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

Bria 3.0 Remote Provisioning Overview

Summary

Remote provisioning is a means for you to:

- Control access to your phone through a login.
- Remotely provision network configuration information and individual account credentials for your 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.

Provisioning works as follows:

- It involves an exchange between a remote web server at your site and the individual Bria installation.
- The exchange can use HTTP or HTTPS
- Provisioning can easily be deployed using any web server, such as APACHE/IIS.
- Provisioning requires some simple scripts on your web server.

Login Options

No Login Dialog

- For small deployments (10-20 users) of technology savvy users.
- Accounts credentials are provided to the user outside of Bria, for example by e-mail.
- Users configure Bria for the network and for Bria features by completing fields on the Accounts window.

Local Login

- For small deployments (10-20 users) of non-technology savvy users.
- Credentials are provided to the user outside of Bria, for example by e-mail.
- These credentials serve as both the login credentials and the SIP account credentials: the user enters these credentials on the login dialog and then Bria uses these same credentials as the SIP credentials.
- Local login provides control in situations in which a computer is shared: Access to Bria is controlled by login, and when the user logs in, their individual data (account credentials, contacts, and so on) are loaded.

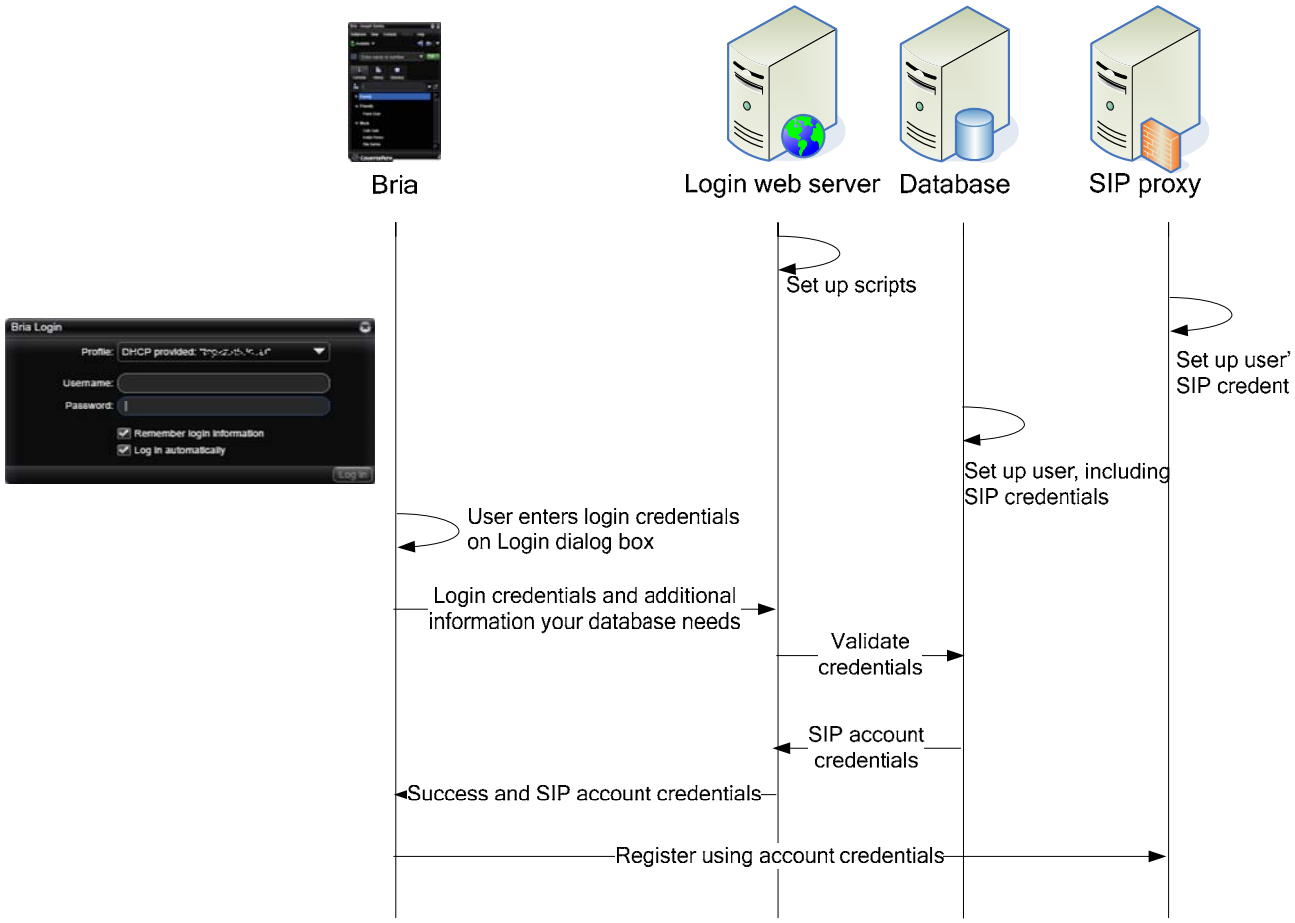
Remote Login Dialog with Login Server

- Our typical deployment methodology.
- Login credentials are provided to the user outside of Bria, for example by e-mail.
- The login server can be hardcoded in a custom brand, or it can be entered manually be each user.
- The user logs in and the login credentials are verified by the login server.
- SIP account credentials are pushed to Bria client in the response from the login server.

Login Dialog with DHCP Login Server

- For enterprise deployments where the login server may not have a fixed IP or where several login servers are being used.
- Login credentials are provided to the user outside of Bria, for example by e-mail.
- The login server is discovered via DHCP options.
- The user logs in and the login credentials are verified by the login server.
- SIP credentials are pushed to Bria client in the response from the login server.

Remote Login Flow Diagram



- Bria login dialog can be customized to include fields such as “Remember Name”.
- The URL of your login/provisioning server is either branded into your custom brand, or discovered through DHCP, or entered by the user on the Login dialog.

  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).
- In the response back to Bria, your server must send the SIP account credentials.

Remote Feature Provisioning

The remote login process includes the ability to send settings that configure Bria. CounterPath provides you with documentation on these settings. For example, you can configure Bria to work in the network that you know the user is on. Or you can enable or disable features of Bria.

Remote feature provisioning works as follows:

- You set up the settings on your database.
- You must modify the login script to include logic for the login server to query your database for settings.
- When you send the response back to Bria, include the settings you want to provision.
- Bria automatically applies the settings that have been received. Bria starts up with the configured behavior.

Remote Update

Bria can be configured to contact your update server at specific times. 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.

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.
- The new software can be an upgrade or a downgrade (rollback to a former version).

Remote upgrade works as follows

- 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. Your server runs your upgrade script to determine whether or not to send an upgrade. 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.
- Your server must send back to Bria the URL to the location of the executable.
- Bria automatically connects to this location, downloads the executable, and installs the new version.

