presentation identity address for all external calls**

- Configure the primary DN for the subscriber.
- Set the *External Calls* and *Emergency Calls* policies in effect for the subscriber to "Use user phone number for Calling Line Identity".
- Make an external call for the subscriber.

**Use the subscriber's configurable CLID as the presentation identity address for all external calls**

- Configure the configurable CLID for the subscriber.
- Set the *External Calls* and *Emergency Calls* policies in effect for the subscriber to "Use configurable CLID for Calling Line Identity".
- Make an external call for the subscriber.

**Use the group CLID as the presentation identity address for all external calls**

- Configure the group CLID for the subscriber's group.
- Set the *External Calls* and *Emergency Calls* policies in effect for the subscriber to "Use group/department phone number for Calling Line Identity".
- Make an external call for the subscriber.

**Use the group-level department CLID as the presentation identity address for all external calls**

- Configure the department CLID for the subscriber's group-level department.
- Set the *External Calls* and *Emergency Calls* policies in effect for the subscriber to "Use group/department phone number for Calling Line Identity".
- Make an external call for the subscriber.

**Use a different presentation identity address for emergency calls than other external calls**

- Set the *Emergency Calls* policy in effect for the subscriber to the desired value.
- Set the *External Calls* policy in effect for the subscriber to the desired value.
- Make an emergency call for the subscriber.
- Make an external call for the subscriber.

**Use the subscriber's extension as the presentation identity address for enterprise calls**

- Configure the primary extension for the subscriber.
- Set the *Enterprise Calls* policy in effect for the subscriber to "Use extension".
- Make an enterprise call for the subscriber.

**Use the group's location code plus the subscriber's extension as the presentation identity address for enterprise calls**

- Configure the location code for the subscriber's group.
- Configure the primary extension for the subscriber.
- Set the *Enterprise Calls* policy in effect for the subscriber to "Use location code plus extension".
- Make an enterprise call for the subscriber.

**Use the external presentation identity address for enterprise calls**

- Set the *External Calls* policy in effect for the subscriber to the desired value.
- Set the *Enterprise Calls* policy in effect for the subscriber to "Use External Calls Policy".
- Make an enterprise call for the subscriber.

**Use the subscriber's extension as the presentation identity address for group calls**

- Configure the primary extension for the subscriber.
- Set the *Group Calls* policy in effect for the subscriber to "Use extension".
- Make a group call for the subscriber.

**Use the group's location code plus the subscriber's extension as the presentation identity address for group calls**

- Configure the location code for the subscriber's group.
- Configure the primary extension for the subscriber.
- Set the *Group Calls* policy in effect for the subscriber to "Use location code plus extension".
- Make a group call for the subscriber.

**Use the external presentation identity address for group calls**

- Set the *External Calls* policy in effect for the subscriber to the desired value.
- Set the *Group Calls* policy in effect for the subscriber to “Use External Calls Policy”.
- Make a group call for the subscriber.

## 16.3 Privacy

**Enforce the subscriber’s privacy for group calls**

- Enable the *Enforce Group Calling Line Identity Restriction* policy in effect for the subscriber.
- Make a group call for the subscriber where the subscriber requests privacy for the call (such as via the Calling Line ID Delivery Blocking or Connected Line Identification Restriction service).

**Enforce the subscriber’s privacy for enterprise calls**

- Enable the *Enforce Enterprise Calling Line Identity Restriction* policy in effect for the subscriber.
- Make an enterprise call for the subscriber where the subscriber requests privacy for the call (such as via the Calling Line ID Delivery Blocking or Connected Line Identification Restriction service).

## 16.4 Redirection Handling

**Do not allow the subscriber’s alternate numbers for the redirecting identity**

- Configure the Alternate Numbers service for the subscriber with an alternate DN.
- Disable the *Allow Alternate Numbers for Redirecting Identity* policy in effect for the subscriber.
- Make a call to the alternate DN for the subscriber that is redirected (such as via Call Forwarding Always).

**Do not allow the subscriber’s configurable CLID for the redirecting identity**

- Configure the configurable CLID for the subscriber.
- Set the *External Calls* and *Emergency Calls* policies in effect for the subscriber to “Use configurable CLID for Calling Line Identity”.
- Disable the *Allow Configurable CLID for Redirecting Identity* policy in effect for the subscriber.
- Make a call to the subscriber that is redirected (such as via Call Forwarding Always).

**Use the subscriber’s identity as the connected identity for all redirected calls**

- Set the *Connected Line Identification Privacy on Redirected Calls* policy in effect for the subscriber to “Privacy For All Calls”.
- Make a call to the subscriber that is redirected (such as via Call Forwarding Always).
- Note that if the originating party later redirects the call themselves, the calling identity and asserted identity for the originally called subscriber (the subscriber with the *Connected Line Identification Privacy on Redirected Calls* policy in effect) are used for the redirection.

**Use the subscriber's identity as the calling identity and asserted identity for all redirected calls**

- Set the *Calling Line Identity for Redirected Calls* policy in effect for the subscriber to "Redirecting User's Identity for All Redirections".
- Make a call to the subscriber that is redirected (such as via Call Forwarding Always).

## 16.5 Private Call Category Handling

**Override the subscriber's CLIR for private call category calls**

- Enable the *Override CLID Restriction For Private Call Category* policy in effect for the subscriber.
- Make an external call from the subscriber where the subscriber requests privacy for the call (such as via the Calling Line ID Delivery Blocking service), and the *Contact* header entry returned by the Network Server for the origination has the *cat* parameter set to "PRIVATE".

**Use the subscriber's group call presentation identity for private call category calls**

- Configure the subscriber's group without a location code.
- Set the *Group Calls* policy in effect for the subscriber to the desired value.
- Enable the *Use Enterprise CLID For Private Call Category* policy in effect for the subscriber.
- Make an external call from the subscriber where the *Contact* header entry returned by the Network Server for the origination has the *cat* parameter set to "PRIVATE".

**Use the subscriber's enterprise call presentation identity for private call category calls**

- Configure the subscriber's group with a location code.
- Set the *Enterprise Calls* policy in effect for the subscriber to the desired value.
- Enable the *Use Enterprise CLID For Private Call Category* policy in effect for the subscriber.
- Make an external call from the subscriber where the *Contact* header entry returned by the Network Server for the origination has the *cat* parameter set to "PRIVATE".

## 16.6 Dialable Caller ID

**Use the Dialable Caller ID presentation identity for the subscriber's incoming calls**

- Enable the *Dialable Caller ID* policy in effect for the subscriber.
- Make an external call to the subscriber where the originating party does not request privacy.

## Acronyms, Abbreviations, and Terminology

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

| | |
|---|---|
| Address | A phone number or SIP URI. |
| Alternate DN/extension | A DN or extension assigned to the Alternate Numbers service for a subscriber. |
| CDR | Call Detail Record |
| CLI | Command Line Interface |
| CLID | Calling Line Identification, Calling Line Identity, or Calling Line ID |
| CLIP | Calling Line Identification Presentation (same functionality as OIP). The Calling Name Delivery, Calling Number Delivery, Internal Calling Line ID Delivery, and External Calling Line ID Delivery services are the CLIP services on the Application Server. |
| CLIR | Calling Line Identification Restriction (same functionality as OIR). The Calling Line ID Delivery Blocking service is the CLIR service on the Application Server. |
| CN | Core Network |
| COLP | Connected Line Identification Presentation (same functionality as TIP). |
| COLR | Connected Line Identification Restriction (same functionality as TIR). |
| Configurable CLID | The *Calling Line ID Phone Number* (if any) configured for a subscriber. |
| CS | Circuit Switched |
| DCLID | The Dialable Caller ID call processing policy. |
| Department CLID | The *Department Calling Line ID Number* (if any) configured for a department. |
| DN | Directory Number. An E.164 phone number configured on the Application Server for DN purposes (such as the primary DN for a subscriber or the group CLID for a group). |
| Enterprise Call | A call routed directly between two subscribers in different groups of the same enterprise. |
| External Call | A call that is not routed as a group or enterprise call. This includes calls between two subscribers in the same group or enterprise that are forced to be external calls by the call processing policies in effect. |
| Group Call | A call routed directly between two subscribers in the same group. |
| Group CLID | The *Calling Line ID Group Number* (if any) configured for a group. |
| IM | IP Multimedia |
| IMPU | IP Multimedia Public Identity. Also commonly referred to as a PUI. |
| IMS | IP Multimedia Subsystem |

| | |
|---|---|
| Internal Call | A call that is routed as a group or enterprise call. |
| IP | Internet Protocol |
| ISC | IMS Service Control |
| NCOS | Network Class of Service |
| OIP | Originating Identification Presentation (same functionality as CLIP). The Calling Name Delivery, Calling Number Delivery, Internal Calling Line ID Delivery, and External Calling Line ID Delivery services are the OIP services on the Application Server. |
| OIR | Originating Identification Restriction (same functionality as CLIR). The Calling Line ID Delivery Blocking service is the OIR service on the Application Server. |
| PAI | P-Asserted-Identity |
| PPI | P-Preferred-Identity |
| Primary DN/extension | The DN/extension assigned to a subscriber's profile. |
| PSI | Public Service Identity |
| PUI | Public User Identity. Also commonly referred to as an IMPU. |
| RPID | Remote-Party-ID |
| SIP | Session Initiation Protocol |
| Standalone Mode | An Application Server deployed in non-IMS mode. |
| Subscriber | A BroadWorks user or virtual subscriber. |
| TIP | Terminating Identification Presentation (same functionality as COLP). The Connected Line Identification Presentation service is the TIP service on the Application Server. |
| TIR | Terminating Identification Restriction (same functionality as COLR). The Connected Line Identification Restriction service is the TIR service on the Application Server. |
| Trusted Location | A trusted location is a SIP location the Application Server considers trusted and allowed to receive the full identity information for the call without privacy being applied. A trusted location is expected to apply privacy itself or forward the privacy information along as applicable. All network devices are considered trusted. A SIP access device is only considered trusted if the *Trusted* policy is enabled for its identity/device profile type. |
| TS | Technical Specification |
| URI | Uniform Resource Identifier |
| User | A BroadWorks user. |
| Virtual Subscriber | A BroadWorks subscriber that represents an instance of a service such as an Auto Attendant or a Call Center. |

## References


[1] BroadSoft, Inc. 2015. *BroadWorks Call Processing Policies Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[2] BroadSoft, Inc. 2015. *BroadWorks Application Server Command Line Interface Administration Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[3] BroadSoft, Inc. 2015. *BroadWorks SIP Network Interface Interworking Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[4] BroadSoft, Inc. 2015. *BroadWorks SIP Access Interface Interworking Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[5] BroadSoft, Inc. 2015. *BroadWorks Application Server System Provider Web Interface Administration Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[6] BroadSoft, Inc. 2015. *BroadWorks Application Server Group Web Interface Administration Guide - Part 1, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[7] BroadSoft, Inc. 2015. *BroadWorks Application Server Group Web Interface Administration Guide - Part 2, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[8] BroadSoft, Inc. 2015. *BroadWorks User Web Interface Administration Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[9] BroadSoft, Inc. 2015. *BroadWorks Accounting Call Detail Record Interface Specification, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[10] BroadSoft, Inc. 2015. *BroadWorks Service Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[11] BroadSoft, Inc. 2015. *BroadWorks Service Interaction Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[12] BroadSoft, Inc. 2015. *BroadWorks AS Mode IP Multimedia Subsystem Solution Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[13] BroadSoft, Inc. 2015. *BroadWorks AS Mode ISC Interface Specification, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[14] BroadSoft, Inc. 2015. *BroadWorks SIP Trunking Solution Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[15] BroadSoft, Inc. 2015. *BroadWorks Call Center Solution Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[16] BroadSoft, Inc. 2015. *BroadWorks Mobility Guide, Release 21.0*. Available from BroadSoft at xchange.broadsoft.com.

[17] J. Elwell, “Connected Identity in the Session Initiation Protocol (SIP)”, RFC 4916, Internet Engineering Task Force, June 2007. Available from http://www.ietf.org/.

[18] 3rd Generation Partnership Project (3GPP). 2014. *Interworking between the IP Multimedia (IM) Core Network (CN) Subsystem and Circuit Switched (CS) Network; Release 12*. Available from http://www.3gpp.org/.




 

[19] BroadSoft, Inc. 2013. *Calling Line Identity Compliance Enhancements Feature Description, Release 18.0*. Available from BroadSoft at xchange.broadsoft.com.