Integration with Aruba Networks WiFi Infrastructure
SocialSign.in is a web services company based in New York City and San Francisco that enables commercial venues to easily integrate marketing and sponsorship workflows into on-premise guest WiFi networks.

Aruba customers have the ability to extract additional value from their existing infrastructure by running SocialSign.in as part of their deployments. A joint solution extends digital marketing initiatives to a physical setting. Improve guest experience and gain a deeper understanding of foot traffic while requiring no additional hardware.

This guide will walk you through setting up SocialSign.in authentication on your existing Guest Network using an Aruba Mobility Controller.

**PREREQUISITES**

- Mobility Controller and Access Points (APs)
- New or existing Guest VLAN
- Policy Enforcement Firewall Next Generation License (PEFNG)

*Note: This guide is specific to Aruba OS firmwares 6.3 and later. For help configuring an earlier release, please contact support@socialsign.in.*

Configurations may vary; please contact support@socialsign.in for assistance.
## CONFIGURATION STEPS

### 1. Set Up RADIUS Server and Server Group

To perform authentication, please list SocialSign.in’s RADIUS Service in the Servers section of the authentication configuration.

**NAVIGATE TO**

Security ★ Authentication ★ Servers

Create a new RADIUS server with parameters provided by SocialSign.in. Add this RADIUS server to a new Server Group.

**SAMPLE SETTINGS**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>107.x.x.x</td>
</tr>
<tr>
<td>Key</td>
<td>myradiuskey</td>
</tr>
<tr>
<td>Auth port</td>
<td>20</td>
</tr>
<tr>
<td>Acct port</td>
<td>21</td>
</tr>
<tr>
<td>NAS ID</td>
<td>0</td>
</tr>
</tbody>
</table>

![Configuration Interface Screenshot](image-url)
2 Set up walled garden

A guest’s device must access a few additional domains prior to authorization. Create a domain whitelist for use with the guest portal.

*Note: This requires the Policy Enforcement Firewall Next Generation License PEFNG.*

**NAVIGATE TO**

- Advanced ➤ Stateful Firewall ➤ Destination

Create a Firewall Destination Whitelist.

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>socialsign.in</td>
<td>Accept</td>
</tr>
<tr>
<td>fbcdn.net</td>
<td>Accept</td>
</tr>
<tr>
<td>facebook.com</td>
<td>Accept</td>
</tr>
<tr>
<td>facebook.net</td>
<td>Accept</td>
</tr>
<tr>
<td>akamaihd.net</td>
<td>Accept</td>
</tr>
</tbody>
</table>
3 Create two user roles for AAA profile and Captive Portal `ssi-guest-logon & ssi-guest`

**NAVIGATE TO**

Security ▶ Access Control ▶ User Roles

Clone the roles guest-logon and guest from the Aruba settings, or create your own guest role for authenticated users. The ssi-guest-logon role must have the following initial setup; it will later be connected to the Captive Portal which will automatically create another role for allowing access to 'Walled Garden' domains.

*Note: The Captive Portal Profile is not yet defined. Once we create our Captive Portal, we will return to this page to connect it to this role.*

**ADD THE FOLLOWING DOMAIN NAMES**

- ra-guard
- logon-control
- captiveportal
- v6-logon-control
- captiveportal6
- ssi-guest-logon
4 Add a Captive Portal

**NAVIGATE TO**
- Security ► Authentication ► L3 Authentication

**SETTINGS**
- Default Role: ssi-guest
- Redirect Pause: 1
- User Login: ✗
- Guest Login: ✗
- Logout Popup Window: ✗
- Use HTTP for authentication: ✔
- Show FQDN: ✔
- Authentication Protocol: PAP
- Login Page: http://socialsign.in/spot
- Welcome Page: http://socialsign.in/spot/success
- Show Welcome Page: ✔
- Add switch IP address in the redirection URL: ✔
- White List: add whitelist from Step 2 here
- Bypass Apple Captive Network Assistant: ✗
- Please use the Default values for the remaining settings.

Add the custom RADIUS server group from **Step 1** to this Captive Portal profile.
5 Captive Portal Profile

**NAVIGATE TO**
Security ▶ Access Control ▶ User Roles

Add this Captive Portal profile defined here to the ssi-guest-logon role. See Figure from **Step 3**.

6 SSID connection

**NAVIGATE TO**
Wireless ▶ AP Configuration ▶ <your_config> ▶ Wireless LAN ▶ Virtual AP

Add Virtual AP to main AP group

Create a new custom SSID profile, and connect your AAA Profile. Apply, and then update your guest VLAN.

- Save the Mobility Controller configuration to complete setup.