Bria 4 Configuration Guide

Enterprise Deployments

CounterPath Corporation
Suite 300, One Bentall Centre
505 Burrard Street, Box 95
Vancouver, BC V7X 1M3
Tel: 604.320.3344
sales@counterpath.com www.counterpath.com

This manual corresponds to Bria version 4.0.

R1

Contents

About this Manual

This manual applies to all platforms of Bria: Bria *for Windows* and Bria *for Mac*.

This manual is intended for:

- System administrators who are deploying Bria in their enterprise by remotely configuring the client through remote provisioning. (For more information on the options for configuring, see the “Bria 4 Administrator Guide”).
- VoIP service providers who have purchased the retail version of Bria and want to remotely configure Bria for their customers.

It gives an overview of the types of features that can be configured, and provides context for all the settings that you can provision.

This manual is intended to be read in conjunction with:

- The Bria provisioning guide, “Bria 4 Provisioning Guide - Enterprise Deployments”, which describes the mechanism for configuring the features.
- The Bria 4 Settings reference documentation (a Microsoft® Excel® document). The Bria 4 Settings reference documentation provides detailed information on settings that may only be mentioned by name in this configuration manual.
- “Bria 4 Dial Plan Guide”, if you implement dial plans.

1 About Configuration

Bria Settings

Configuration of Bria 4 is achieved largely through assigning appropriate values to settings. Settings let you:

- Configure Bria 4 for the environment (network and so on) in which it will work.
- Configure Bria 4 for server-side functions you support, such as RLS workgroups.
- Configure how some Bria 4 features work, and configure whether a feature is enabled or disabled.
  - How features work: For example, entering the phone numbers to use for voicemail.
  - Enable or disable features: The features that can be set in this way are those that have already been included in your brand before compiling. You can disable features for specific installs. For example, you could enable Workgroup for some users and disable it for others.

Bria and Multiple Accounts

Bria supports up to ten accounts, in any combination of SIP and XMPP.

Bria also supports one Outlook account (in Bria *for Windows*) or one Mac Address Book account (in Bria *for Mac*); these accounts are used for contacts, as described in “Outlook or Mac Address Book Accounts” on page 11.

Using this Manual

In the following pages, the settings are broken down into topics. Topics are organized alphabetically. Within each topic, general information is provided on how the settings in the topic work. Some topics do not apply to specific platforms.

You can read a topic then consult the Bria 4 Settings reference documentation (available separately) for detailed information on each individual setting. Within that reference documentation, you can sort the table by the Topic column in order to group related settings together.

2 Configuration Settings by Topic

2.1 Account Credentials

Account credentials for each account consist of the user name and password. Do not confuse these credentials with the login credentials.

2.2 Account Setup

These settings define the user's account or accounts. There is one section for each account: proxy0, proxy1, and so on.

Each account is either a SIP or an XMPP account, as specified by the proxies:proxyn:protocol setting.

For each account type, a different subset of the proxies settings is applicable. For example, proxies: proxyn:register applies only to a SIP account, while proxies:proxyn:xmpp_resource applies only to an XMPP account. A few settings (such as proxies:proxyn:account_name) apply to both types.

Make sure you configure the appropriate settings for each account type. If a setting in a given section (proxyn) does not apply to that account type, Bria simply ignores it.

XMPP Cross Domain

Bria supports the XMPP cross domain feature. With this feature, the user can send/receive IMs and send/receive presence subscriptions for addresses that are foreign to any of the XMPP accounts set up in Bria. For example, if the XMPP account is zippy-phone.com, the user can receive IMs from kperera11@gmail.com without having to set up gmail.com as an XMPP account.

Account selection: If two XMPP accounts are set up, traffic for a foreign domain will go through one of these two accounts. Usually it will go through the first enabled account in the list, but there is no guarantee. The foreign-domain address becomes linked to this account, so subscription to this address only occurs if that account is enabled.

The XMPP server must allow passthrough of foreign addresses. So Bria will allow the user to attempt to subscribe to kperera11@gmail.com, but zippy-phone.com may or may not send the subscription request on its merry way.

2.3 Account Usage

The setting proxies:proxyn:enabled_features enables or disables the following features on each account:

- Audio call
- Video call. Enable video calls only if you also enable audio calls.
- IM
- Presence

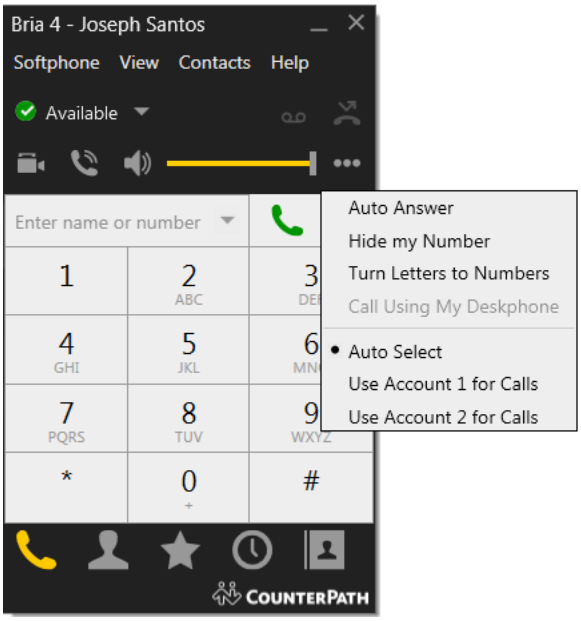
- Workgroup

This setting is a bitmask with a default value that enables every feature.

Preferred Account for Calls

This information applies only if users have more than one SIP account.

The setting feature:accounts:defaultForCall is used by Bria to select the account to use for a phone call when account selection mode is set to Auto Account.



- Bria tests the phone call against the dial plans. It runs through the dial plans in order, starting with the dial plan for the first account, and it stops at the first match. See page 7 for information on dial plans.
- If testing against the dial plan does not result in a selection, the account specified in feature:accounts:defaultForCall is used.

  Typically, this setting is either left empty, in which case the first account is set as the preferred account. Keep in mind that in any event the user can change the preferred account via the Account List.

2.4 Audio Quality

These settings provide controls for audio quality.

2.5 Call Security (Encryption)

About Signaling and Media Encryption

Bria can be configured to support signaling and media encryption (security) for phone calls.

- Signaling encryption is only possible using TLS as the transport; UDP and TCP do not support signaling encryption.
- Media encryption, which is performed using SRTP, can only be supported if signaling encryption is in place, in other words, if TLS is used for the transport.

Setting up for Security outside of Bria

When using TLS, the user must have the root certificate that signs the proxy's chain of certificates. In most cases, the root certificate will already be installed. Procedures for exchange of certificates are outside the scope of this documentation. The certificates must be stored on the Bria computer, in the root certificate store.

Setting up the root certificate on the Bria user's computer ensures that the connection to the proxy is TLS secure (the first hop). Any proxy in the chain (between the user and the other party) that does not support TLS may cause an insecure link in the chain. Therefore, if the other party is outside your domain, you cannot be completely sure that the call is secured at the signaling level, which means that you cannot be sure that it is secured at the media level.

When a call with both signaling and media encryption is established, Bria displays the encryption icon. This icon indicates that the call is secure between each caller and their proxy (the first and last hops); the call may or may not be secure for other hops.

Encryption Options Supported by Bria

You must set up each account to enable or disable call encryption.

Option	How Outgoing Calls are Handled	How Incoming Calls Are Handled
Make and accept only encrypted calls	Bria will place all calls with TLS. The call invite will specify SRTP media encryption. If the correct certificates are not in place or if the other party does not accept encrypted calls, the call will fail.	Bria will only accept INVITEs that are for encrypted calls. If Bria receives a call INVITE that is not encrypted, the call will be rejected.
Do not allow encrypted call	Bria will place only unencrypted calls. If the other party does not accept unencrypted calls, the call will fail.	Bria will only accept INVITEs that are for unencrypted calls. If Bria receives a call invite that is encrypted, the call will be rejected.

Configuring for these Encryption Options

- To support encrypted calls, set proxies:proxyn:transport to TLS and set proxies:proxyn:security_outgoing_srtp to true.
- To support only unencrypted calls, set proxies:proxyn:transport to Auto, UDP or TCP and set proxies:proxyn:security_outgoing_srtp to false.

2.6 Chat Room

If you support XMPP accounts, you can set up persistent chat rooms on your XMPP server. Users with accounts on that XMPP server can then join any chat room (View > Chat Rooms).

Chat rooms are set up to allow the same group of people to have a group IM session, usually on a regular basis. Note that the chat room feature is not the same as group chat: chat rooms involve persistent groups, while the group chats are created on the fly by the user.

Bria supports the following features:

- Open chat rooms: users can join without being already set up as a member of the group.
- Members-only chat rooms: users can join only if already set up as a member.
- Password-protected (confidential) chat rooms: users must enter the password to join.

On your XMPP server, create the chat room. Add members if desired and if supported by your XMPP server. Assign passwords if desired and if supported by your XMPP server.

2.7 Codec Usage

Your brand includes a specific set of built-in codecs. A codec may be royalty-bearing or non-royalty-bearing: see the Bria 4 Settings reference documentation for details. You can restrict codec usage by enabling or disabling a codec and by setting the license count (even on non-royalty-bearing codecs).

Enabling Codecs

To enable a codec, set its codecs:<codec name>:enabled setting to true. When a codec is enabled, it appears in the enabled list in the Preferences > Audio Codecs or Preferences > Video Codecs tab.

Note that whether a codec is enabled is only one of the factors in whether it will be used for a call. The other factors are:

- The license count for codecs. For royalty-bearing codecs, there is a limit to the number of simultaneous calls or number of legs (in the case of a conference call) that can use the codec. Once the limit is reached, that codec will not be used for new calls.
- Whether the codec is also enabled by the other party
- Its ranking in the SDP list
- How the codec is chosen; from the list of codecs that advertised by the other party in their SDP, that are enabled on the local Bria computer, Bria chooses the codec that is listed first.

2.8 Contact List Setup

See “Resources” on page 13.

2.9 Deskphone Control

If you are deploying to an enterprise that uses SIP deskphones, you can configure Bria to use them. Users will be able to initiate calls from Bria (for example, in order to make use of the history or contact list) then switch over to the deskphone for the rest of the call.

The deskphone must be a SIP phone that supports dialog events.

Each user must be configured separately for deskphone, so in order to provision deskphone data, you must provision individual data for each user. The other option is to let the users specify the deskphone URI themselves, on the Preferences > Devices tab.

To set up for deskphone:

- Make sure the deskphone has already been set up in the network and on the PBX, and that it can make phone calls.
- Set feature:deskphone:subscribe_path to the URI of the deskphone. For example, 3210@myEnterprise.com
- To test the deskphone setup, on the Bria dashboard menu, choose Call Using My Deskphone. Then place a call.

2.10 Device Configuration

These settings let you specify whether or not Bria will automatically detect the devices connected to the computer. If device detection is enabled, you can optionally identify the device that you want Bria to chose, if that device is present.

2.11 Dial Plan

The dial plan defines patterns that a user-dialed phone number are matched to. A dial plan is used for any combination of these reasons:

- To modify the input if that is required to ensure that the call gets established. For example, to add the “9” required to obtain an outside line from a PBX.
- To select the account to use to place a call, if users can have more than one account. For example, if you want calls that match one pattern to go through one account and calls that match another pattern to go through another account.
- To prevent unresolvable calls being placed. For example, to prevent using network bandwidth on a call that will certainly fail. You define patterns that you know will work, and only place a call if it matches one of these patterns.

Dial plans are optional: it is possible to instruct the user to modify the input manually (for example, to always include “9” when dialing an outside number) and to either use the preferred account or manually select the account to use for calls.

For detailed information on dial plans, see the “Bria 4 Dial Plan Guide”.

2.12 Directory

If you have set up an LDAP directory or Active Directory (Bria *for Windows* only) on a remote server, you can configure Bria to fetch data from it. This data will be displayed in the Directory in the Resources module.

- To enable the Directory, set feature:ldap:enable or feature:adsi:enable to true; the Directory tab will be included next to the Contacts tab and History tab in the Resources module.

  Make sure to enable the directory only for LDAP or ADSI, not for both!

- Set all the settings with “key” in their name for the appropriate directory type. For example, set feature:adsi:<xx_key> if you are using Active Directory.

  These settings are used to map the attribute in your directory to the corresponding attribute in Bria. Be careful with this mapping, because if the user creates a contact from the entry, the application will allow/disallow certain functions (such as sending an IM) based on whether a property of that contact is populated.

- Complete these settings in the appropriate feature:<type> domain/section to control how the data is retrieved. Read the information in the search_on_demand setting in the settings documentation for information on how these settings work.
  - search_on_demand. If true, then the directory works in “Search-on-demand” mode. If false, it works in “Fetch-and-filter” mode.
  - polltime (Search-on-demand mode only)
  - sizelimit
  - timeout
- Complete these settings in the appropriate feature:<type> domain/section to connect to the directory and find the location of the directory data:

  For LDAP:

  - ldap:auth_method
  - ldap:password
  - ldap:query
  - ldap:root
  - ldap:server
  - ldap:use_tls
  - ldap:username

  For ADSI:

  - adsi:root

Refreshing of Directory

When data in the directory on the server changes, the Directory in Bria is refreshed, either immediately (for Search-on-demand mode) or at the next fetch (for Fetch-and-filter mode).

Synchronization between Directory and Contacts

Users may create contacts from directory entries. Whenever the corresponding directory entry is refreshed, the information in these contacts will be refreshed. If a directory entry is deleted from the server, then the contact is also deleted.

2.13 DTMF

This group of settings configures Bria to handle DTMF. DTMF can be sent in one of these ways:

- Out-of-band using DTMF 2833 packets
- Via SIP INFO
- In-band: Bria will encode the DTMF signals in the audio stream as regular sound.
- Out-of-band using DTMF 2833 and via SIP INFO
- In-band and via SIP INFO

To configure DTMF, set the desired settings to true. Do not set both inband and outofband to true; if you do, the inband setting will be ignored. If you set all three settings to 0, DTMF will not be sent at all.

The preferred DTMF method is out-of-band.

In-band is used only to deal with specific network situations. For example:

- One scenario in which it might be advisable to send in-band is if you own your gateways and:
  - One or more of these gateways does not support 2833 or does not handle it well, and
  - Your gateway is using codes that reproduce DTMF tones well.

  In this case, sending in-band will ensure that DTMF tones get through (because the DTMF tones will bypass the gateway) and that they reproduce accurately at the receiving end.
- Another scenario is:
  - One or more of these gateways does not support 2833 or does not handle it well.
  - Your gateway is using codecs that do not reproduce DTMF tones well (because they are designed to handle human voice rather than artificial sounds).

  In this scenario, using in-band will not help ensure DTMF ones get through. There is in fact no solution in this scenario.

2.14 Feature Enabling at the Account Level

See “Account Usage” on page 3.

2.15 Feature Enabling: Enabling Other Features

Other features are enabled and configured through other settings. See:

- “Deskphone Control” on page 7.
- “Directory” on page 8.
- “File Transfer” on page 10.
- “Network – XMPP” on page 11.
- “Voicemail – MWI Notification” on page 15.
- “Voicemail – Send to Voicemail” on page 16.
- “User Experience” on page 15.
- “Workgroup” on page 17.

2.16 File Transfer

File transfer is automatically supported if the XMPP account is supported.

Both the sender and the recipient must have XMPP accounts and the local user must be subscribing to the recipient's presence through the XMPP account. In addition, both sides must be enabled for XMPP file transfer.

XMPP file transfer is direct if a peer-to-peer connection exists between the two sides. If such a connection is not possible, then the transfer is sent via the XMPP proxy that the XMPP service provides.

The feature:file_transfer:file_save_path lets you specify the path where received files will be saved.

2.17 License Provisioning

The license key can be provided to the client through remote provisioning. See the Bria provisioning guide for details.

Or the key can be provided to the user outside of Bria, through an e-mail, for example. In this case, the user chooses Help > Enter License Key to display the Enter License dialog.

2.18 Network – SIP

This group covers settings in several subtopics, all relating to SIP accounts (not XMPP accounts). Make sure you set them for each of your SIP accounts. For your XMPP accounts, the settings are simply ignored.

DNS

This group of settings let you configure timing for DNS query requests, and lets you optionally specify a primary and secondary DNS server to use.

Firewall Traversal

You must configure the firewall traversal solution for each account. Set proxies:proxyn:firewall_traversal_mode for one of these:

- Auto detect using ICE: Automatically determine the contact address for signaling traffic.
- Advertise the local IP, public IP (discovered via STUN, if available), and media relay IP (discovered via TURN, if available), and use these to automatically determine the best route for media traffic during calls.
- Discover public IP address: Advertise the public IP address (discovered via STUN) for the contact address for signaling traffic, and for the connection address for media traffic.
- Use media relay (TURN): Advertise the public IP address (discovered via STUN) for the contact address for signaling traffic.
- Advertise the address of a media relay server (discovered via TURN) for the connection address for media traffic.
- None: Advertise the local IP address only for both signaling and media traffic.

Then complete the remaining proxies:proxyn:firewall_xx settings as required.

Other settings in this network group let you configure Bria for firewall traversal.

RTP Session

This group of settings let you configure how RTP session activity will be managed.

SIP Signaling

This group of settings let you configure how Bria handles SIP signaling.

2.19 Network – XMPP

This group covers settings relating to XMPP traffic. Make sure you set them for the XMPP account, if you support this.

2.20 Outlook or Mac Address Book Accounts

Bria *for Windows* is automatically set up with an Outlook account, if Outlook is detected on the user's computer. Bria *for Mac* is automatically set up with a Mac Address Book account. The user can enable this account in order to pull contacts from the address book into the Bria contact list.

For more information on populating the contact list, see "Resources" on page 13.

Outlook

For the Outlook account, the user's Bria may automatically detect the Outlook profile and password. If it does not, Bria will default to the first profile and prompt the user for the password. If you want to specify a profile other than the first profile, you can do so in feature:outlook0:profile.

You can also complete:

- feature:outlook0:softphonefield to set the field that will be recognized as a softphone field (and that can therefore be used for IM and presence via a SIP account).
- feature:outlook0:imfield setting to set the field that will be recognized as a jabber field (and that can therefore be used for IM and presence via an XMPP account).

Mac Address Book

For the Mac Address Book account, no setup is required by either your or the user.

2.21 Presence

Triggers for Presence Subscriptions

Presence subscriptions are started in the following cases:

- If the user creates or modifies a contact and adds an address in the Softphone field, then Bria subscribes to that address for presence if:
  - The domain of the address matches the domain of an existing, enabled SIP account.
  - And that SIP account is set up for IM/Presence (“Account Usage” on page 3).

  By default, the subscription is handled in peer-to-peer mode. You can change the mode to Presence Agent mode by setting in the Presence topic in the Bria 4 Settings reference documentation.
- If the user creates or modifies a contact and adds an address in the Instant Message field, then Bria subscribes to that address for presence if:
  - The domain of the address matches the domain of an existing, enabled XMPP account.
  - And the user clicks the Enable XMPP Presence button on the Contact Profile.

  The subscription is handled by the XMPP server; no setup is required in Bria.

How SIP Presence Subscriptions are Handled

Bria supports IETF standard SIMPLE presence using a SIP subscription to the presence event package. Bria supports the SIMPLE rich presence extensions (RPID - RFC 4480), which allows detailed presence information to be conveyed in a standards-compliant manner.

Peer-to-Peer Presence Mode

In peer-to-peer presence modes, the clients in the network send SIP SUBSCRIBE and NOTIFY messages directly to one another. The Bria that receives the request consults the local copy of the privacy rules to determine whether a rule already exists. If no rule exists for the other party, then the request is deferred to the user through a popup; the user’s action typically results in a privacy rule being created. The amount of SIP message traffic on the network can be substantially larger than in presence agent mode.

Presence Agent Mode

In presence agent mode, when Bria is first started, it sends presence information to the network using the SIP PUBLISH mechanism (RFC 3903). Bria still sends a SUBSCRIBE message per contact found in the contact list when it is first started, but the presence agent will simply return a NOTIFY message with the current presence document on behalf of the contact that was subscribed to. As well, Bria subscribes to the presence info (winfo - RFC 3857, 3858) event package which will inform the user when they have to make a presence authorization decision.

2.22 Resources

“Resources” refers to the storage location for contacts and privacy rules.

Resources for Contacts

Bria supports these resources:

- Local storage. All contact data is always stored locally (on the user’s computer). This means that some data exists in two places. For example, an XMPP address will be stored on the corresponding XMPP roster and will also be stored locally.

  No setup is required for local storage: it is automatic.

- XMPP roster. If the user creates an XMPP account, the contacts on that XMPP roster are pulled into Bria when the user enables the account. Bria supports vCards; see “XMPP Storage Options”, below.
- Outlook contacts or Mac Address Book contacts. Bria is automatically set up with an account corresponding to this resource. If the user enables this account, the contacts from that resource are pulled into Bria.
- Remote storage. You can set up a WebDAV and XCap remote server as a remote storage source for contacts. When the user starts Bria (and assuming that the SIP account is enabled), the contacts from that server will be pulled into Bria.

How Contacts Created by the User are Stored

When the user manually adds a contact in Bria, the contact is stored as follows:

- All data in the contact is stored locally.
- If you have set up remote storage, then all data is also sent to that location.
- Instant message address are considered to be XMPP addresses. If the XMPP address has a domain that matches the domain of an existing, enabled XMPP account, then the address is sent to that roster when the user clicks the Enable XMPP Presence button on the Contact Profile. Otherwise, the address is not sent.
- Contact data is never sent to the vCards associated with the XMPP roster (if you support vCards). This vCard resource is read only.
- Contact data is never sent to the Outlook or Mac Address Book. These resources are read only.

When the user manually modifies a contact, for example, adding an XMPP address to an existing contact, the same rules apply.

XMPP Storage Options

You may decide to support a self-administered XMPP account. (Or you may decide not to support this self-administered account and instead simply allow users to set up an XMPP account for their existing accounts such as Gmail).

If you do support a self-administered XMPP account and the contact roster on the server includes vCard data, you should set proxies:proxyn:xmpp_download_vcards to true on the proxyn that corresponds to the XMPP account. In this way, when the user enables the XMPP account, the vCard data will be pulled into Bria and each record will form a separate contact.

Remote Storage Source

To set up remote storage, complete the following settings in the proxyn that corresponds to the SIP account (typically proxy0):

- proxies:proxyn:resource_list_method
- proxies:proxyn:resource_lists_path
- proxies:proxyn:resource_lists_path_xcap
- proxies:proxyn:resource_lists_poll_time
- proxies:proxyn:resource_list_use_sip_credentials
- proxies:proxyn:resource_lists_user_name
- proxies:proxyn:resource_lists_password
- proxies:proxyn:xcap_oma_auid
- system:webdav:ignore_versioning.

For more information, see the “Configuring an XCAP Server for Resources Storage and Presence” manual.

Resources for Privacy Rules

The XMPP roster and the remote storage (if they exist) may include privacy rules (a privacy list or a black list and white list).

If the remote storage source holds a privacy list, you should specify its name in proxies:proxyn:privacy_server_filename.

When the user initially enables the corresponding account, any rules already set up in the storage for that account (in the local or remote storage for SIP, or on the XMPP server for XMPP) are pulled into Bria.

When the user creates a privacy rule, that rule is stored in the privacy list for each account that is currently enabled. So a rule may be added to more than one privacy list.

2.23 Shortcut Keys

Bria *for Windows* supports shortcut keys for several functions. Default key combinations are defined, but you can change these definitions, if desired.

2.24 User Experience

This group of settings let the user change the behavior of the Bria GUI.

Also look at the settings in “Feature Enabling: Enabling Other Features” on page 9.

2.25 Video

These settings provide controls for video quality.

2.26 Voicemail – MWI Notification

This group of settings let you configure Bria to subscribe to your voicemail server to receive notification that messages are waiting for the user. To use MWI, you must have a voicemail server that supports MWI.

MWI is set up in each account, that is, in the proxies:proxyn settings.

Receiving MWI Information

MWI subscription can be performed using SIP subscriptions or via MWI NOTIFY (implicit subscription).

- To use SIP subscriptions, set proxies:proxyn:subscribe_to_message_waiting to 1 and set the subscription parameters via the proxies:proxyn:message_waiting_<xx> settings.
- To use MWI NOTIFY, set proxies:proxyn:subscribe_to_message_waiting to 0. Bria will not subscribe to your voicemail server. Whenever Bria receives an MWI NOTIFY, it will handle it as per RFC 3842.
- To disable MWI, set proxies:proxyn:subscribe_to_message_waiting to 0.

Connecting to the Voicemail Server

If you support MWI, you can make the MWI icon clickable. To do so, enter the voicemail server URL in proxies:proxyn:voicemail_url.

2.27 Voicemail – Send to Voicemail

You can configure Bria to automatically send unanswered phone calls to voicemail. (Other call handling features are described in “Voicemail – MWI Notification” on page 15).

There are two ways to send to voicemail, using a 486 SIP response or using a 302 SIP response.

To configure for “send to voicemail”, set these settings in proxies:proxyn:

Option for “Send to voicemail”	forward_no_answer	forward_no_answer_uri	forward_no_answer_after_in_secs
Disabled	0	Empty	Ignored
Using 486	1	Empty	As desired
Using 302	1	The phone number for sending to voicemail	As desired

Note that there are some drawbacks to enabling client-side send-to-voicemail. Firstly, the Bria client will probably not handle redirects as well as your voicemail server. For example, in Bria voicemail, if Bob forwards to Alice and Alice does not answer, the next forward will be to Alice’s voicemail; the call will not be directed back to Bob’s voicemail.

Secondly, the Bria configuration may conflict with the corresponding settings on your voicemail server.

Forwarding Calls

The “forward_always_<xx>” and “forward_busy_<xx>” settings are typically set at runtime by the user, not through remote provisioning.

2.28 Web Browser Configuration

You can add up to three web pages. Each page will appear in a tab in the Resources panel alongside Contacts, History and so on.

2.29 Workgroup

You can configure Bria to display information about users in a workgroup. Only Bria *for Windows* supports workgroup. Workgroups implement functionality also often associated with BLF (Busy lamp field) and BLA (Bridged line appearance).

A workgroup is a group of people who work together. Via the Bria Workgroup window, members of a workgroup can monitor each others' calls, pick up on behalf of another member, and join an established call.

Workgroups can be set up in two ways:

- In server mode by integrating with an RLS application. In this mode, workgroups can be set up through remote provisioning or they can be set up by each user, on the Account > Presence tab.
- In peer-to-peer mode. In this mode, each Bria endpoint subscribes to other Bria endpoints. The feature is set up entirely within each individual Bria; there is no server component. Peer-to-peer workgroups are set up by each user; they cannot be set up through remote provisioning.

In both modes, ach member of the workgroup can be set up as:

- A regular member: every member monitors and is monitored by everyone else.
- Or as a supervisor: the supervisor monitors but is not monitored by other members.

Configuring in RLS Mode

In RLS mode, workgroups are implemented through support of dialog events (RFC 4235) and through subscription to a "resource list server" (RLS) in accordance with RFC 4662. The workgroup feature uses full updates (not partial updates) for dialog events.

The server application (your PBX that includes workgroups or the workgroup application) must support RFC 4235 and RFC 4662. Bria does not support resource list subscriptions for the "presence" event package.

How Workgroup Works

Here is a typical implementation. The RLS application is set up with one or more resource lists. Each list has its own URL. Each list contains the URIs (extensions) of people who are considered to be in a workgroup and can therefore monitor each other.

On the Bria side, each user is set up with the URI of the resource list they belong to. Each user is also set up to allow monitoring by other users.

When the SIP account becomes registered, Bria automatically contacts the RLS with the URL of the specified list. The RLS sends out subscription requests to all the URIs in the list. Each online user automatically responds to the request. When responses are received, the RLS sends status information to the requesting user.

When all the "online" (SIP account is registered) users in the workgroup do this, the result is that each user is able to monitor the activity of every other online member of the list.

One variation on this setup is for supervisors. The setup is identical except that the supervisor is not set up to allow monitoring by other users. When the supervisor goes online, their requests to monitor other people in the list will be accepted, but requests from other people to monitor that supervisor will be blocked. The result is that the supervisor is able to monitor the activity of everyone in the list but no-one can see the supervisor.

How to Set up

1. On the RLS application, create the resource list or lists and add the appropriate people. Each list has a name such as "sip:2000@mydomain.com" or "sip:salesgroup@mydomain.com".

2. Decide which account workgroup will work on. Remember that the first account is proxy0, the second account is proxy1, and so on.

3. Provision each user as follows:

Setting	Value for “Regular” Member	Value for Supervisor
feature:accounts:defaultForWorkgroup	0 (for example)	0 (for example)
proxies:proxyn:workgroup_type	0	0
proxies:proxyn:workgroup_subscription_AOR	The workgroup URL	The workgroup URL
proxies:proxyn:allow_dialog_subscriptions	1	0
feature:workgroup:show_on_start	<as desired>	<as desired>