




# **Bria 3 Configuration Guide**

## ***Retail 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

© May 2010 CounterPath Corporation. All rights reserved.

This document contains information proprietary to CounterPath Corporation, and shall not be used for engineering, design, procurement, or manufacture, in whole or in part, without the consent of CounterPath Corporation.

CounterPath and the  logo are trademarks of CounterPath Corporation.

The content of this publication is intended to demonstrate typical uses and capabilities of the Bria softphone application from CounterPath Corporation. Users of this material must determine for themselves whether the information contained herein applies to a particular IP-based networking system.

CounterPath makes no warranty regarding the content of this document, including—but not limited to—implied warranties of fitness for any particular purpose.

In no case will CounterPath or persons involved in the production of this documented material be liable for any incidental, indirect or otherwise consequential damage or loss that may result after the use of this publication.

Windows, Windows Vista, Active Directory, and Outlook are registered trademarks of Microsoft Corporation in the United States and other countries.

This manual corresponds to Bria version 3.0.

# Contents

About Configuration .....	2
Configuration Settings by Topic .....	3
Account Credentials .....	3
Account Setup .....	3
Audio Quality .....	4
Codec Usage .....	4
Dial Plan .....	6
Directory .....	12
DTMF .....	13
Encryption (Call Security) .....	13
Feature Enabling at the Account Level .....	14
Feature Enabling: Enabling Other Features .....	15
File Transfer .....	15
License .....	15
MWI Notification .....	16
Network .....	17
Presence .....	18
QoS .....	19
Resources .....	19
User Experience .....	19
Video .....	19
Voicemail: “Send to Voicemail” .....	20
Workgroup .....	20
Zero-Touch Configuration .....	21
A Comparison to Bria 2.5 .....	22



# About this Manual

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 3.0 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:

- “Provisioning Bria *Retail Edition*”, which describes the mechanism for configuring the features.
- The Bria Settings reference documentation (a Microsoft® Excel® document). The Bria Settings reference documentation provides detailed information on settings that may only be mentioned by name in this configuration manual.

# 1 About Configuration

## Bria Settings

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

- Configure Bria for the environment (network and so on) in which it will work.
- Configure Bria for server-side functions you support, such as WebDAV storage.
- Configure how some Bria 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 QoS for some users and disable it for others.

## Bria and Multiple Accounts

Bria supports up to ten accounts. However, in discussions in this manual, it is usually assumed that you will have only one SIP account and, optionally, one XMPP account.

## 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.

You can read a topic, then consult the Bria 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

For information on these settings, see “*Provisioning Bria Retail Edition*”.

### 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. proxies:proxyn:xmpp\_priority 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.

## 2.3 Audio Quality

These settings provide controls for audio quality.

## 2.4 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 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 panel in the Preferences > Audio Codecs or Preferences > Video Codecs tab.

### License Count

Each codec may have a limit to the number of simultaneous calls that can be made using that codec – in other words a limit to simultaneous use of a codec.

The built-in limit for royalty-bearing codecs is 2. There is no limit for non-royalty-bearing codecs.

You can restrict the codecs available by assigning a value to the `codecs:<codec name>:license_count` setting. To disable a codec entirely, assign a value of 0. If you assign a value that is higher than the built-in value, the value you assign is ignored.

For a limited-use codec, once the usage limit has been reached, that codec will not be offered in negotiation until the “in-use” count drops, for example, when one phone call ends.

Note that whether a codec is enabled and whether it is within its license count are only two of the factors in whether it will be used for a call. The other factors are:

- Whether the codec is also enabled by the other party
- Whether it is in under the bandwidth limit of the local Bria computer.
- Its ranking in the SDP list (see below).
- How the codec is chosen (see below).

## Presenting Local Media Capabilities in SDP

For the incoming audio or video (the audio or video the other party sends), Bria advertises a list of codecs in the INVITE or 200 OK SDP.

- For the invite (the offer), this list is made up of the codecs that are enabled and that are under the bandwidth limit of the local Bria computer.
- For the 200 OK (the counter-offer), this list is controlled by the `media:sdp:specify_all_codecs_in_offer_answer` setting. False (the default) means the list is made up of the codecs in the invite that are in the bandwidth limit of the local Bria computer. True means the list is made up of all codecs that are enabled in the local Bria computer (not just those in the invite) and that are in the bandwidth limit of the local Bria computer.



The codecs are prioritized within that list, with preferred codecs appearing first, based on the number each codec is assigned in codecs:<codec name>:priority.

## Handling the Media Capabilities of the Other Party

For outgoing audio or video (the audio or video you send the other party), there are two ways to configure Bria:

- Let Bria determine the codecs to use for each call. This is the default.  
From the list of codecs that advertised by the other party in their SDP, that are enabled on the local Bria computer and that are under the bandwidth limit of the local Bria, Bria chooses the codec with the best sound, based on the network conditions.  
To set up for this scenario, set system:network:honor\_first\_codec to false.
- Use the other party's preferred codec.  
From the list of codecs that advertised by the other party in their SDP, that are enabled on the local Bria computer and that are under the bandwidth limit of the local Bria, Bria chooses the codec that is listed first.  
To set up for this scenario, set system:network:honor\_first\_codec to true.

## 2.5 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 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.
- 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.

### Quick Reference to the Dial Plan Settings

For information on the individual Bria settings that relate to the dial plan:

- `digit_map`. See “Dial Plan Syntax”, below.
- `digit_map_timer_critical`. See “Timers” on page 8.
- `digit_map_timer_partial`. See “Timers” on page 8.

## The Default Dial Plan

The default dial plan is:

```
#n\a\a.T;match=1;prestrip=2;
```

where #n is the account prefix (#1 for the first account in the list (proxy0), #2 for the second account (proxy1), and so on).

If the input is the account prefix and the number, then the Account for this dial plan is selected. The account prefixed is stripped from the number before the call is placed.

If all Accounts use this dial plan, then the behavior is as follows: if the input includes the account, then that account is used. In other words, you can force selection of a specific account by including the account prefix. If the input does not include #n, then the default account is used.

## How Dial Plans Are Used

The input (what the user types, selects or drags onto the display) is processed as follows:

### Cleanup

This step is not part of the dial plan: it is always performed even when there is no dial plan.

Input is cleaned up by removing spaces and dashes, open brackets, and close brackets. Cleanup allows Bria to support calls placed using contacts from a contact list, including Microsoft® Outlook®.

### Matching

The input is compared to the patterns defined by the dial plan for each enabled account. Each account has one dial plan, and each dial plan has one or more patterns.

- When a match is found between the input and the pattern, the account that this pattern belongs to is selected and the transformation for this pattern is performed.
- If no match is found, the default account is selected and no transformation is performed. (The default account is the enabled account that appears first in the list in the Account Settings window.)

For details on matching see “How the Input Is Processed” on page 9.

## Transformation

The selected transformation is performed.

## Place Call

Then the call is placed using the transformed input.

# Dial Plan Syntax

The dial plan establishes the expected patterns of characters for a telephone number or SIP address, and allows for modification (transformation) of input based on the match to a pattern.

The dial plan is defined for each account in proxies:proxyn:digit\_map, where n is the account number.

The dial plan has the following syntax:

```
pattern[[pattern[...]];match=1;<transformation>=<value>;[match=2;<transformation>=<value>;[...]]
```

Where

- Items in [ ] are optional.
- Pattern: the pattern that will be matched. Each pattern is separated by a | pipe. The pipe is optional after the last pattern. Each pattern is implicitly numbered, starting from 1.
- Match and Transformation: A pair that identifies the pattern number to compare to the input, and the transformation or transformations to perform on the input when a match is obtained. The transformation is optional (meaning the input that matches this pattern is not transformed).

"match=" is a literal. "n" identifies the pattern. "transformation=" is replaced by a keyword, see below.  
"value" is replaced by a value.

Spaces are allowed only in the <value> items.

Remember that dial plans are applied after the input has been cleaned up (page 6)!

## Example

```
\a\a.T|xxxxxxxxxx;match=1;prestrip=2;match=2;pre=8;
```

where:

- \a\a.T is the first pattern.
- xxxxxxxxxxxx; is the second pattern.
- match=1;prestrip=2; is the first match-transformation pair.
- match=2;pre=8; is the second match-transformation pair.
- Some elements use the back slash \ character. If you are defining a pattern via remote provisioning (that is, in an HTTP response), you must enter two backslashes, because the Bria provisioning software interprets one backslash as an escape key.

## Pattern

### Valid Content

The content for a pattern follows the digit map rules of RFC 2705, supplemented by the rules for regular expressions. Where there is an overlap between the digit map and regular expression rules, the digit map rules apply. For this reason, there are some special cases, included in the table below.

The following table describes the most common elements. As mentioned, all regular expression elements are supported.

Some elements use the back slash \ character. If you are defining pattern a via remote provisioning (that is, in an HTTP response), you must enter two backslashes, because the Bria provisioning software interprets one backslash as an escape key.

Element	Origin	Description
0 1 2 3 4 5 6 7 8 9	Literals	Literal digits, used as is.
# * a to z	Literals	Literal characters, used as is. Special cases: <ul style="list-style-type: none"> <li>The literal x character is represented by \x.</li> <li>The literal t character is represented by \t.</li> </ul>
x	Digit map rules	Wildcard for any single digit, 0 to 9.
\a	Regular expression rules	Wildcard for any single alphanumeric character.
[digit-digit]	Regular expression rules	A digit within the specified range.
[character-character]	Regular expression rules	A character within the specified range.
[digit1, digit2, digit3]	Regular expression rules	One of the characters in the collection.
.	Digit map rules	Repeat the last element 0 or more times. Use of this element results in a pattern with "minimum requirements". For example, xxxx. means repeat the last x 0 or more times, which means this pattern matches three or more digits (not four or more digits)! Use of this element results in a pattern with "minimum requirements".
T	Digit map rules	<p>A timeout period will take place before automatic dialing starts. The typical timer value is 4 seconds, but a different value can be set in the setting proxies:common:digit_map_timer_critical.</p> <p>The T timer forces Bria to wait after a match is made. This timer should always be included in the following situations:</p> <ul style="list-style-type: none"> <li>Any pattern that uses the . (dot). For example, if the pattern is xxxx. then adding a timer allows the user to type three or more digits. If there is no timer, then Bria makes the match as soon as the user types three digits.</li> <li>Any dial plan that has two patterns that are similar in elements but different in length. For example, if one pattern is xxx and the other pattern is xxxxxxx, then adding the timer allows the user to continue typing past three digits, in order to get a match on the second pattern.</li> </ul> <p>In this situation, the T timer should be included in the shorter pattern.</p>

### Timers

There are two timers, the T timer and the long timer. These timers are used in input comparison, as described in "How the Input Is Processed" on page 9.

Both timers can be configured via the Bria settings:

- T timer is set in proxies:common:digit\_map\_timer\_critical. The default value is 4000 milliseconds (4 seconds).
- The long timer is set in proxies:common:digit\_map\_timer\_partial. The default value is 20000 milliseconds (20 seconds).

### Transformation Keywords

Keyword	Description
prestrip	Strip the first n characters from the input before placing the call.
poststrip	Remove n number of characters from the end of the input before placing the call.
pre	Add the specified prefix to the input before placing the call.
post	Attach the specified postfix to the input before placing the call.
replace	Replaces the input with the specified string before placing the call.

### Order of Transformations

These transformations are always performed in the following order (the order in which the transformations are entered in the dial plan is not significant):

prestrip > poststrip > pre > post > replace

## How the Input Is Processed

### Comparing Input to the Dial Plan Patterns

The input is compared to each dial plan in turn, starting with the first listed account. The process is slightly different depending on how the call is placed, as described in the table below.

It is possible for the same input to get matched to different dial plans depending on whether the input is entered on the fly or dragged. It is important to keep this in mind when designing dial plan patterns.

## Results of the Comparison

How Call Placed	Type of Match	Meaning of Match	Result If User Presses Enter or Call	Result if User Stops typing
User is typing	Partial match	The characters typed so far follow the pattern but there are not yet enough characters for a pending or complete match.	The default account is used. No transformation is performed.	If the user stops typing for the long timer length (usually 20 seconds), then the default account is selected. No transformation is performed on the characters typed so far.
	Pending match	One of the following: <ul style="list-style-type: none"> <li>The pattern has no . (dot) but does have the T timer, and there is a perfect match.</li> <li>The pattern has a . (dot) and the T timer, and the minimum requirements are met.</li> </ul>	This pattern's account is immediately selected and the transformation is performed.	If the T timer expires, this pattern's account is selected and the transformation is performed.
	Complete match	One of the following: <ul style="list-style-type: none"> <li>The pattern has no . (dot) and no T timer, and there is a perfect match.</li> <li>The pattern has a . (dot) but does have the T timer, and the minimum requirements are met.</li> </ul>	This pattern's account is immediately selected and the associated transformation is performed.	This pattern's account is immediately selected and the associated transformation is performed.
	No match	The characters typed do not match the patterns for any dial plan.	The default account is selected and no transformation is performed.	Nothing happens even after the T timer and long timer have expired
Dragged or selected	Complete	The input is an exact match for the pattern.	The account is selected and the associated transformation is performed	
	No match	The input does not match the patterns for any dial plan.	The default account is selected and no transformation is performed.	

The default account is the first enabled account in the Account List, that is, the account with the lowest proxyn number (for example, proxy1 is lower than proxy2).

# Examples

## Example 1

```
\a\A.T|xxxxxxx.T;match=2;pre="9"
```

This simple example shows how to differentiate between a PSTN number and a SIP address, and to how add a "9" dialing prefix only to the PSTN number.

## Example 2

```
3xxT|1xxxxxxxxxx|[2-9]xxxxxxxx|x.T;match=2;pre="9";match=3;
pre="91";match=4;prestrip=1;pre="9011"
```

3xxT	
	The first pattern is any three-digit number beginning with 3. No transformation. The assumption is that this is an internal extension. The timer forces Bria to wait after detecting a three-digit number beginning with 3, in case the user is actually dialing a local call starting with 3.
1xxxxxxxxxx	The second pattern is any eleven-digit number beginning with 1. Prefix with 9 and dial as is. The assumption is that this is a long-distance PSTN call within North America (within North America, all long-distance calls start with 1).
[2-9]xxxxxxxx	The third pattern is any ten-digit number beginning with a number other than 1. The assumption is that this is a local PSTN call in a ten-digit dialing zone.
+x.T;	The fourth pattern is a number of any length that begins with +, to indicate an international PSTN call from North America. Delete the +, prefix with 9011 (011 is the number to access an international line from North America).
match=2;pre="9";	For the second pattern, prefix 9 to access an outside line.
match=3;pre="91";	For the third pattern, prefix 9 and 1 to access an outside line and enter the long-distance code.
match=4;prestrip=1;pre="9011"	"For the fourth pattern, remove the + and prefix 9011 to access an outside line and enter the international code.

## Example 3

```
#1xxxxxxxxT|#19xxxxxxxx|xxxxxxxxT|9xxxxxxxx;match=1;prestrip=2;pre=9;match=2;prestrip=2;
match=3;pre=9;
```

#1xxxxxxxxT	The pattern is a dialing prefix followed by seven digits. The timer forces Bria to wait to allow a match to the second pattern. The #1 is stripped off and 9 is prepended to access an outside line.
#19xxxxxxxx	The pattern is a dialing prefix followed by a 9 and seven digits. The #1 is stripped off.
xxxxxxxxT	The pattern is seven digits. The timer forces Bria to wait to allow matching to the fourth pattern. 9 is prepended to access an outside line.
9xxxxxxxx	The pattern is a 9 and seven digits. The input is not transformed.

This example assumes that the dial plan belongs to the first account.

The dial plan is slightly trivial, because it does not cover all the situations that a dial plan should be designed for (local calls, long-distance calls, international calls, and so on for the locale).

However, the example does illustrate two ideas:

- Handling of the account prefix (#1), to deal with users who have upgraded from eyeBeam. These users may have been accustomed to dialing an account prefix to force eyeBeam to use a specific account.

Use of # to identify the account is now deprecated. The dial plan should be capable of determining the account to use for this number. However, since users may still be in the habit of entering the prefix, you may want to include this pattern to handle such a scenario.

- Distinguishing between a local seven-digit call in which 9 is not dialed (to access an outside line) and one in which 9 is dialed to access an outside line.

## 2.6 Directory

If you have set up an LDAP directory or Active Directory 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:
  - `polltime`
  - `search_on_demand`
  - `sizelimit`
  - `timeout`Read the information in the `search_on_demand` setting in the settings documentation for information on how these settings work together.
- 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:password`
  - `ldap:query`
  - `ldap:root`
  - `ldap:server`
  - `ldap:use_tls`
  - `ldap:username`For ADSI:
  - `adsi:root`



## 2.7 DTMF

This group of settings configures Bria to handle DTMF. DTMF will be sent using either:

- Out-of-band using 2833 DTMF packets
- Out-of-band using 2833 DTMF, with a fallback to in-band.
- In-band, by encoding the DTMF signal in the audio stream.

The preferred method is out-of-band. In-band is used only to deal with specific network situations, as described in the reference section for these settings.

## 2.8 Encryption (Call Security)

### About Encryption

Bria can be configured to support specific combinations of 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 certification 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.

## 2.9 Feature Enabling at the Account Level

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

- Audio call
- Video call
- IM
- Presence
- File transfer
- Workgroup (BLF)

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

### Minimum Configuration

Bria has rules relating to features on accounts. Because you are configuring accounts through provisioning, you are responsible for ensuring these rules are followed.

At least change the setting as follows:

- Set IM to disabled on all accounts, then enable it either on the XMPP account (if supported) or on one SIP account only.
- Set Presence to match IM.
- Set File Transfer to disabled on all accounts, then enable it only on the XMPP account (if supported). If XMPP is not supported, disable file transfer on all accounts.

If you do not change the settings' default value in this way, then for a while the setup you have configured will work. But the first time the user makes a change (even something as harmless as changing their display name) and then clicks **Apply** on the Accounts List, Bria will enforce these internal rules. At that point, the behavior of Bria will change, seemingly for no reason, resulting in confusion for the user.

For example, if you enable IM and presence on two SIP accounts, then it will be possible to establish presence subscriptions on either account. But when the user does something that triggers Bria to enforce the “only one account” rule, some subscriptions may terminate and the user will not understand why.

### Optional Configuration

If desired, you can impose further restrictions on use of phone calls and workgroup on different accounts. For example, you may want to implement a business rule that only Account 1 is used for phone calls. When changing the accounts to use for phone calls and workgroup, the following rules apply:

- For phone calls, an account must be either enabled for both audio and video, or disabled for both.
- Workgroup (BLF) can be enabled on one or more (or all) SIP accounts.

## 2.10 Feature Enabling: Enabling Other Features

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

- “File Transfer” on page 15
- “Directory” on page 12
- “MWI Notification” on page 16
- “Presence” on page 18
- “Voicemail: “Send to Voicemail”” on page 20.
- “User Experience” on page 19.

## 2.11 File Transfer

File transfer lets users send and receive files. .

To use XMPP for file transfer, 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.

To enable XMPP file transfer on the local client, set `feature:file_transfer:enable` to true.

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 or via the public server proxy.jabber.org.

## 2.12 License

### Provisioning the License

The license key can be provided to the client through remote provisioning. See “*Provisioning Bria OEM Edition*” 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.

### Revoking Licenses

Whether you provision licenses or users enter the license key manually, you can manage licenses by logging onto your account on the CounterPath store.

Note that to revoke a license, you must do so through the store. It is not enough to remotely provision an empty license key string the next time that the user logs on, because after the initial provisioning, the key is stored outside of settings and Bria reads it in that outside location.

## 2.13 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.

## 2.14 Network

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.

### 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. This group can be divided into several groupings:

- Keep alive: Settings to configure how keep-alive messages work.
- Port: Settings to configure the listening port. In the Settings reference documentation, start with the setting `proxies:proxyn:listen_sip_port`.
- SIP: One setting for rport usage.

### SIP Signaling

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

### RTP Session

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

### 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.

### SDP

This group of settings lets you configure how SDP session activity will be managed.

## 2.15 Presence

This group of settings lets you configure how presence is supported when presence is handled using SIMPLE on SIP accounts. For presence on XMPP accounts, no special configuration is required: presence subscriptions are always created for XMPP buddies.

If you are not supporting presence through SIP, make sure you disable presence on every SIP account.

If you are supporting presence through SIP and your users have several SIP accounts, you will typically enable presence on only one SIP account. Make sure you disable presence on the other SIP accounts.

If you support presence, you should also read “Resources” on page 19 for information on how Bria stores the presence information (buddy list) and privacy rules.

### **How 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.

## 2.16 QoS

This group of settings lets you configure the quality of service you offer, if applicable.

There are two types of services. The service to use depends on what your VoIP service provider supports:

- GQoS, which is available for audio and video.
- DSCP (also known as ToS), which is available for audio, video and signaling.  
In a network that has the default configuration, the recommended value for audio is 46, because “46” is the standard marking for audio.

Bria supports 802.1p QoS packet tagging. If you set up for QoS, Bria will include the specified information in the packets that it sends to the network provider. Whether the packet is delivered with the specified service depends on whether your broadband router and the network provider between you and the other party supports multiple transport services. In other words, whether each network provider reads the QoS information and prioritizes packet delivery based on the requested service.

## 2.17 Resources

Typically the contact list is stored locally. Privacy and presence information associated with a SIP account are also typically stored remotely. Privacy and presence information associated with an XMPP account are always stored on the XMPP server.

Bria *for Windows* also includes support for MicroSoft Outlook® integration. Typically, you do not configure Bria to use Outlook. Instead, you set storage to local and then let users choose to switch to use their Microsoft Outlook contacts.

To store the contact list and SIP information remotely using WebDAV or XCAP, see the “Configuring for Remote Storage of Resources” manual.

If you support both local and remote storage, Bria continually synchronizes the local and remote lists.

## 2.18 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 15.

## 2.19 Video

These settings provide controls for video quality.

## 2.20 Voicemail: “Send to Voicemail”

You can configure Bria to automatically send unanswered phone calls to voicemail. (Other call handling features are described in “MWI Notification” on page 16).

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	Ignored
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\_<xx>” settings are typically set at runtime by the user, not through remote provisioning.

## 2.21 Workgroup

You can configure Bria to display information about users in a workgroup. Workgroup functionality is implemented through support of dialog events (RFC 4235) and through subscription to a “resource list server” in accordance with RFC 4662. The full RFC 4662 format is followed, which means that for any given monitored extension, Bria reveals each separate appearance of that extension and its activity.

You must configure for workgroups as follows:

- On your SIP server, create users.
- On your SIP server, create workgroups and add users to the desired workgroups.
- In Bria, set proxies:proxyn:workgroup\_subscription\_AOR to the URL where the client can subscribe to the workgroup. Set this setting only in the default account.
- In Bria, set proxies:proxyn:allow\_dialog\_subscription to allow or prohibit users in a workgroup monitoring each others’ calls.

When the user chooses to view workgroup and if the workgroup\_subscription\_AOR for any given proxy (account) specifies a URL, then Bria immediately registers with the SIP registrar and if the workgroup\_subscription\_AOR for any given proxy (account) specifies a URL, then Bria automatically subscribes to the workgroup. If the subscription succeeds, the user will be able to display the Workgroup window on the softphone.



## 2.22 Zero-Touch Configuration

These settings control whether zero-touch configuration is enabled. When this configuration is enabled, Bria automatically detects the audio and video devices connected to the Bria computer, automatically detects the type of connection, and displays device configuration messages.

### Bandwidth Detection

Zero-touch configuration includes a feature that lets Bria calculate the connection for local Bria's computer, by determining how long it takes to download a file of a fixed file: the faster the download, the better the connection is assumed to be.

If you decide to support this feature (`zero_touch_bw_enabled=true`), you must provide a file of size 100 to 200 KB, at the specified URL. You must configure Bria for this URL by completing the setting `auto_bandwidth_url`.

If you do not want to provide this file, you must disable the feature (`zero_touch_bw_enabled=false`). The user will be able to specify their connection type on the Preferences > Advanced > Network panel.

### Devices

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.

# A Comparison to Bria 2.5

## A.1 Summary

Following is a summary of major differences in settings between Bria 2.5 and Bria 3.0.

### New Settings

- Feature enabling per account. The setting `proxies:proxyn:enabled_features` let you enable features on a specific account, in order to match your internal business rules or network setup.
- Workgroup. The setting `proxies:proxyn:allow_dialog_subscriptions` lets you control whether other users in a workgroup will be able to monitor the local user's call activity.
- Directory using Active Directory. Bria now supports connecting to an external directory using Active Directory as well as LDAP. A new group of settings have been added, `feature:adsi:<setting name>`. The setting names are sometimes identical to the LDAP settings names, but sometimes there are small differences, such as `displayNameKey` (LDAP) versus `displayName_Key` (Active Directory), so be careful. See the settings reference documentation for the complete list of settings.
- Resource lists. Some settings that were previously shared by WebDAV and XCap are now split into separate settings.
- RTP inactivity timers. The Preferences > Advanced panel now includes the RTP timers. The descriptions for these settings have been improved.
- For other new settings, see the detailed list below.

### Differences in Configuration of Features

- Advertisement: the URL for the advertisement panel cannot be provisioned; it must be included in your brand at build time.
- Alerts: the setting `ui:general:call_immediately_on_selection` has moved to `ui:call:call_immediately_on_selection`.
- Anonymous calling method: `proxies:proxyn:anonymous_calling_method` is not supported. Anonymous calling is always supported via a SIP message.
- Call security (call encryption): There are fewer options. Read the revised information for the setting .
- Diagnostics: `diagnostics` is controlled by different settings, which should always be manipulated by the user through Help > Troubleshooting.
- DTMF: DTMF via INFO is no longer supported. Read the revised information for the setting `system:dtmf:enabled`.
- MWI indicator: the setting `feature:availability:show_mwi_always` is not supported. The MWI icon always shows.
- Resources - Global Contact List: the key setting `storage:contact_list_storage:resource_list_method` has a new option "outlook" to support integration with Microsoft® Outlook®. See the settings in the topic "Resources - Global Contact List" in the settings reference document.
- Resources - Individual Accounts: privacy lists are not supported in Bria 3.0, therefore the setting `proxies:proxyn:privacy_server_filename` is not applicable.
- Ringer volume: the ringer volume cannot be configured.
- UI domain: none of the settings in the "ui" domain are supported except for those that are exposed on the Preferences panel.

## Features not Configurable

The following features cannot be enabled or disabled through provisioning. These features are permanently enabled; if you need to disable any of these features, you may want to consider obtaining a custom brand; contact CounterPath.

- Call recording
- Conference call
- Hiding panels in the Preferences window.
- IM Archive
- Importing sounds
- Letter-to-digits mode
- Menus: Hiding an individual menu item.
- Workgroup (BLF)

## Features not Supported

The following features are not supported in Bria 3.0, so the related settings are not applicable:

- Call screening.
- File transfer via content indirection.
- Firewall traversal The settings relating to configuration of the firewall traversal method have changed. See the new settings in the topic "Network SIP - Firewall Traversal" in the settings reference document.
- Firewall traversal: XTunnels is no longer supported, therefore the related settings are not applicable.
- Ringtones: the ability to allow the user to assign ringtones to an individual contact.
- SIP Handling: the ability to accept SIP responses with custom headers is not supported.
- SIP Handling: the ability to configure the code or reason string to use in a SIP response.
- Web browsers.

## A.2 Details

Status	Domain	Section	Setting	Topic	Subtopic	Comment
Revised	proxies	proxyn	domain	Account credentials		Description for XMPP changed.
Revised	proxies	proxyn	username	Account credentials		Description for XMPP changed.
Deleted	feature	advertisement_module	url	Advertisement		Custom builds only. URL must be set at build time
Deleted	proxies	proxyn	anonymous_calling_method	Anonymous Calling		SIP is always used.
Deleted	proxies	proxyn	security_incoming_level_max	Call Security		Options are simplified; see the Excel document.
Deleted	proxies	proxyn	security_outgoing_fallback	Call Security		
Deleted	proxies	proxyn	security_outgoing_tls	Call Security		
Deleted	feature	call	custom_announcementn	Custom Announcement		Feature is not supported
Deleted	system	diagnostics	enable_logging	Diagnostics	Enabling	Diagnostics should be controlled through GUI
Deleted	system	diagnostics	file_size	Diagnostics	Enabling	There is no limit
Deleted	system	diagnostics	folder	Diagnostics	Enabling	The default is the user's home folder
Deleted	system	diagnostics	number_of_files	Diagnostics	Enabling	There is no limit
Deleted	diagnostics	log_level	<module>	Diagnostics	Level	Diagnostics should be controlled through GUI
Deleted	system	diagnostics	log_level	Diagnostics	Level	Diagnostics should be controlled through GUI
New	feature	adsi	<setting name>	Directory	Active Directory	
Deleted	rtp	2833	enabled	DTMF		Description changed to reflect that INFO is no longer supported.
Deleted	rtp	2833	packet_time_in_ms	DTMF		Setting is not supported
Deleted	rtp	2833	payload_number	DTMF		Setting is not supported
Deleted	ui	call	play_letter_dtmf	DTMF		DTMF is played when a letter or number is pressed.
Deleted	<type>	<menu name>	Hide	Feature Enabling		Menus must be branded out in a custom build
Deleted	feature	Call	enable_hangup	Feature Enabling		The user can always hang up a call
New	proxies	proxyn	enabled_features	Feature Enabling		
Deleted	feature	message_archive	enable	Feature Enabling	IM Archive	Must be branded out in a custom build
Deleted	feature	call	letter-to-digit	Feature Enabling	Letter-to-digits	Must be branded out in a custom build
Deleted	feature	call	allow_conference_on_gui	Feature Enabling	Phone Calls	Conference call must be branded out in a custom build

Status	Domain	Section	Setting	Topic	Subtopic	Comment
Deleted	feature	call	enable_recording	Feature Enabling	Phone Calls	Must be branded out in a custom build
Deleted	feature	contact	assign_ringtone	Feature Enabling	Ringtones	Feature is not supported.
Deleted	feature	audio	allow_import_sounds	Feature Enabling	Sounds	Feature is not supported.
Deleted	feature	file_transfer_content_indirection	enable	File Transfer	Content Indirection	Feature is not supported.
Deleted	feature	file_transfer_content_indirection	maximum	File Transfer	Content indirection	
Deleted	proxies	proxyn	send_file_server	File Transfer	Content Indirection	
Deleted	feature	options_pages	<name>	GUI Customization		Preference panels must be branded out in a custom build.
Deleted	feature	help_menu	has_license_key	License		Menu item always appears.
Deleted	menu_urls	file	customn	Menu Customization		Feature is not supported.
Deleted	feature	availability	show_mwi_always	MWI Notification		MWI always shows
Revised	feature	availability	subscribe_to_message_waiting	MWI Notification		Improved description
New		sdp	use_old_style_hold	Network	SDP	
Deleted	proxies	proxyn	override_stun_server	Network SIP	Firewall - Relay Server	Firewall traversal is done through different settings; see the Excel document.
Deleted	proxies	proxyn	xtunnels_enabled	Network SIP	Firewall - Relay Server	
Deleted	proxies	proxyn	xtunnels_password	Network SIP	Firewall - Relay Server	
Deleted	proxies	proxyn	xtunnels_server	Network SIP	Firewall - Relay Server	
Deleted	proxies	proxyn	xtunnels_use_sip_credentials	Network SIP	Firewall - Relay Server	
Deleted	proxies	proxyn	xtunnels_username	Network SIP	Firewall - Relay Server	
New	proxies	proxyn	firewall_server_auth_realm	Network SIP	Firewall Traversal	
New	proxies	proxyn	firewall_server_password	Network SIP	Firewall Traversal	
New	proxies	proxyn	firewall_server_username	Network SIP	Firewall Traversal	
New	proxies	proxyn	firewall_traversal_mode	Network SIP	Firewall Traversal	
New	proxies	proxyn	firewall_traversal_server	Network SIP	Firewall Traversal	

Status	Domain	Section	Setting	Topic	Subtopic	Comment
Deleted	proxies	proxyn	ice_enabled	Network SIP	Firewall Traversal - ICE	
Deleted	proxies	proxyn	send_internal_ip_address	Network SIP	Firewall Traversal - STUN	
Deleted	proxies	proxyn	stun_server	Network SIP	Firewall Traversal - STUN	
Deleted	system	stun	total_retransmit_packets	Network SIP	Firewall Traversal - STUN	
Revised	rtp	inactivity	rtcp_timer_in_ms	Network SIP	RTP Session	Description revised; these settings are not exposed in the Preferences window
Revised	rtp	inactivity	rtp_timer_in_ms	Network SIP	RTP Session	
Revised	rtp	inactivity	timer_enabled	Network SIP	RTP Session	
Revised	proxies	proxyn	proxy	Network SIP	SIP signaling	Description revised for XMPP
Deleted	availability		no_notes_for_base_states	Presence		Notes are always included
Deleted	Feature	custom_login	preserve_uppercase_settings	Provisioning		The case of the setting names is no longer an issue; so "SettingName" is identical to "settingname"
New	feature	outlook	password	Resources	Global Contact List	
New	feature	outlook	profile	Resources	Global Contact List	
New	feature	outlook	softphonefield	Resources	Global Contact List	
New	System	contact_list_storage	contacts_server_filename	Resources	Global Contact List	
Revised	System	contact_list_storage	resource_list_method	Resources	Global Contact List	Description revised to include Outlook
Revised	System	contact_list_storage	resource_lists_path	Resources	Global Contact List	Revised to clarify that this setting is now used only for WebDAV
New	System	contact_list_storage	resource_lists_path_xcap	Resources	Global Contact List	
Revised	proxies	proxyn	resource_lists_path	Resources	Individual Accounts	Revised to clarify that this setting is now used only for WebDAV
New	proxies	proxyn	resource_lists_path_xcap	Resources	Individual Accounts	
Deleted	proxies	proxyn	privacy_server_filename	Resources	Individual Accounts	Privacy is not supported.
Deleted	system	screen_calls	enable	Screen Calls		Feature is not supported.

Status	Domain	Section	Setting	Topic	Subtopic	Comment
Deleted	system	screen_calls	reg_exp	Screen Calls		
Deleted	feature	call	response_code_dnd	SIP Handling		Custom codes are not supported.
Deleted	feature	call	response_code_no_resource	SIP Handling		
Deleted	feature	call	response_reason_blocked	SIP Handling		
Deleted	feature	call	response_reason_dnd	SIP Handling		
Deleted	feature	call	response_reason_no_resources	SIP Handling		
Deleted	feature	call	sip_response_code_blocked	SIP Handling		
Deleted	feature	fac_response	custom_header	SIP Handling		
Deleted	system	diagnostics	enable_minidump	Testing		Minidump is not supported
Deleted	ui	contact	status_alert	User Experience	Alerts and Sounds	Alert popup appears and the alert options appear in the Preferences > Alerts.
Deleted	audio	tuning_wizard	ringer_volume	User Experience	Audio Quality	Volume cannot be controlled
Deleted	tuning	tuning_wizard	ringer_volume	User Experience	Audio Quality	Volume cannot be controlled
Deleted	ui	call	auto_answer_allow_delay	User Experience	Auto answer	Delay is handled differently
Deleted	feature	contact	methods	User Experience	Contacts	All methods appear by default.
Deleted	feature	contact	use_semicolon_to_separate_email_addresses	User Experience	Contacts	Email integration is not supported
Deleted	ui	contact	default_group_changeable	User Experience	Contacts	The group name is not changeable.
Deleted	ui	contact	double_click_action	User Experience	Contacts	Double-click is not supported.
Deleted	ui	contact	max_address_length	User Experience	Contacts	There is no limit
Deleted	ui	contact	max_number_of_contacts	User Experience	Contacts	There is no limit
Deleted	ui	contact	nameless_group	User Experience	Contacts	The group is named "Ungrouped"
Deleted	ui	contact	use_last_group	User Experience	Contacts	The last group is used
Deleted	ui	contact	use_subtype	User Experience	Contacts	Subtypes are not supported
Deleted	system	general	never_show_domains	User Experience	General	Domains never show
Deleted	ui	call	context_menu	User Experience	General	The user can right-click for the menu.
Deleted	feature	im	limit_message_size	User Experience	IM	There is no limit
Deleted	feature	im	only_allow_im_to_online_buddy	User Experience	IM	IM is allowed to offline buddies

Status	Domain	Section	Setting	Topic	Subtopic	Comment
Deleted	ui	im	message_new_window	User Experience	IM	IM tabs are not supported
Revised	ui	Im	popup_on_new_session	User Experience	IM	This setting is now exposed in a different way on the GUI; it is included in the events list on the Alerts tab, as "For IM".
Deleted	ui	skinux	current_language	user experience	Language	Languages are handled through a different mechanism
Deleted	system	license	key	License		The license key is no longer handled in this way; see the Bria 3.0 Provisioning Guide for more information
Deleted	feature	custom_login	display_dialog_after_signout	User Experience	Login	The login dialog does not appear after logout
Deleted	feature	audio	mute_speaker_dtmf	User Experience	Phone Calls	DTMF is heard
Deleted	feature	call	letter_to_digit_default	User Experience	Phone Calls	Letter-to-digit mode remains enabled until turned off manually.
Deleted	feature	call	only_allow_call_to_online_buddy	User Experience	Phone Calls	Calls are allowed to offline buddies
Deleted	feature	contact	always_ignore_domain	User Experience	Phone Calls	The domain is ignored
New	ui	call	call_immediately_on_selection	User Experience	Phone Calls	
Deleted	ui	call	display_additional_callerid	User Experience	Phone Calls	Additional information is always displayed when available
Deleted	ui	call	end_timeout	User Experience	Phone Calls	This value is not configurable
Deleted	ui	call	failed_timeout	User Experience	Phone Calls	This value is not configurable
Deleted	ui	call	transfer_timeout	User Experience	Phone Calls	This value is not configurable
Deleted	ui	general	call_immediately_on_selection	User Experience	Phone Calls	Replaced by setting in ui domain
Deleted	ui	custom_message	max_length	User Experience	Presence	No maximum
Deleted	ui	default	status	User Experience	Presence	Values cannot be suppressed.
Deleted	ui	contact	must_have_contact_to_block	User Experience	Privacy	Privacy is not supported
Deleted	ui	privacy	glob_accept_contact_from_contacts_only	User Experience	Privacy	Privacy is not supported
Deleted	ui	main_window	confirm_exit	User Experience	Prompts	There is no prompt
Deleted	ui	main_window	confirm_exit_always	User Experience	Prompts	There is no prompt
Deleted	ui	main_window	show_prompt_on_close	User Experience	Prompts	There is no prompt
Deleted	feature	sys_tray	show_volume_control	User Experience		The volume control is never shown
Deleted	ui	availability	status	User Experience	Presence	The current status is not saved at exit



Status	Domain	Section	Setting	Topic	Subtopic	Comment
New	video	performance	restricted_mode_enabled	Video		
Revised	proxies	proxyn	forward_no_answer_uri	Voicemail	Send to Voicemail	Improved description
Deleted	feature	browser_modules	urln	Web Browser		This feature is not supported.
Deleted	feature	browser_modules	use_postn	Web Browser		
Deleted	feature	embedded_browser	additional_header	Web Browser		
Deleted	feature	workgroup	enable	Workgroups (Busy Lamp Field)		Must be branded
New	proxies	proxyn	allow_dialog_subscriptions	Workgroups (Busy Lamp Field)		
New	system	network	connection_type	Zero-touch Configuration	Bandwidth	

