**CounterPath Corporation**
Suite 300, Bentall One Centre
505 Burrard Street Box 95
Vancouver BC V7X 1M3
Canada V6B1R8

Telephone: +1.604.320.3344
www.counterpath.com

# CounterPath Softphones
## Deployment Overview

This overview applies to Bria Desktop – Bria *for Windows* and Bria *for Mac* – and to the suite of Bria Mobile products – Bria iPhone Edition, Bria iPad Edition, and Bria Android Edition.

When you deploy Bria, you can customize the client in several ways:

- You can make some changes to the look of the client.
- You can customize the feature set that is included (removing features you do not want to include).
- You can pre-configure many of the features you do want to include.
- You can decide whether you want to implement remote provisioning features – remote login, remote feature provisioning and remote upgrade.

This overview is intended to help you make the decision about the last point: implementing remote provisioning.

Once you have made this decision, you can read the “Bria 3 Branding Guide” and complete the appropriate branding form.

# 1 Deployment Options

## 1.1 No Login

This option applies to Bria Desktop and Bria Mobile.

- For small deployments (10 to 20 users) of technology savvy users.
- The user can have more than one SIP account. The user can optionally have one or more XMPP accounts (XMPP is not yet supported on all platforms).
- No server-side implementation is required.

#### How It Works

- Bria starts without a login screen.
- The user manually enters SIP account credentials (and optional XMPP account credentials, if XMPP is supported) on the Accounts window. These credentials are stored on the Bria computer or device.
- Each time Bria is started, Bria registers each configured account with the SIP registrar (and XMPP server, if applicable), using the stored account credentials.
- For Bria Desktop, the license key must be entered manually by the user. (For Bria Mobile, the license key is already built into the softphone.)

#### Branding and Customization Options

- Bria can be pre-configured to work in your network.
- Bria can be customized to include only the features you want to support. Individual Account and Preferences panels can be hidden.

#### To Deploy with No Login

- Complete the “no provisioning” branding form.

  For Bria Desktop, this form is blue.

  For Bria iPhone Edition and Bria iPad Edition, it is purple.

  For Bria Android, it is orange.
- Read the appropriate branding guides:

  “Bria 3 Branding Guide for Category 1 Customers”

  “Bria iPhone &iPad Edition Branding Guide for Category 1 Customers”

  “Bria Android Edition Branding Guide for Category 1 Customers”
- Provide the user with SIP account credentials and XMPP account credentials (if applicable) outside of Bria (by e-mail, for example).

  The account credentials for both SIP and XMPP are user name (e.g. kperera@domainA.com), the password, and the authorization name (only for SIP and only if required by your network). The account password should not be encrypted because the user will enter it manually.
- For Bria Desktop, provide the user with the license key outside of Bria.

# 1.2 Local Login

This option applies to Bria Desktop only.

- For small deployments (10 to 20 users) of non-technology savvy users.
- The user is restricted to one SIP account and optionally one XMPP account.
- Local login provides control in situations in which a computer is shared: Access to Bria is controlled by login, and when a user logs in, their individual data (account credentials, contacts, and so on) are loaded.
- No server-side implementation is required.

### How It Works

- When Bria starts, a login screen appears.
- The user enters their SIP account credentials. Bria automatically uses these credentials to set up the account. In other words, the login credentials are identical to the SIP account credentials.
- To support an XMPP account there are two options:
  - The same account credentials can be used for the SIP and XMPP accounts. For example, the SIP account credentials are kperera@domainA.com with password “secret” and the XMPP account credentials are also kperera@domainA.com with password “secret”.
  - The XMPP account credentials are different. In this case, once Bria is running, the user will have to set up the XMPP account by choosing Softphone > Accounts from the menu.
- All users using the same computer will have the same network configuration settings except for the SIP (and XMPP) account credentials.
- The license key must be entered manually by the user.

### Branding and Customization Options

The options are the same as for the “no login” option:

- Bria can be pre-configured to work in your network.
- Bria can be customized to include only the features you want to support. Individual Account tabs and Preferences panels can be hidden.
- If you support XMPP, Bria will be customized for the option you choose.

### To Deploy with Local Login

- Complete the blue “Branding Bria 3 for Category 1 *No Remote Provisioning*” form.
- Read “Bria 3 Branding Guide *for Category 1 Customers*”
- Provide the user with the SIP account credentials outside of Bria (by e-mail, for example).
- The account credentials for both SIP and XMPP are user name (e.g. kperera@domainA.com), the password, and the authorization name (only for SIP and only if required by your network). The account password should not be encrypted because the user will enter it manually.
- Provide the user with the license key outside of Bria.

# 1.3 Remote Login

This option applies to Bria Desktop and Bria Mobile.

Remote login and provisioning is a means for you to control access to your phone through a login, and remotely provide a license key to the softphone (for Bria Desktop only).

It also provides these added benefits:

- Authenticate users, so that only valid users can use your softphone.
- Remotely provide network configuration information and individual account credentials for users.
- Remotely enable or disable and remotely configure many of the features of Bria.
- Remotely deploy upgrades to the software as and when you want (for Bria Desktop only).

### Summary

- Remote login involves an HTTP exchange between the individual Bria softphones and a login server.
- Multiple SIP accounts and multiple XMPP accounts can be supported.
- Users can be provisioned with individual configuration settings.
- In Bria Desktop, the license key can be included in the provisioning response. (For Bria Mobile, the license key is already built into the softphone.)

### Branding and Customization Options

- Bria can be delivered with an initial configuration that includes only the features you want to support.
- Bria can be delivered with specific configuration screens hidden. If a configuration field is not hidden, it can be made read-only (Bria Mobile only).
- The login dialog can be customized to include fields such as “Remember me”.

### Deployment Options

Remote login can be deployed using:

- Your own “custom” login server.
- The CounterPath Client Configuration Server (CCS) deployed on your own server. The CCS supports all CounterPath softphones, including the clients for iPhone®, iPad® and Android™ devices.
- The CCS hosted by CounterPath.

See the following pages for details.

If you are using BroadSoft’s Device Management System for provisioning, contact CounterPath Sales to discuss options.

### To Deploy with Remote Login

- Complete the “with provisioning” branding form.

  For Bria Desktop, this form is dark red. For Bria iPhone Edition and Bria iPad Edition, it is green.

  For Bria Android, it is bright blue.
- Read the appropriate branding guides:

  “Bria 3 Branding Guide *for Category 1 Customers*”

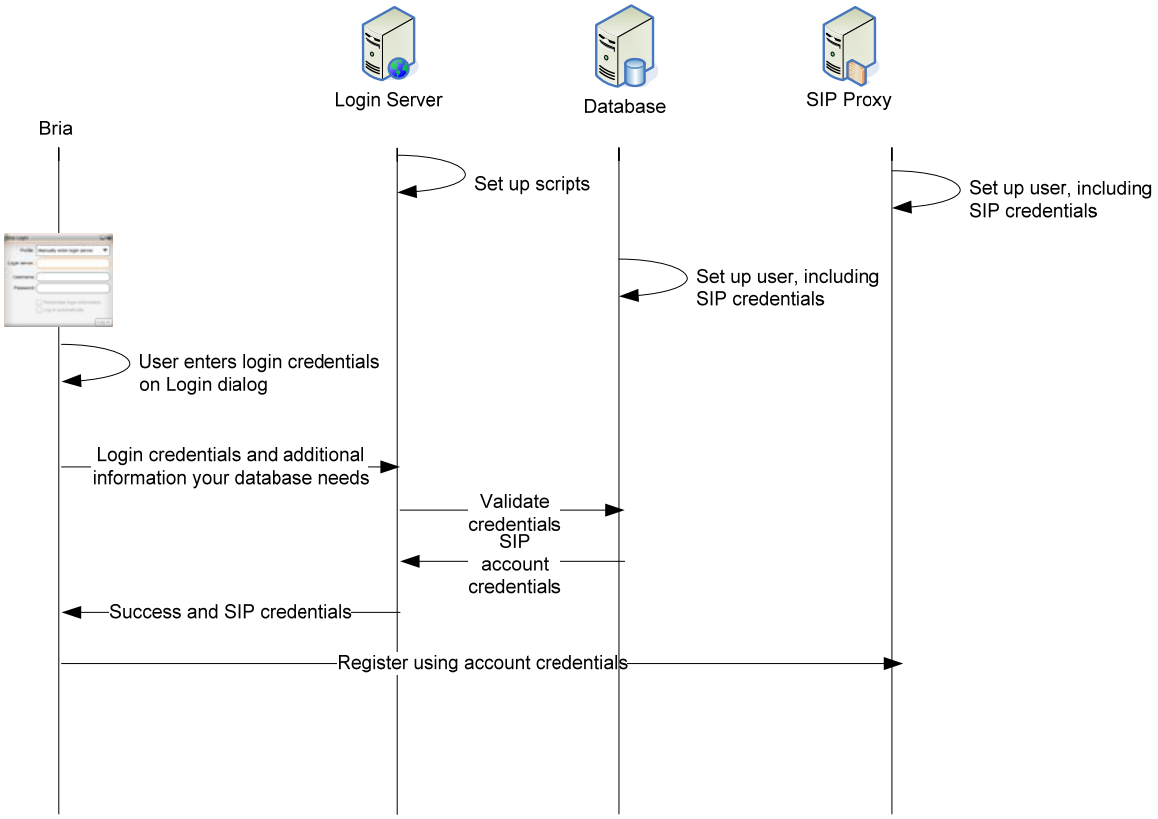
  “Bria iPhone &iPad Edition Branding Guide *for Category 1 Customers*”

  “Bria Android Edition Branding Guide *for Category 1 Customers*”

- Read the appropriate provisioning guide:
  - "Bria 3 Provisioning Guide *for OEM Deployments*" and/or "Bria Mobile Edition Provisioning Guide *for Category 1 Customers"*.
- "Provisioning CounterPath Softphones via the CCS"

# 2 Details on Remote Login

## How Provisioning Works with a Custom Login Server




- You must set up a login server. Typically this server connects to a customer care system or other database in your organization. Provisioning can easily be deployed using any login server, such as APACHE/IIS[1].
- Your login server address must be provided to the Bria client. The address can be specified in one of three ways:
  - Discovered via DHCP options (for Bria *for Windows* only).
  - Manually configured: entered by the user on the Login dialog (Bria Desktop only).
  - Hard-coded in the phone as part of the customization of Bria for your deployment (Bria Desktop and Bria Mobile).

  This URL can include macros that your login/provisioning server requires to validate the request; for example, the computer's MAC ID. When the request is sent, Bria replaces the macros with the real data from Bria and the computer.

  When your server receives the request, it is your server's responsibility to interpret and use the macros, to validate login credentials (username and password) and provide the SIP account credentials (username, password and optional authorization name).
- The URL should also include a script to include logic for the login server to query your database for settings. CounterPath provides you with a sample login script that you must modify to suit.

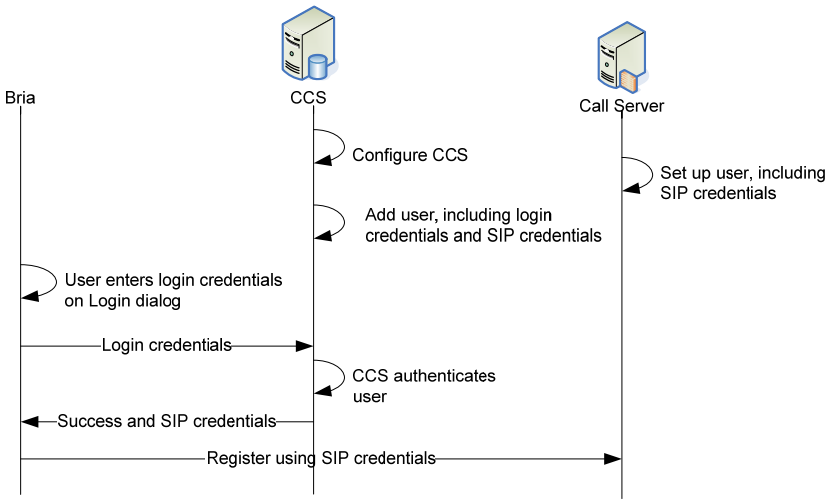
[1] Apache is a trademark of The Apache Software Foundation.

- When Bria starts, a login screen appears and the user enters their login credentials.
- Bria sends an HTTP or HTTPS request to the login server. The login server reads the HTTP request and verifies the login credentials. The login server also executes your script to obtain the desired data.
- The login server sends down a success or failure provisioning response. A success response includes the credentials for the SIP or XMPP account.
- Bria applies the data in the response and the softphone starts up with the configured behavior.

## How Provisioning Works with the CCS

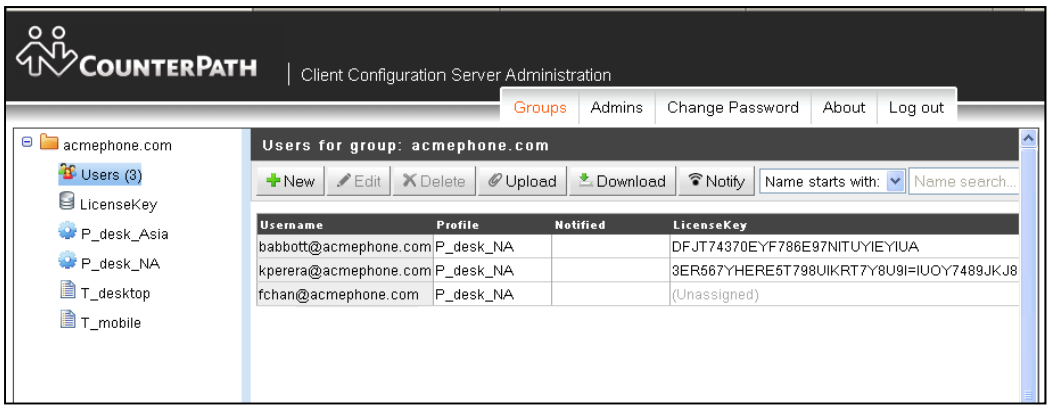
### CCS without a Customer Support System

You can deploy the CCS on its own to provision your users.



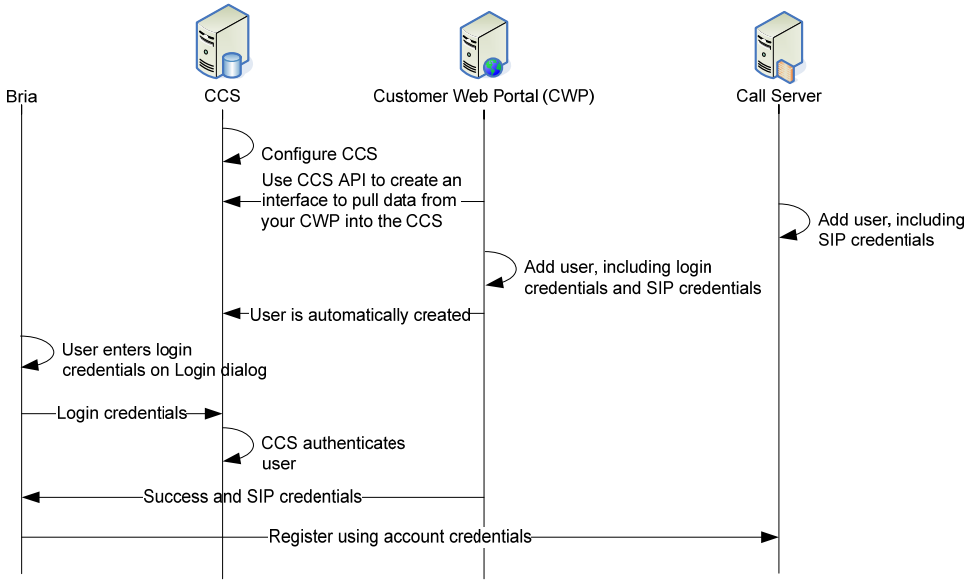

- If you are deploying your own CCS, you install it on your own server.
- CounterPath provides you with administrator credentials to connect to the CCS, either on your own server or on CounterPath's CCS.
- Configure CCS: On the CCS, the administrator sets up templates (one each for Bria Desktop and Bria Mobile), profiles for different types of users, attributes to hold login credentials and settings data, and finally users.
- Your login server must be provided to the Bria client, in the same way as for a custom login server deployment: DHCP, manually, or hard-coded.
- When Bria starts, a login screen appears and the user enters their login credentials.
- Bria sends an HTTPS request to the CCS. The CCS reads the HTTP request and verifies the login credentials. It then creates a provisioning response using the most current data and sends it down to the softphone.
- Bria applies the data in the response and the softphone starts up with the configured behavior.

This illustration shows three users set up for "Acemphone":



### CCS with a Customer Support System

If you have a customer care system, you can integrate it into the CCS and pull data from that system into the CCS.




The workflow is very similar to deploying with a customer support system. The major difference is that instead of adding users on the CCS, you create an interface to pull users from your customer support system into the CCS.

## Advantages of the CCS

- The CCS handles all the logic for interpreting the login request from the softphone client: there is no programming effort on your part and you do not have to create scripts.
- If you use the CounterPath-hosted CCS, you do not need to invest in any hardware.
- CCS does not require a customer care system, but if you have one, you can use the CCS API to pull data from that system into the CCS database.
- The CCS seamlessly supports both Bria Desktop and Bria Mobile: the CCS detects which platform a user is using and sends the provisioning response that is appropriate to that platform.
- The CCS has an easy-to-user web interface that lets you set up the initial CCS framework and then quickly add users. The web interface supports uploading of users from a file.
- Bria Desktop and Bria Mobile use different formats for the provisioning response. Bria Mobile's format is XML. The CCS includes a validation feature that ensures that you have created valid XML.
- The CCS includes a pool feature that lets you load a set of license keys into the CCS, and then have the CCS automatically assign a key each time a new user logs on for the first time.
- The CCS includes a feature that lets you create an email notification template and then send emails to one or more users.
- If you are a reseller, you can deploy the CCS is a tenanted mode. Tenanted mode is supported on both the self-deployed CCS and on the CounterPath-hosted CCS.

# 3 Remote Update (Refresh)

If you support remote login, Bria can be configured to contact your update server at specific times when the user is already logged on, to request updates to settings. The server can send down changes to any Bria setting. This feature can be used, for example, to change the SIP proxy to use.

There is no need to restart the client after settings are changed.

## How Provisioning Works with a Custom Login Server

There are two approaches:

- The easy approach:

  You configure Bria (via provisioning) so that the update server setting specifies the same URL as the login server. You also specify update timers that trigger Bria to contact the server.

  When the update timer expires, Bria contacts the server. Your server handles the request as it does a regular login request, and simply verifies the login credentials and sends down all the settings. Any changes in the values of settings since the user logged on will be applied immediately in Bria.
- A more sophisticated approach, for example, if you want to send down only changed settings in an update response:

  You configure Bria (via provisioning) so that the update server setting specifies a special update URL. You also specify update timers that trigger Bria to contact the server.

  When the update timer expires, Bria contacts the server. Your server must include code to interpret the request as an update request, and send down the desired settings. Any changes in the values of settings since the user logged on will be applied immediately in Bria.

## How Provisioning Works with the CCS

The CCS implements the “easy approach” above.

You simply include your CCS URL and the timer settings in your template. When the update timer expires, Bria contacts the CCS. The CCS simply verifies the login credentials and sends down all the settings. Any changes in the values of settings since the user logged on will be applied immediately in Bria.

If you don’t want to support remote update, you omit these settings from your template.

# 4 Remote Upgrade

Bria always checks for software upgrades on startup. It can also be configured to contact your upgrade server at specific times to check for software upgrades.

- Bria is branded for the URL of your upgrade server.
- The URL can include macros that your upgrade server reads (using an upgrade script you write and install) that provide information about the user. For example, the user's current build of Bria.

  When the contact is made, Bria replaces the macros with the real data from Bria and the computer.
- You can flag an upgrade as mandatory or optional.

Remote upgrade works the same way whether you are using your own server or the CCS:

- When you want to provide a software upgrade, obtain the upgrade from CounterPath and put it in the location specified by the URL.
- When Bria is scheduled for an upgrade check, it contacts your upgrade server (or the CCS). Your upgrade server/the CCS runs your upgrade script to determine whether or not to send an upgrade. If you have your own upgrade server, the content of this script is up to you. It can include logic that uses the macros included in the URL; for example, it can query the user's current build.
- The upgrade server/CCS sends a response to Bria: either an upgrade is available (in which case the response must include the URL of the location of the executable) or it is not available.
- If the response is that an upgrade is available, Bria prompts the user to download. When the user responds, Bria connects to the specified executable URL and downloads the executable.