Bria 4 Provisioning Guide

OEM Deployments

CounterPath Corporation.
Suite 300, One Bentall Centre
505 Burrard Street Box 95
Vancouver BC V7X 1M3
Tel: 1.604.320.3344
sales@counterpath.com www.counterpath.com

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. 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.

This manual corresponds to Bria version 4.8.

Rev 2

Contents

About this Manual

This manual describes the *mechanism* of remote login and provisioning if you are implementing provisioning using your own provisioning server. It describes how to set up a server (or servers) for the remote login request and, optionally, the remote provisioning response and the remote upgrade feature of Bria.

- **Remote login request**: Controls access to the application; the softphone will not start until the user has logged in.
- **Remote provisioning response**: Configures the softphone remotely as part of the login process.
- **Remote upgrade feature**: Deploy upgrades of the software remotely.

This provisioning process applies, with very minor exceptions, to Bria 4 *for Windows* and Bria 4 *for Mac*.

Intended Audience

This manual is intended for:

> Service providers who have purchased a branded and/or customized version of Bria 4.

If you have purchased retail Bria from the CounterPath website, you should be reading the manual “Bria 4 Configuration Guide - Enterprise Deployments”.

This manual is intended to be read in conjunction with:

> “Bria 4 Configuration Guide - OEM Deployments” which describes the features that can be configured through remote provisioning.

1 About Provisioning

1.1 Provisioning Functions

Bria provisioning includes the following features:

Login request: Controlling access to the VoIP service through a remote login.

License key provisioning: The ability to provide a license key remotely.

Feature provisioning response: Updating the Bria configuration (changing the default settings). Bria can be configured differently for each user. This feature is optional and is handled as part of the response to the login request ("Response Step" on page 9).

Upgrade: Providing upgrades to the executable by making new versions of Bria available to each Bria installation to download. This feature is optional. ("Remote Upgrades" on page 11).

1.2 Licenses

When you obtain Bria, you purchase a license with a specified number of seats.

Scope of Licenses

A license can be shared by users on the same computer if the users are using the Windows administrator or regular user accounts. However, a user who uses the computer with the Windows guest account and starts Bria will automatically draw down the license count (assuming that a license key has already been entered).

Drawing Down of Licenses

Each time a user enters the license key, the license count is drawn down on the CounterPath license database. When the count is drawn down to 0, then the next time the key is entered, an error message appears for that user.

You can either increase your license count or revoke unused seats. To revoke seats, go to the CounterPath License Portal and log in.

If you seem to have drawn down more license counts than expected, the problem may be that one or more Windows guest accounts have used seats. You can request that CounterPath revoke these licenses in order to reinstate the number of seats actually in use.

Provisioning and Managing Licenses

Remote login lets you provision the license at initial login, then manage the license at further logins, as desired. See "License Key Management" on page 9 for more details.

Setting up Your Service for the Licensing Server

Periodically, Bria connects to CounterPath's license server in order to verify that a valid license is being used. Therefore, at all times, Bria will need to have an Internet connection.

Bria connects to https://secure.counterpath.com via port 443; make sure your firewall allows this HTTPS traffic to this URL. In addition, if you have explicitly set a web proxy (Start > Control Panel > Internet Options > Connections) then Bria will use this proxy; make sure the proxy allows this traffic.

1.3 What Provisioning Does: Writing to Settings

Each provisioning function involves writing to settings stored on the Bria computer. These settings control the behavior of various features of Bria. For example, a successful login request will result in the creation of new settings representing the account.

For detailed information on settings and the features they control, see “Bria 4 Configuration Guide - OEM Deployments”.

1.3.1 Provisioned Settings Overwrite GUI Settings

Settings are assigned values in several ways:

- A setting has a default value.
- Some settings can be changed by the user on the GUI.
- Remote provisioning lets you can change the value of any setting.

NOTE: Provisioned settings overwrite user settings.

At initial startup, default values are loaded. At user login, the provisioning response values are loaded (overwriting some or all of the default values). The user then may change settings manually, if enabled. These settings will be overwritten on Refresh if there are corresponding provisioning response values. Settings are persisted over application shut down.

Keep in mind that provisioned settings override user settings. A user may complain that they change a value on the GUI but each time they restart Bria, their changes are lost. You are probably overwriting their value when you provision.

The “Settings for Bria Desktop” reference documentation (a Microsoft® Excel® document) includes two columns, Screen and Field, that identify settings that are represented on the softphone GUI.

1.3.2 Syntax of Settings

Each setting has a fully qualified name:

<domain>:<section>:<setting>

For example:

proxies:proxy0:register.

The syntax for setting values via provisioning is:

<domain>:<section>:<setting>=<“value”>

For example:

proxies:proxy0:domain=“.com”

Variable values:

- Must appear in double quotes.
- Are always a string. True is represented by “true” or “1”. False is represented by “false” or “0”.
- Are usually not case sensitive. The Bria process that interprets the settings ignores the case of the value (uppercase or lowercase), except for literals such as display names.

1.4 The Mechanism of Remote Provisioning

Each remote provisioning service involves an exchange between the login server and an individual Bria client. The exchange is performed over HTTP or HTTPS.

1.4.1 Servers

You must deploy servers to handle the provisioning requests:

- The “login server”: A server to handle login requests. This server is a web server that can serve one plaintext or XML file.
- The “upgrade executable server”: A server to handle requests from the Bria application to determine if an update is available and where to get the upgrade from, if you decide to implement remote upgrades.
- The “upgrade delivery server”: A server that hosts the binary files that will be downloaded when a user decides to initiate an upgrade, if you decide to implement remote upgrades.

You may decide to deploy these server roles on the same physical server.

The URL for the upgrade executable server (if it is being used) is set in your brand or set by including it in the provisioning response that you send when the user logs in. The upgrade delivery server is always provided in the response to the “is an update available” request — it cannot be branded or provisioned.

Login Server

The hardware requirements of the login server depend on what the server will do. If the server will have a complicated backend database and processing in order to retrieve the settings that are to be provisioned, then the server should have higher processing capabilities. Regardless, the login server is a simple web server and it only needs to serve one file for provisioning.

1.4.2 Bria-to-Server Exchange

The exchange between Bria and the appropriate server involves the following:

- Bria sends an HTTP or HTTPS request to the server when the appropriate trigger occurs. For login, the trigger is the user pressing OK on the Bria login dialog. For remote upgrade, the trigger is the expiry of the upgrade timer.
- The server responds.
- Bria reads the response and takes the appropriate action: Bria starts the softphone and registers with the SIP proxy or Bria finds and installs the upgrade.

Use of Scripts and Macros

You may want to run an appropriate script on the web server, to provide the information required by Bria. To run a script, include it in the URL for that server.

You may require information about the user's deployment when running scripts. The URL for the appropriate server can include macros to capture the information. When Bria contacts the server, it replaces the macros with the real data and includes this information in the HTTPS request.

Your script must understand the names assigned to the macros.

Macro	Description	Value
$build$	The unique buildstamp.	For example, 12345
$computerid$	Unique ID for this computer. Windows only	
$computername$	From the operating system	
ip	The IP address of this computer	
$language$	The language of the installed application. Windows only	en-US, de-DE, es-ES, fr-FR, it-IT (Windows only), nl-NL (Windows only), pt-BR (Brazilian Portuguese), ru-RU, zh-CN (Simplified Chinese)
$license$	The license key.	
$loginname$ / $loginusername$	The login username. This is the username the user enters in the Login dialog and is not necessarily the same as the SIP username. See "Credentials Required" on page 7.	
$loginpassword$	The login password. This is the password the user enters in the Login dialog. See "Credentials Required" on page 7.	
mac	The MAC address of the machine running Bria.	
$osusername$	The user name on the operating system. Windows only.	
$osversion$	The operating system version.	
$osarch$	The hardware architecture on the operating system. Windows only.	
$platform$	The operating system platform.	windows, mac, UNDEFINED.

1.4.3 Communication Mechanism

All communications between Bria and the login server are performed over HTTP or HTTPS, as follows:

- Remote login and provisioning uses POST.
- Remote upgrade uses GET.

If you are using HTTPS, you need a trusted certificate (not self-signed). Bria will only accept certificates whose authenticity can be verified through the trust chain.

1.4.4 Data Format

The information is organized into three portions, which must appear in this order:

- [DATA]
- [SETTINGS]
- [##MEMORY##]

Example

```
[DATA]
Success=1
[SETTINGS]
proxies:proxy0:display_name="Kokila Perera"
proxies:proxy0:enabled="1"
proxies:proxy0:username="6045550008"
proxies:proxy0:password="dfher43d89dhferuieo98375uy8”
proxies:proxy0:domain="acphone.com"
```

[DATA]

This section contains the response to requests:

Success=<value>, a boolean. This data is required.

Failure=<message>, which is optional if the success is 0. For login, the string you enter here will be displayed in the Login dialog.

[SETTINGS]

This section contains settings to be written to persistent memory. The values will be used immediately.

At shutdown, these settings will be written to the local settings file on the Bria computer.

### [##MEMORY##]

This section contains settings to be written to non-persistent memory. The values will be used immediately, but only for the current session.

At shutdown, these settings will not be written to the local settings file.

CRLF (Carriage Return / Line Feed)

The response must end with a CRLF. If this is missing, the last line of the response is ignored.

Handling and Encryption of Passwords

All “password” settings in any domain/section are handled as follows:

- Bria does not interpret passwords in any way, so the value the login server passes to Bria can be encrypted.
- Bria encrypts the value before storing it, regardless of whether or not it is already encrypted. When a stored value is read in order to pass it to the login server, it is first decrypted.
- When a password that the user has entered into a dialog is then passed to the login server, Bria does not encrypt the value.

2 Remote Login and Configuring

2.1 Credentials Required

Login Credentials

Login refers to the process of signing into the VoIP service via your login server. The Bria user must enter login credentials — login name and login password — in order to access Bria.

Login credentials are written to the settings file only if the “Remember login information” box on the dialog is checked.

Login credentials cannot be changed through provisioning.

SIP and XMPP Account Credentials

SIP account credentials allow the user to register for your VoIP service; they are known to your SIP registrar. These credentials are username and password.

The XMPP account credentials allow the user to access the XMPP server; they are known to the XMPP server. These credentials are user name and password.

Account credentials are sent down to Bria by your login server in the login response. Bria writes the credentials to the settings file on the Bria computer.

These credentials are represented in Bria by settings in the proxies domain. For more information on these settings, see the Bria Settings list.

Providing Credentials

When setting up a new user, provide only the user login credentials — login name and login password — outside of Bria. At user login, the SIP and XMPP account credentials will be downloaded to Bria during provisioning. Your provisioning server must be able to provide a customized provisioning file to each user; each file will contain different account credentials.

- The account user name and login user name can be identical or different.
  - The login user name is meaningful to the user (for example, their own name).
  - The account user name follows the syntax for your accounts – it may be a number or words.
- The account password and the login password are typically different for security reasons.
  - The login password should not be encrypted, because the user will enter it manually.
  - The account password does not have to be human-readable.

2.2 Branding Bria for Remote Login

2.2.1 Login Profiles

There are two remote login profiles, a manual or built-in approach. Choose the profile you want to use in your brand:

- Manual Configuration profile: The user enters the login server URL on the Login dialog.
- Built-in URL profile: Your brand of Bria has the login server URL built-in. With this profile, if you change the URL, you must request a new brand of Bria.

Once a login server URL is available, the login process is the same for both profiles.

2.2.2 Skipping Login

There are two situations in which login may fail:

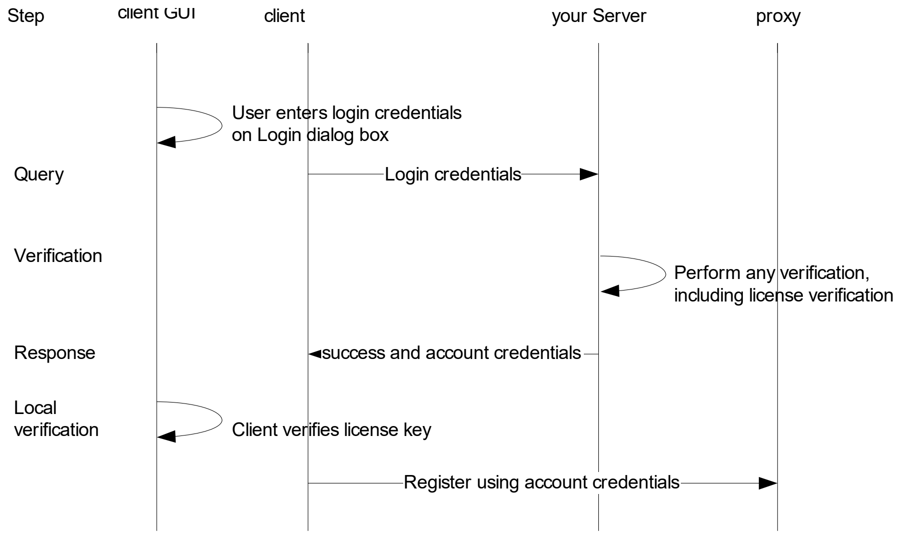
- The login server cannot be reached. Bria can be configured to allow the login to be skipped in this situation.
- The login server can be reached but the user enters the wrong login credentials. Login cannot be skipped in this situation.

Login skip is only allowed if the user has already successfully logged in at least once. If the login attempt fails after an earlier successful login attempt, the user does not know that the login has been skipped. Bria uses the account credentials and other settings that are stored on the Bria computer.

You must decide if you want to support login skip, to allow users that were previously configured in the event that the server is not reachable either due to an outage or because the user has moved to a network environment where communication to the server is not possible.

2.3 The Login Process

The login procedure is identical for all remote login profiles. The login server must be set up to handle the following procedure.


Step
client GUI
client
your Server
proxy
User enters login credentials
on Login dialog box
Query
Login credentials
Verification
Perform any verification,
including license verification
Response
success and account credentials
Local
verification
Client verifies license key
Register using account credentials

2.3.1 Login Procedure Is Invoked

The Login dialog is displayed. (You can speak to your account representative about customizing the login dialog.) The user enters the required information and presses Login.

2.3.2 Query Step

Bria sends the data from the Login dialog to the login server using an HTTP POST. The POST data is of type application/x-www-form-urlencoded, containing key-value pairs as branded via the Login Parameters string.

License Key Management

You may want to maintain license key information such as the distribution of licenses to users.

To help you maintain this information, you can capture data by including the appropriate macro in the login parameters.

2.3.3 Verification Step

The login server should perform any suitable verification on the sent data, according to your business rules.

Typically, this verification will include a check for the license key. You may decide to send a license key or (for an existing deployment) you may determine that there is no need to send a license key.

2.3.4 Response Step

Response Step: Failure

If there is a problem with any of the data, your server should return failure data in the following format:

```
[DATA]
Success=0
Failure="<message>"
```

where:

- Success=0: This line is required. The 0 indicates a failure.
- Failure: This line is optional. The string you enter here is displayed in the Login dialog.

The response must end with a CRLF (Carriage return / line feed).

Response Step: Pass

If your server can handle the request, it should return a success message and the account credentials. It can also return other settings that can be specified only at login.

This example includes a license key being sent down to the computer:

```
[DATA]
Success=1
LicenseKey="48jey45379ryeioo8a7e934q8dhfudufoladskiuwb"
[SETTINGS]
proxies:proxy:user_name="6045550008"
[##MEMORY##]
proxies:proxy0:password="rosebud"
```

where:

- Success=1: This line is required. The 1 indicates a success.
- LicenseKey: The license key for the computer. This data should be sent for a new deployment or if you want to change the existing license key.
- Settings: The username will be saved at shutdown.
- ##Memory##: The password will not be saved at shutdown.

The response must end with a CRLF (Carriage return / line feed).

2.3.5 License Key Verification by Bria

Bria next takes one of these actions, depending on the response received from the server:

If the response was a failure: The Login dialog appears again. The process goes back to “Login Procedure Is Invoked” on page 9.

If the response was a success: Bria checks if there is a license key in the response.

- If the response includes a key, Bria validates the key and then starts.
- If the response includes a key and validation fails, then the Enter License Key dialog appears.
- If the response does not include a license key, then Bria checks if there is already a key stored on this computer.
    - If yes, then Bria verifies that the key is valid and then starts.
    - If no, then the Enter License Key dialog appears. When the user enters the license key (obtained outside of Bria, for example in an email sent to all new customers), Bria verifies that the entered license key is valid. If the key is valid, Bria starts.

3 Remote Upgrades

You can make software upgrades of Bria available on a web server. Bria can be set up to check with this upgrade executable server for software upgrades. If an upgrade is available, the user is prompted to download and install it.

3.1 General Setup

Remote upgrade is controlled by the following Bria settings. You can change the default values through remote provisioning. Optionally, you may have provided CounterPath with the values for the following settings. If you decide the values you provided are no longer suitable, you can change them through remote provisioning.

Domain:Section	Setting	Comment
feature:auto_update	code_server_url	The "upgrade executable server": the server that handles remote update requests. The setting must be specified before any remote update can be performed.
feature:auto_update	code_check_initial_t_s	The initial value of the upgrade timer used for timing the first time the client hits the upgrade server. After the initial hit, the client hits the upgrade server every 24 hours.

3.1.1 Setting Up

Set up an upgrade server as follows:

- You can use a script to include logic that determines a given deployment needs an upgrade.

  If you are using scripts, set the URL for the upgrade server to include the script and any macros (for example, the language and the build macros).
- You can skip the script and manually set up your upgrade server to simply provide a success response when an upgrade is available and a failure response at other times.
- Place the executable on the "upgrade location" when you want to deploy an upgrade.

3.1.2 Timing of Upgrade Checks

Bria contacts the upgrade server as follows:

1. Bria starts and the initial upgrade timer starts using the value in code_check_initial_t_s.
2. When the initial upgrade timer expires, Bria checks for an upgrade. Bria performs an upgrade if it is available.
3. Bria checks the upgrade server every 24 hours. Bria performs an upgrade if it is available.

3.1.3 How Remote Upgrade Is Performed

Bria Sends a GET

When triggered by the timer, Bria checks for available upgrades by sending a GET to the upgrade executable server.

For example, if you are using scripts, the value of feature:auto_update:code_server_url might be:

```
https://executablepgradeserver.com/exe_upgrade.php?build=$build$&language=$language&name=$loginame$
```

This URL could result in a GET to your web server of:

```
https://executablepgradeserver.com/exe_upgrade.php?build=38740&language=en-US&name=kperera
```

If you are not using scripts, the value of feature:auto_update:code_server_url is the URL of the upgrade server:

```
https://executablepgradeserver.com
```

Server Response

The upgrade executable server must respond with the following:

```
[DATA]
Success=0
```

or

```
[DATA]
Success=1
version=60000
url=https://executableupgradeserver.com/newversion.exe
```

where:

- Success=1: True (there is an upgrade) or 0=false (there is no upgrade).
- version: Identifies a build stamp set by Bria during build time. Bria uses this version to determine whether to prompt the user to install the upgrade.
- url: The absolute path to the installer software for the new version.

The response must end with a CRLF (Carriage Return / Line Feed).

The response **cannot** include a [SETTINGS] section. In other words, none of the user's current settings can be changed via this response.

If no upgrades are found, Bria will check for upgrades every 24 hours.

Handling of the Upgrade

If an upgrade is available, Bria compares the build number of the application on the user's computer to the build number specified in the response (60000 in the above example).

- If the response has the same number, Bria does not prompt the user to download
- If the response has the lower number, Bria does not prompt the user to download: downgrades are not supported.

- If the response has a higher number, Bria prompts the user to download the upgrade.
    - If the user initiates the download, Bria will download the installer and save it to the local Bria program folder. Bria will also prompt the user to exit in order to install the new version. The user can install immediately or postpone installation.
    - If the user declines the upgrade, Bria will enter its timing cycle and display the download prompt again in 24 hours.