Fingerprint Finder Begin Site Configuration Guide

Introduction

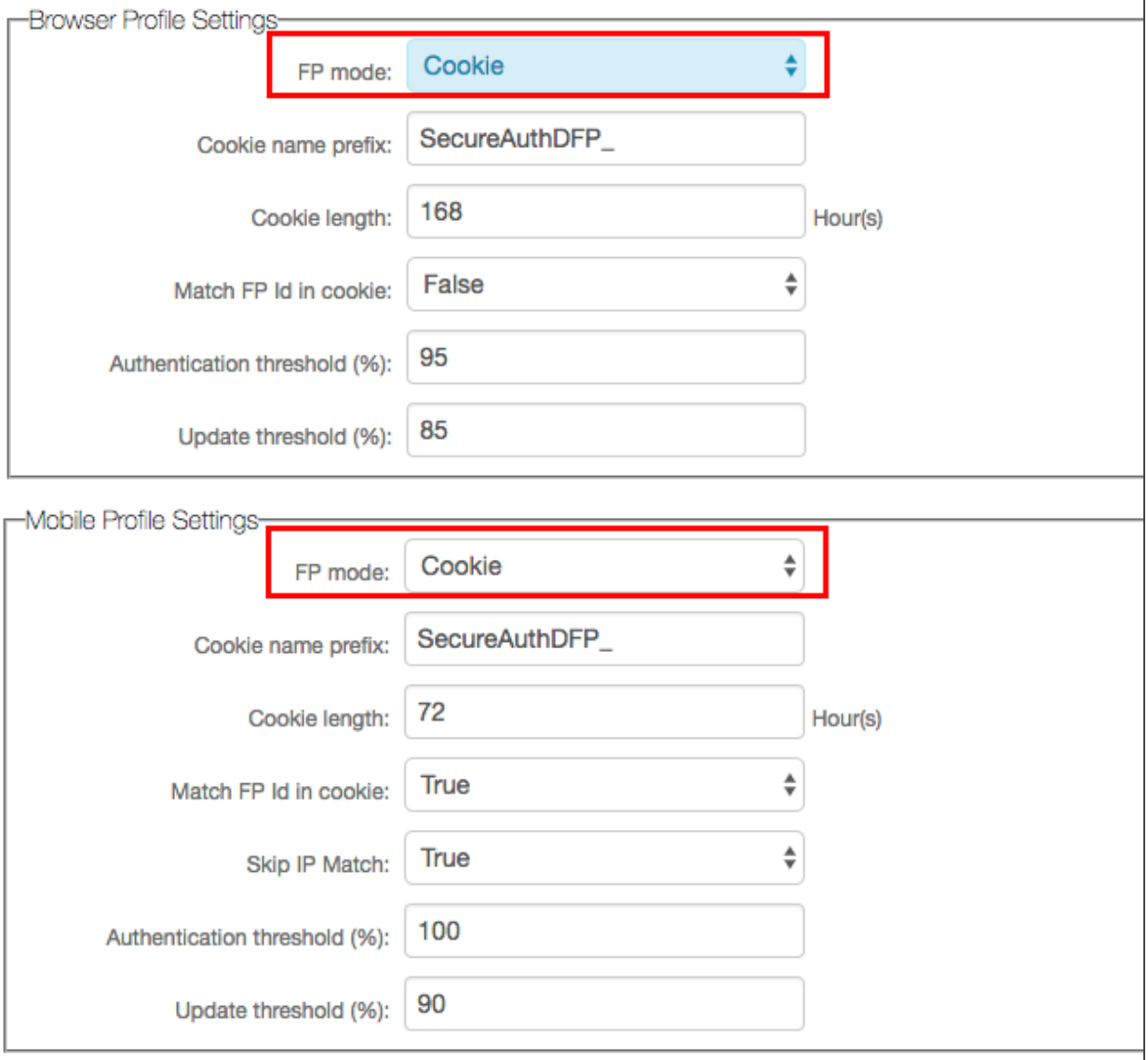
Use this guide to enable a SecureAuth IdP realm to utilize a **Fingerprint Finder** begin site.

At this begin site, SecureAuth IdP can search for a Device Recognition Profile cookie and extract the user ID from it. From there, the end-user follows the SecureAuth IdP workflow configured in the realm (e.g. Multi-Factor Authentication) without requiring to enter the user ID, and is asserted to the Post Authentication target.

Prerequisites

1. Have a Device / Browser Profile Cookie

In the **Device Recognition** section in the **Workflow** tab, ensure that in the **Browser Profile Settings** and **Mobile Profile Settings**, **Cookie** is selected from the **FP Mode** dropdowns



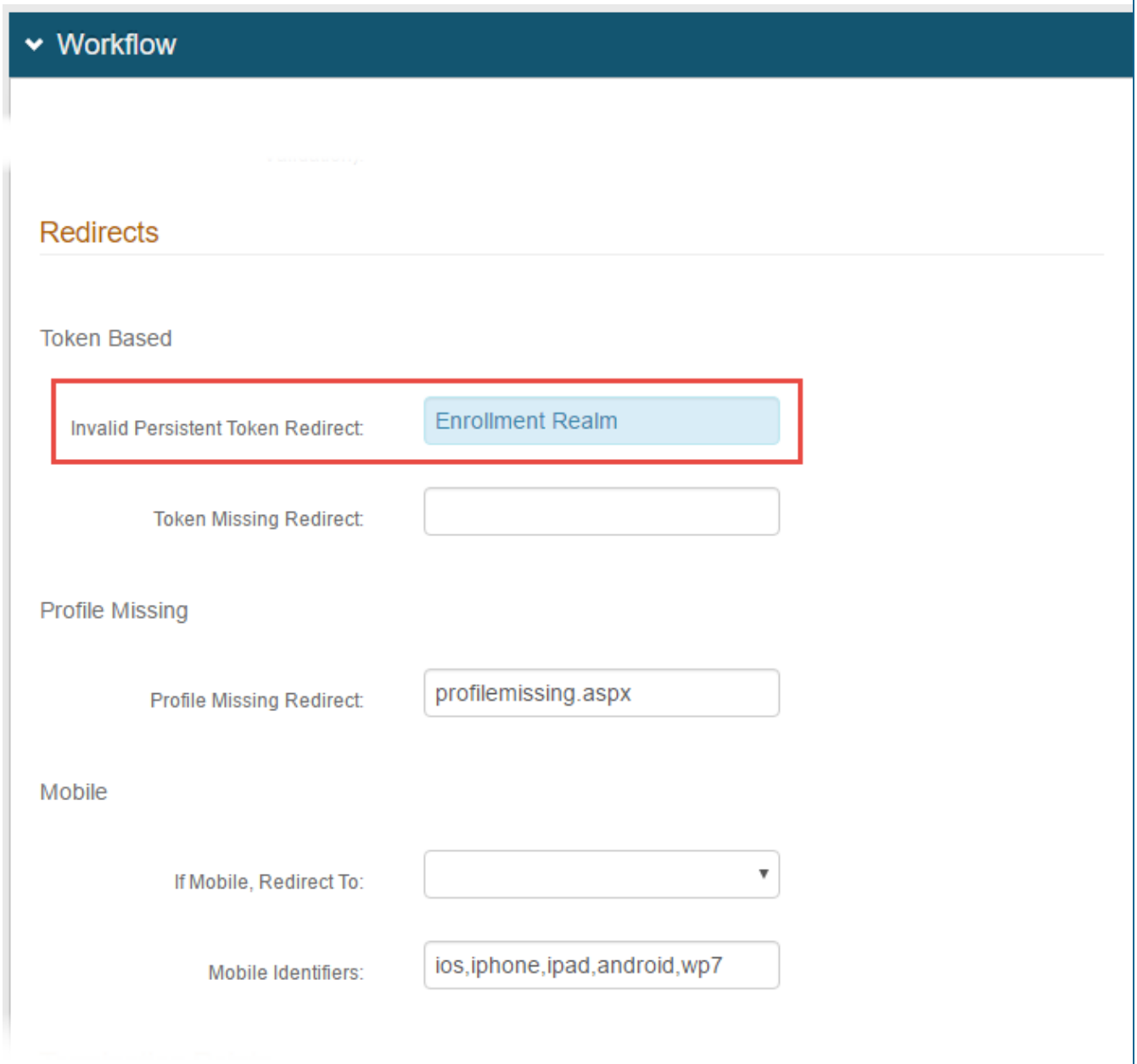
2. Create a **New Realm** or edit an existing realm to which Cert Finder applies in the SecureAuth IdP Web Admin

3. Configure the following tabs in the Web Admin before configuring for Cert Finder:

- **Overview** – the description of the realm and SMTP connections must be defined
- **Data** – an enterprise directory must be integrated with SecureAuth IdP
- **Workflow** – the way in which users will access the target must be defined
- **Multi-Factor Methods** – the Multi-Factor Authentication methods that will be used to access the target (if any) must be defined
- **Post Authentication** – the target resource or post authentication action must be defined
- **Logs** – the logs that will be enabled or disabled for this realm must be defined

SecureAuth IdP Configuration Steps

Workflow

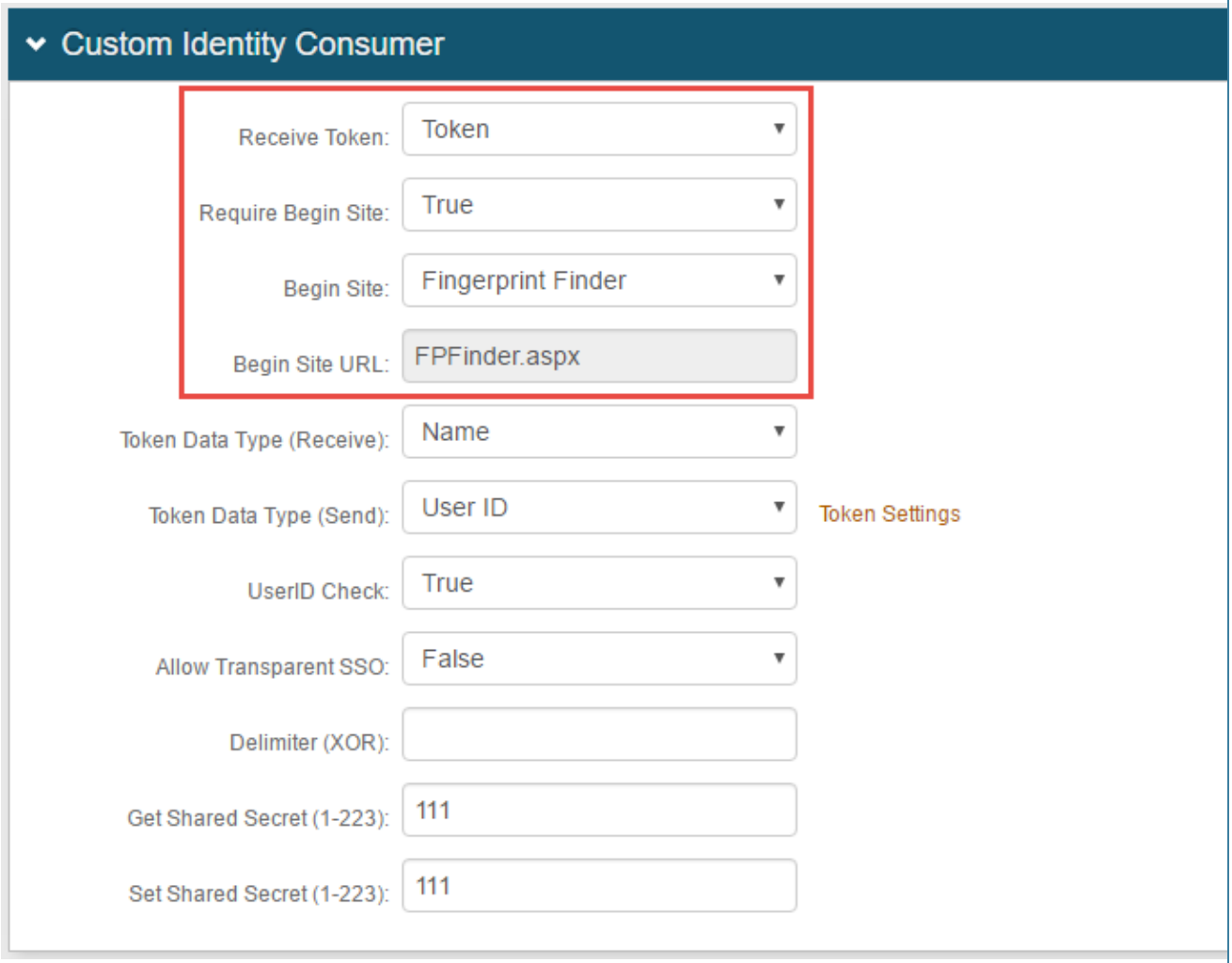


1. In the **Workflow** section, set the **Invalid Persistent Token Redirect** to the SecureAuth IdP realm in which end-users can enroll for a device / browser profile cookie

    If end-users land on the Fingerprint Finder begin site without a valid profile cookie, then they are redirected to this realm to enroll for a profile cookie that can then be used for the begin site

    It is recommended that the enrollment realm have the same Post Authentication action so that the end-user ends up at the same destination despite the realm

Custom Identity Consumer



2. Select **Token** from the **Receive Token** dropdown
3. Select **True** from the **Require Begin Site** dropdown
4. Select **Fingerprint Finder** from the **Begin Site** dropdown
5. **FPFinder.aspx** auto-populates in the **Begin Site URL** field

Click **Save** once the configurations have been completed and before leaving the **Workflow** page to avoid losing changes