Barracuda Safe Browser Setup Guide - With the Barracuda Web Security Service

https://campus.barracuda.com/doc/6553659/

If you have a Barracuda Web Security Service Account, you can deploy and use the Barracuda Safe Browser on mobile devices. If you don't have an account, see Create a Barracuda Cloud Control Account to create one. The Barracuda Safe Browser supports iOS 9.0 and higher.

See also:

- Barracuda Safe Browser - FAQ
- Barracuda Safe Browser User Guide

Basic Setup in the Barracuda Web Security Service

The Barracuda Safe Browser provides the same functionality as iOS browsers, but it's integrated with the Barracuda Web Security Service. There are two ways to provision the Barracuda Safe Browser.

Option 1 - Provision devices from within the Barracuda Web Security Service*:*

1. Log into your Barracuda Web Security Service account and navigate to the **REMOTE FILTERING > Safe Browser > Provisioning** page.
2. Click **Add IP** and enter a **Location** (ex: *Finance*, *Student Housing*, *London Office*) and the external **IP address** of your Wi-Fi network. This IP address will be used by the Barracuda Web Security Service to identify a device or group of mobile devices managed by this account.
3. Select *Enabled* or *Disabled* for this IP address. Click **Add**.
4. Click **Add** to provision this IP address.
5. The first time a user logs into the Barracuda Safe Browser from their device, provisioning will be automatic.
6. See Authentication below to configure LDAP authentication for users.

Option 2 - If you don't know the external IP address of your Wi-Fi network, or if users will launch the browser from outside the network:

1. If you don't know the external IP address of your Wi-Fi network, leave the **IP address** field blank on the **REMOTE FILTERING > Safe Browser> Provisioning** page. Go ahead and create a **Shared Secret**..
2. Give your users the **Provisioning Key** and **Shared Secret**.
3. The first time a user launches the Barracuda Safe Browser on their device, they will be prompted to enter the **Provisioning Key** and **Shared Secret** to provision the device.
4. See Authentication below to configure LDAP authentication for users.

Basic Setup of the iOS Mobile Device

1. From within your Wi-Fi network, launch the Safari browser on your iOS device and visit the iTunes App Store to fetch the Barracuda Safe Browser application.
2. When the application has downloaded, you'll see the Safe Browser icon on the display. From within the organization's Wi-Fi network, run the Barracuda Safe Browser. You will see a popup that says "Device Provisioned". If you see an error message instead, check to make sure that you have entered the external IP address for your network in the Barracuda Web Security Service as described above.
3. **Enable Restrictions for the Safari browser locally on the device** through Settings > Restrictions, or using an MDM or Apple Configurator.
4. Once the local browser is restricted, the icon for that browser will disappear from the UI on the mobile device, and the user is ready to run Barracuda Safe Browser with policies you've configured in the Barracuda Web Security Service. Your Barracuda Web Security Service policy will now be applied to all traffic from the Barracuda Safe Browser and will be reflected in reports.

Managing the Application in iOS

View Bookmarks: From the **Bookmarks** button at the bottom of the iOS display, you can view bookmarks provisioned to the device by Barracuda Web Security Service as well as the bookmarks added by the user.

Log Out, Unprovision and **Clear History:** From the **Settings** button at the bottom of the iOS display you can view the Username, Hostname, Auth Key, Device ID and Version. If you need to log out the current user if the device will be shared, you can **Log Out**, **Unprovision** the device and **Clear History**. When the next user runs the Barracuda Safe Browser, the device will be re-provisioned and the user will be prompted to log in per the configuration by Barracuda Web Security Service.

The Default browser

You *cannot* make the Barracuda Safe Browser the default browser. This is because iOS does not allow changing the “default” browser. You can restrict Safari as described above, and then use an alternate browser like the Barracuda Safe Browser. However, **links from emails, social media feeds and other apps will need to be copied and pasted to the address bar.**

View Bookmarks: From the **Bookmarks** button at the bottom of the iOS display, you can view bookmarks provisioned to the device by the Barracuda Web Security Service as well as the bookmarks added by the user.

From the **Settings** button in the Barracuda Safe Browser you can:

- Change the **Home Page** of the browser
- Change the default **Search Engine**
- Set the browser to either request web sites rendered for desktops or for mobile devices
- **Accept Cookies**
- Set **Private Browsing** to *On* or *Off*. Setting to *On* means that neither the browsing history nor cookies will be saved/stored.
- **Clear History**
- **Clear Cookies and Data**
- **Log Out**
- Touch **About** to see:
    - Username, Host name, Authentication Key, Device ID, Provisioned To, and Version

Creating shortcuts to web pages on the device home screen

While you cannot create shortcuts from the Barracuda Safe Browser, you can create shortcuts with the Apple Configurator tool that contain a URL that starts with "bsb://" e.g. bsb://www.barracuda.com. This link, for example, would launch a shortcut into the Barracuda Safe Browser. These shortcuts can be pushed out to devices via an MDM or a mobile config file.

Authentication

On the **REMOTE FILTERING > Safe Browser > Provisioning** page, configure the following settings:

- **Session Authentication**: If you want to require users to log in with LDAP credentials before browsing, select *Forced Authentication.* Selecting *Optional Authentication* will give the user the choice of either logging in and browsing with assigned polices, or browsing as a guest under a different set of policies. Select *None* if you don't want the user to be presented with a log in option – the user will only browse as a guest.
  Use the **REMOTE FILTERING > Authentication** page to configure your authentication server. The only required settings are IP address, Server Alias, Port and UID Attribute.

  Note: If you configure LDAP authentication in the Barracuda Web Security Service for your Barracuda Safe Browser users, you can apply user-specific policies for each mobile user. Otherwise you can only apply global policies to all mobile users. To configure LDAP authentication, you'll need to expose your LDAP server to the Internet by port forwarding from your Barracuda Web Security Service external IP address to port 389 (non-secure) or port 636 (secure) for your LDAP server. Currently the Barracuda Web Security Service supports Microsoft Active Directory. **Only one authentication server can be configured.**

- **Session Timeout**: If you have configured LDAP authentication for your mobile users, use this

setting to specify the amount of time, in minutes, that is allowed to elapse before a user's login expires and re-authentication is required. To disable session expiration (so that a session does not expire until the user logs off), set this value to ***0*** hours or minutes. The recommended setting is *24 hours*.
- **Idle Timeout** - If you have configured LDAP authentication for your mobile users, use this setting to specify the amount of time, in minutes, that a user's session is allowed to remain idle before that login session automatically expires. To disable session expiration based on idle time, set this value to ***0*** hours or minutes. The recommended setting is *8 hours*.

Managing Filtering Options

On the **REMOTE FILTERING > Safe Browser** page, configure the following settings:

- **Bypass Password:** Creating a password means that the user (or the administrator of the mobile device) can enter it to bypass all filtering by pressing the **Bypass** action button on their mobile device.
- **Bypass Filter:** Enter any IP addresses that you want to bypass filtering by the Barracuda Web Security Service.
- **Fail Open:** Set to *Yes* if you want the Barracuda Safe Browser to allow all web requests if the mobile device cannot reach the Barracuda Web Security Service for some reason. Setting to *No* means that all requests would be blocked in that case.
- **Enable Geolocation**: Setting to *Yes* means that the last location from which the user of the device logged in, or that the settings were synchronized, will be displayed in the Barracuda Web Security Service. If this feature is enabled, then on the **Remote Filtering > Safe Browser > Devices** page showing the **Last Seen Devices**, you'll see the username, the domain, the Device ID, the IP address, the last-seen location and time/date that the user last made a web request. This feature is useful for locating lost or stolen devices.
- **Allow Temporary Bypass Filtering:** Enabling this feature allows the administrator or user to temporarily bypass filtering by the Barracuda Web Security Service for up to 5 minutes, at which point filtering automatically resumes. If you are connecting from an Internet cafe or hotel portal, for example, and need to temporarily disable the Barracuda Safe Browser to be connected to that network, this provides a 5 minute period in which to do so. Only 3 temporary bypasses are allowed once the Barracuda Safe Browser is installed. The **Bypass Password**, configured per above, is *not* required.
- **Allow Bypass Filtering:** Users who have administrative rights on their mobile devices can bypass filtering indefinitely in their Barracuda Safe Browser. The **Bypass Password**, configured per above, is required.

Managing Devices

From the **REMOTE FILTERING > Safe Browser > Devices** page you can view the last logged

activity from any mobile device running the Barracuda Safe Browser, including the Domain, Username, Device Type/OS, MAC Address, IP Address, Location and Date/Time Last Seen.