Standard Multi-Factor Authentication Workflow Configuration

Introduction

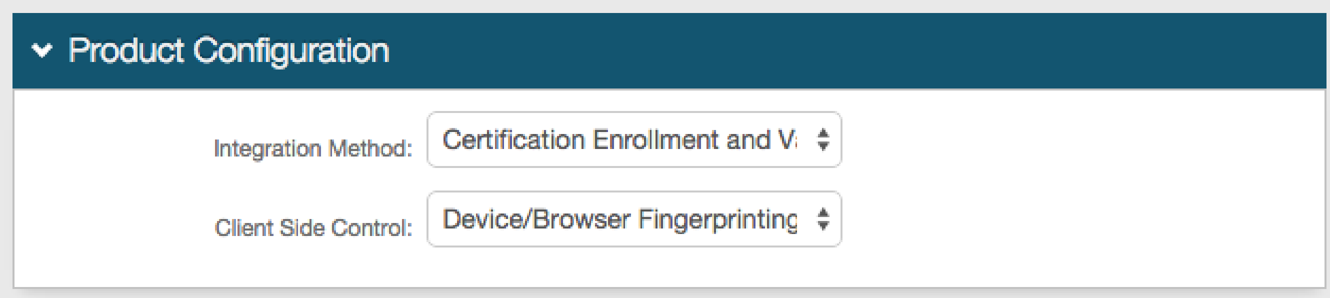
Use this guide as a reference to configure a SecureAuth IdP realm that uses the Standard Multi-Factor Authentication workflow.

The **Username | Second Factor | Password** workflow prompts the end-user for the username, then a second factor option of the end-user's choice, and then the password, in that order.

This can be applied to any realm to access web, SaaS, mobile, or network applications and devices, and SecureAuth IdP out-of-the-box Identity Management (IdM) tools via Multi-Factor Authentication.

SecureAuth IdP Configuration Steps

Workflow



Product Configuration

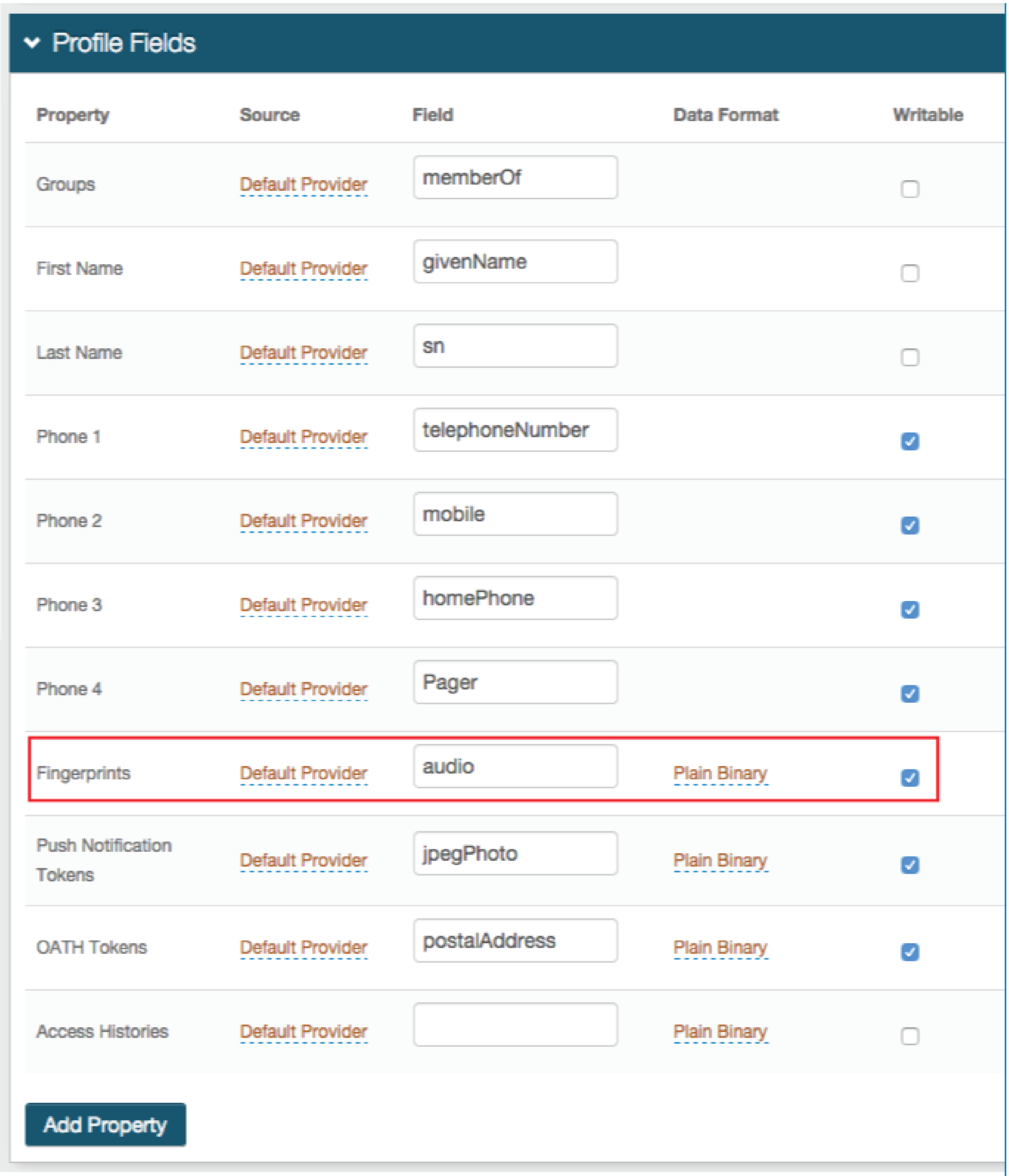
Integration Method: Certification Enrollment and V

Client Side Control: Device/Browser Fingerprinting

1. In the **Product Configuration** section, select **Certification Enrollment and Validation** from the **Integration Method** dropdown

2. Select **Device/Browser Fingerprinting** from the **Client Side Control** dropdown

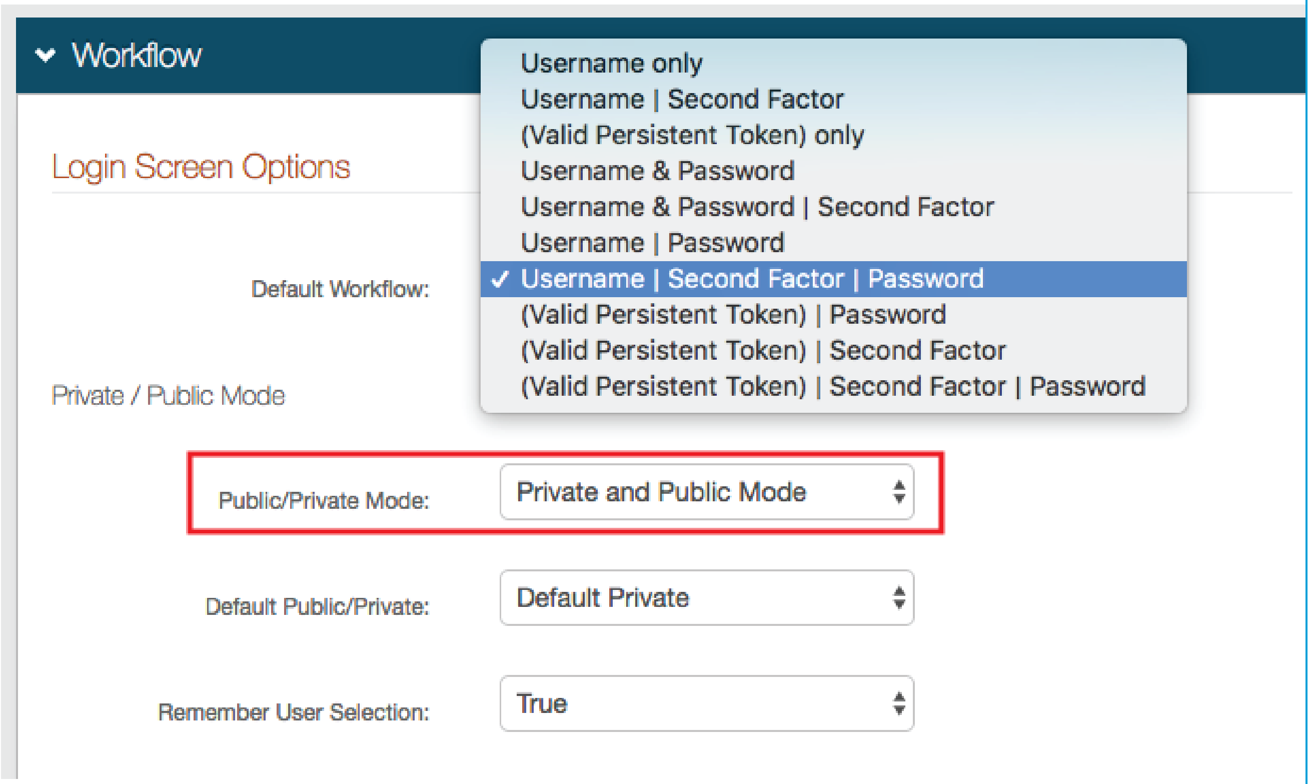
> If using a different directory than LDAP, a stored procedure must be created to contain the **Fingerprints**
>
> For LDAP data stores, the **audio** field is typically mapped to the **Fingerprints Property** in the **Data** tab
>
> The Fingerprints Property can be stored as **Plain Binary** or in **JSON** format, and has distinct requirements for the LDAP directory attribute mapped to the **Property** based on the **Data Format** selection
>
> For **Plain Binary**, these requirements must be met for the directory field that contains the device / browser profile information:
>
> - **Length**: 8 kB minimum per Profile Record; and if the **Total FP Max Count** is set to -1, then the size must be **unlimited**
> - **Data Type**: Octet string (bytes)
> - **Multi-valued**
>
> For **JSON**, these requirements must be met for the directory field that contains the profile information:
>
> - **Length**: No limit / undefined
> - **Data Type**: DirectoryString
> - **Multi-valued**



Profile Fields

Property	Source	Field	Data Format	Writable
Groups	Default Provider	memberOf		☐
First Name	Default Provider	givenName		☐
Last Name	Default Provider	sn		☐
Phone 1	Default Provider	telephoneNumber		☑
Phone 2	Default Provider	mobile		☑
Phone 3	Default Provider	homePhone		☑
Phone 4	Default Provider	Pager		☑
Fingerprints	Default Provider	audio	Plain Binary	☑
Push Notification Tokens	Default Provider	jpegPhoto	Plain Binary	☑
OATH Tokens	Default Provider	postalAddress	Plain Binary	☑
Access Histories	Default Provider		Plain Binary	☐

Workflow



Workflow
Username only
Username | Second Factor
(Valid Persistent Token) only
Username & Password
Username & Password | Second Factor
Username | Password
(Valid Persistent Token) | Password
(Valid Persistent Token) | Second Factor
(Valid Persistent Token) | Second Factor | Password

Login Screen Options

Default Workflow: ✓ Username | Second Factor | Password

Private / Public Mode

Public/Private Mode: Private and Public Mode

Default Public/Private: Default Private

Remember User Selection: True

3. Select **Username | Second Factor | Password** from the **Default Workflow** dropdown

4. Select **Private and Public Mode** or **Private Mode Only** from the **Public/Private Mode** dropdown

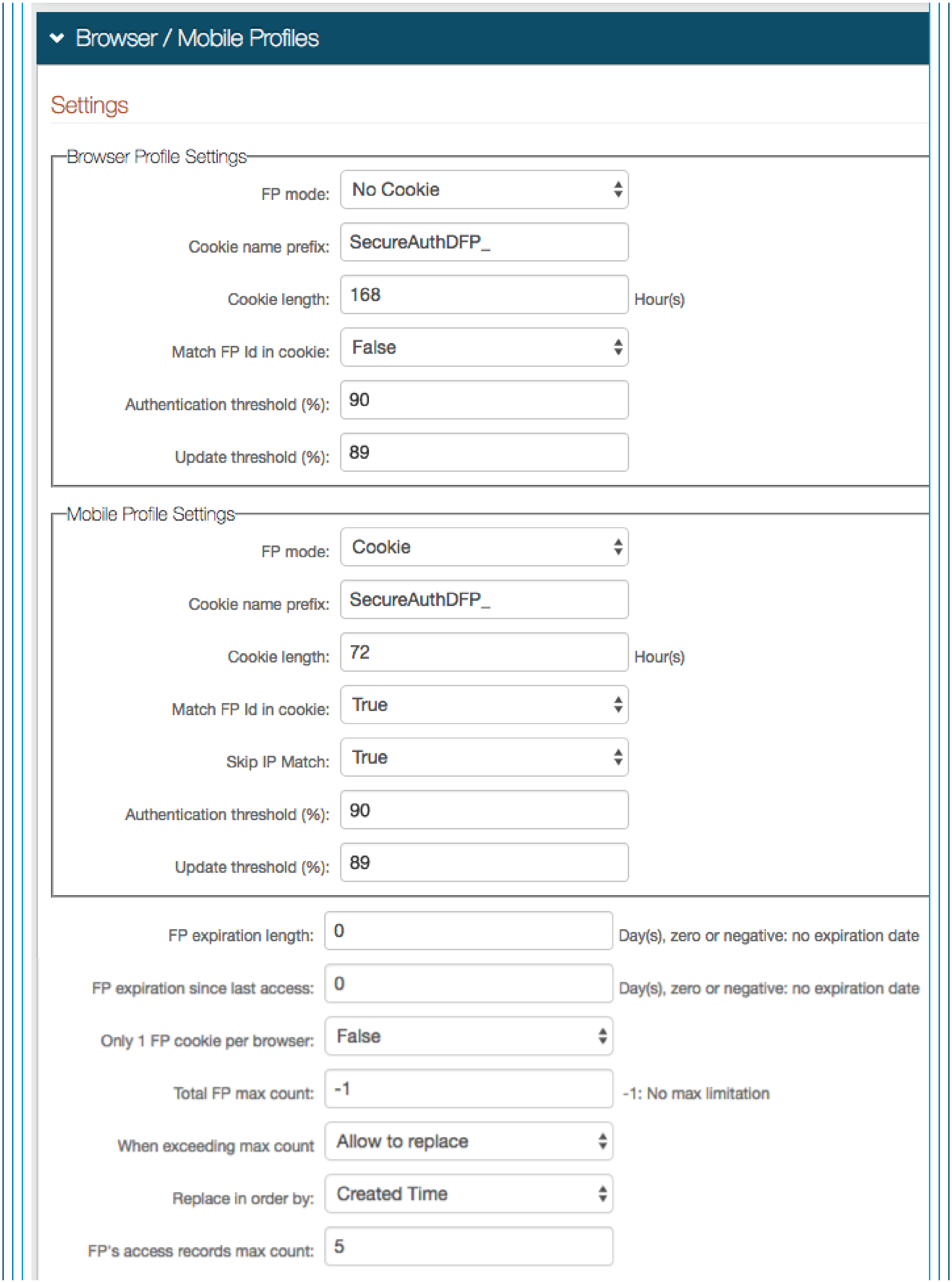
   Selecting **Private and Public Mode** or **Private Mode Only** generates a device / browser profile in this realm and checks for existing profiles

5. Select which option is selected by default on the client-side page from the **Default Public/Private** dropdown

   SecureAuth recommends selecting **Default Private** to ensure that profiles are generated and checked in the realm

6. Select **True** from the **Remember User Selection** dropdown to automatically select **Private** or **Public** on the client-side page, based on the user's previous selection

Browser / Mobile Device Digital Fingerprinting



Browser / Mobile Profiles

Settings

Browser Profile Settings

FP mode: No Cookie

Cookie name prefix: SecureAuthDFP_

Cookie length: 168 Hour(s)

Match FP Id in cookie: False

Authentication threshold (%): 90

Update threshold (%): 89

Mobile Profile Settings

FP mode: Cookie

Cookie name prefix: SecureAuthDFP_

Cookie length: 72 Hour(s)

Match FP Id in cookie: True

Skip IP Match: True

Authentication threshold (%): 90

Update threshold (%): 89

FP expiration length: 0 Day(s), zero or negative: no expiration date

FP expiration since last access: 0 Day(s), zero or negative: no expiration date

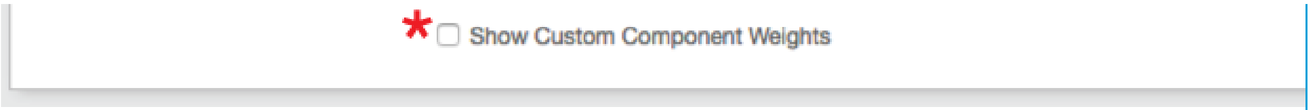
Only 1 FP cookie per browser: False

Total FP max count: -1 -1: No max limitation

When exceeding max count Allow to replace

Replace in order by: Created Time

FP's access records max count: 5



* □ Show Custom Component Weights

7. In the **Browser Profile Settings** section, select **Cookie** from the **FP Mode** dropdown to enable SecureAuth IdP to deliver a cookie to the browser after authentication; or select **No Cookie** if no cookie is to be used

8. If **Cookie** is selected in step 9, then provide the **Cookie name prefix** and **Cookie length**, or leave as default

The cookie name appears as **Cookie Name Prefix + company name + hashed value of user ID**

The **Cookie length** sets for how many hours the cookie is valid, e.g. 72 hours

9. Select **True** from the **Match FP in cookie** to require the profile ID to be presented and then matched to a profile ID in the directory, with an acceptable **Authentication Threshold** score; or select **False** to not require ID matching between the cookie and the stored profile

If **No Cookie** is selected in step 7, then steps 8 and 9 can be ignored

10. Set the **Authentication Threshold** to **90-100%** based on preference

11. Set the **Update Threshold** to a percentage just below the **Authentication Threshold**

The **Update Threshold** *must be* less than the **Authentication Threshold**

Review the **Profile Comparison Score** information below for more explanation of the Thresholds

SecureAuth IdP provides two (2) **threshold values**:

- **Authentication Threshold** (the high one) determines whether additional 2-Factor Authentication is required (OTP)
- **Update Threshold** (the low one) determines whether an existing profile is to be updated with new information from the presented profile, or if a new profile is to be created

For example, if the **Authentication Threshold** is set to **90** and the **Update Threshold** is set to **89**, then the following evaluation would be done on subsequent authentications:

<Profile-Score> represents the score of the presented profile

If <Profile-Score> 90, then no additional Multi-Factor Authentication is required

If <Profile-Score> **<** 90, but **=** 89, then additional Multi-Factor Authentication is required and the existing profile is updated with the presented profile information

If <Profile-Score> **<** 89, then additional Multi-Factor Authentication is required, and a new profile is created

12. In the **Mobile Settings** section, select **Cookie** from the **FP Mode** dropdown to deliver a cookie to the mobile device; or select **App Mode** to utilize the DR App for further device / browser validation

13. Leave the **Cookie name prefix** as the default, or set it to a preferred name

The cookie name appears as **Cookie Name Prefix + company name + hashed value of user ID**

14. Set the **Cookie Length** to the amount of hours during which the cookie is valid, e.g. 72 Hours

15. Select **True** from the **Match FP in cookie** to require the profile ID to be presented and then matched to a profile ID in the directory, with an acceptable **Authentication Threshold** score; or select **False** to not require ID matching between the cookie and the stored profile

If **App Mode** is selected in step 12, then steps 13 - 15 can be ignored

16. Select **True** from the **Skip IP Match** dropdown to not require an exact IP Address match for profile comparison; or select **False** to require an exact match

17. Set the **Authentication Threshold** to **90-100%** based on preference

18. Set the **Update Threshold** to a percentage just below the **Authentication Threshold**

The **Update Threshold** *must be* less than the **Authentication Threshold**

See **Profile Comparison Score** information in step 11

19. Set the **FP expiration length** to the number of days the profile is valid

For example, if this field is set to 10 days, then the user's profile expires in 10 days, no matter how often it is used

Set to **0** for no expiration

20. Set the **FP expiration since last access** to the number of days the profile is valid since last usage

For example, if this field is set to 10 days, then the user's profile expires if it is not used during the 10 days since it was last employed

Set to **0** for no expiration

21. Set the **Total FP max count** to the maximum number of profiles that can be stored in a user's account at a given time

If a maximum is to be set, a typical configuration would limit profile storage to **5-8**

Set to **-1** for no maximum entries

22. If a maximum is set in step 21, then select **Allow to replace** from the **When exceeding max count** dropdown to enable the replacement of an existing profile with a new one; or select **Not allow to replace** if the profiles cannot be automatically replaced

If **Not allow to replace** is selected, then the user or administrator must manually remove stored profiles from the user profile on the **Self-service Account Update Page** or **Account Management (Help Desk) Page**

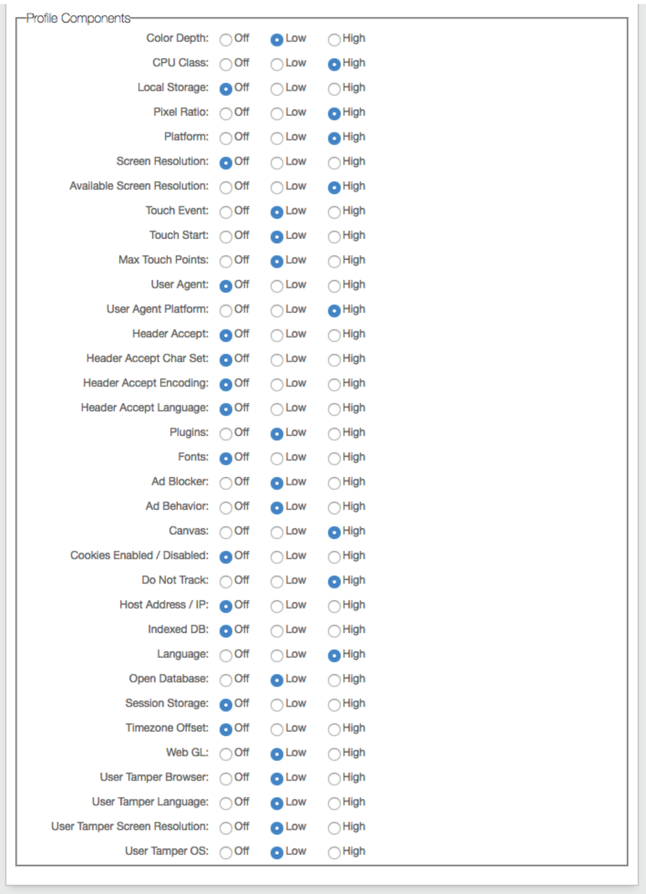
23. If a maximum is set in step 21 and **Allow to replace** is selected in step 22, then select **Created Time** from the **Replace in order by** dropdown to enable the replacement of the oldest stored profile with the new one; or select **Last Access Time** to enable the replacement of the least recently used profile with the new one

24. Set the **FP's access records max count** to the number of access history entries per profile stored in the profile

SecureAuth recommends setting this to **5**

* Check **Show Custom Component Weights** to modify the defaulted weights of each profile's components

Custom Component Weights



Profile Components

Color Depth:	○ Off	● Low	○ High
CPU Class:	○ Off	○ Low	● High
Local Storage:	● Off	○ Low	○ High
Pixel Ratio:	○ Off	○ Low	● High
Platform:	○ Off	○ Low	● High
Screen Resolution:	● Off	○ Low	○ High
Available Screen Resolution:	○ Off	○ Low	● High
Touch Event:	○ Off	● Low	○ High
Touch Start:	○ Off	● Low	○ High
Max Touch Points:	○ Off	● Low	○ High
User Agent:	● Off	○ Low	○ High
User Agent Platform:	○ Off	○ Low	● High
Header Accept:	● Off	○ Low	○ High
Header Accept Char Set:	● Off	○ Low	○ High
Header Accept Encoding:	● Off	○ Low	○ High
Header Accept Language:	● Off	○ Low	○ High
Plugins:	○ Off	● Low	○ High
Fonts:	● Off	○ Low	○ High
Ad Blocker:	○ Off	● Low	○ High
Ad Behavior:	○ Off	● Low	○ High
Canvas:	○ Off	○ Low	● High
Cookies Enabled / Disabled:	● Off	○ Low	○ High
Do Not Track:	○ Off	○ Low	● High
Host Address / IP:	● Off	○ Low	○ High
Indexed DB:	● Off	○ Low	○ High
Language:	○ Off	○ Low	● High
Open Database:	○ Off	● Low	○ High
Session Storage:	● Off	○ Low	○ High
Timezone Offset:	● Off	○ Low	○ High
Web GL:	○ Off	● Low	○ High
User Tamper Browser:	○ Off	● Low	○ High
User Tamper Language:	○ Off	● Low	○ High
User Tamper Screen Resolution:	○ Off	● Low	○ High
User Tamper OS:	○ Off	● Low	○ High

Set the components based on how profiles should be analyzed against the Thresholds

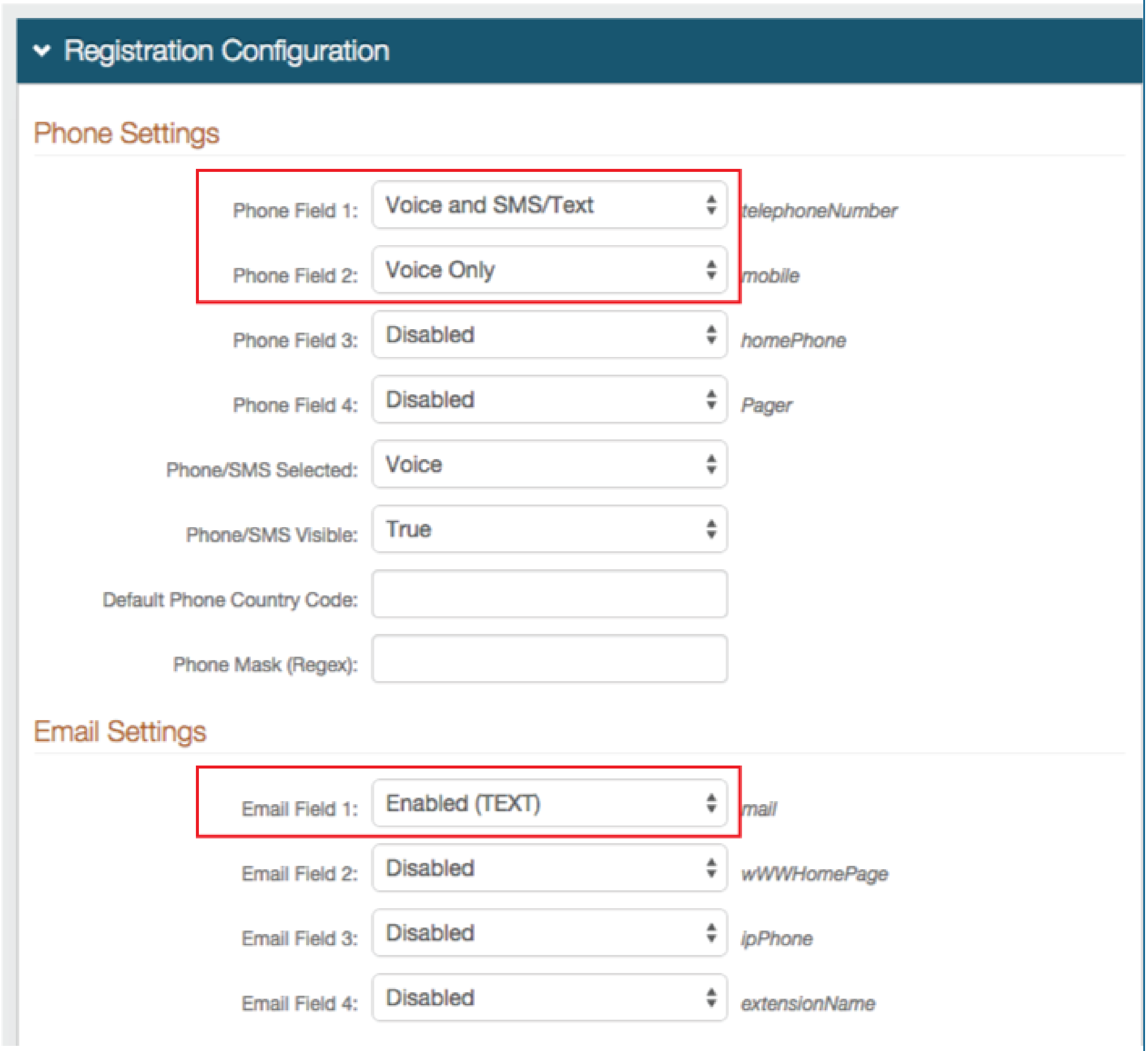
- **Off:** Component is not considered in profile analysis
- **Low:** Component is considered in profile analysis with low effect (small changes do not drastically change profile)
- **High:** Component is considered in profile analysis with high effect (small changes could drastically change profile, requiring new profile for device / browser)

Refer to the table below for specific component information

Component	Definition	Affected by (example)	Default Weight
Color Depth	Number of bits used to indicate the color of single pixel or number of bits used for each color component of single pixel	Settings change	Off
CPU Class	Classification of central processing unit (CPU)	New device	High
Local Storage	Has local storage or not	Settings change (true / false)	Low
Pixel Ratio	Comparison of width and height of pixel	New device	High
Platform	Framework on which applications run	New platform type	Off
Screen Resolution	Clarity of text and images displayed on screen	Laptop dock, settings change	Off
Available Screen Resolution	Available screen space on display	Laptop dock, settings change, menu bar location	High
Touch Event	Touch screen detection and capabilities	Settings change, mobile to desktop device change	Off
Touch Start			
Max Touch Points			
User Agent	Information about browser and operating system	New browser	High
User Agent Platform	Native platform on which browser runs; mobile platform identifier	New platform type	Off
Header Accept	Supported content types	Settings change	Off
Header Accept Char Set	Supported character set	Settings change	Off
Header Accept Encoding	Supported encoding algorithms	Settings change	Off
Header Accept Language	Supported languages	Settings change	Off
Plugins	List of native plugins	Native plugin addition / removal	High
Fonts	List of browser fonts	Font addition / removal	High
Ad Blocker	Installation of AdBlock	Settings change (true / false)	Off
Add Behavior	Installation of IE specific AddBehavior	Settings change (true / false)	Off
Canvas	HTML5 API used to draw graphics and animations on web page via scripting in JavaScript	New browser	High
Cookies Enabled / Disabled	Browser cookies setting	Settings change (true / false)	Low
Do Not Track	Enablement of DoNotTrack	Settings change (true / false)	Low
Host Address / IP	Host / IP address of device	Network connection change	High
Indexed DB	Has indexed DB or not	Settings change (true / false)	Off
Language	Browser language	Language settings change	High
Open Database	Browser storage allowed in open database	Settings change (true / false)	Off
Session Storage	Has session storage or not	Settings change (true / false)	Off
Timezone Offset	Amount of time subtracted from or added to UTC to get current time	Location change	High
Web GL	JavaScript API for rendering interactive 3D graphics within compatible web browser without use of plug-ins	New device	High
User Tamper Browser	Has user tampered with browser	Tampering (true / false)	Off
User Tamper Language	Has user tampered with language settings		
User Tamper Screen Resolution	Has user tampered with screen resolution settings		
User Tamper OS	Has user tampered with OS settings		

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

Multi-Factor Methods



Registration Configuration

Phone Settings

Phone Field 1:	Voice and SMS/Text	*telephoneNumber*
Phone Field 2:	Voice Only	*mobile*
Phone Field 3:	Disabled	*homePhone*
Phone Field 4:	Disabled	*Pager*
Phone/SMS Selected:	Voice	
Phone/SMS Visible:	True	
Default Phone Country Code:		
Phone Mask (Regex):		

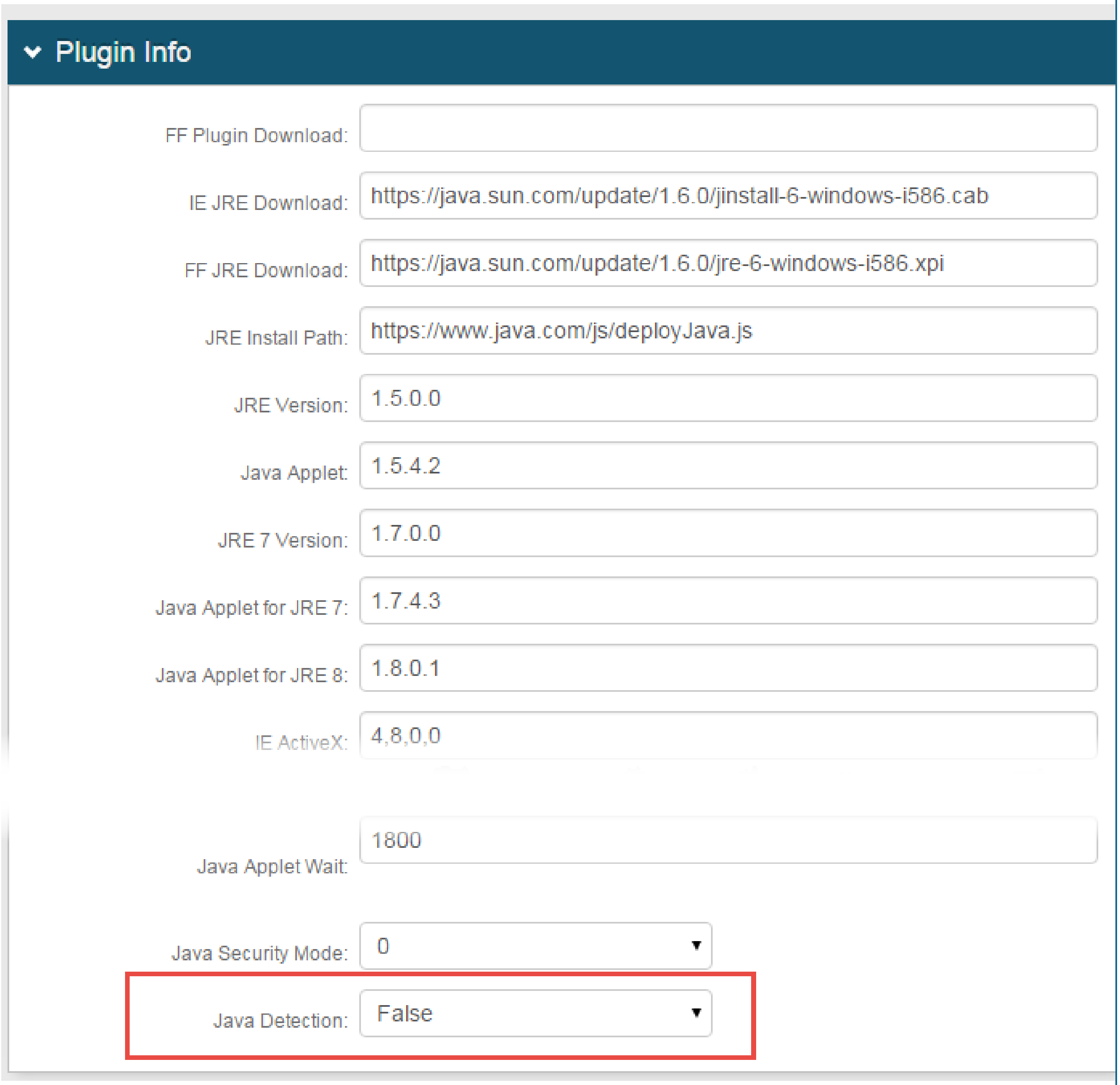
Email Settings

Email Field 1:	Enabled (TEXT)	*mail*
Email Field 2:	Disabled	*wWWHomePage*
Email Field 3:	Disabled	*ipPhone*
Email Field 4:	Disabled	*extensionName*

25. In the **Registration Configuration** section, ensure that at least one registration method is enabled for use in this realm

Click **Save** once the configurations have been completed and before leaving the **Multi-Factor Methods** page to avoid losing changes

System Info



Plugin Info

FF Plugin Download:	
IE JRE Download:	https://java.sun.com/update/1.6.0/jinstall-6-windows-i586.cab
FF JRE Download:	https://java.sun.com/update/1.6.0/jre-6-windows-i586.xpi
JRE Install Path:	https://www.java.com/js/deployJava.js
JRE Version:	1.5.0.0
Java Applet:	1.5.4.2
JRE 7 Version:	1.7.0.0
Java Applet for JRE 7:	1.7.4.3
Java Applet for JRE 8:	1.8.0.1
IE ActiveX:	4,8,0,0
Java Applet Wait:	1800
Java Security Mode:	0 ▾
Java Detection:	False ▾

26. In the **Plugin Info** section, select **False** from the **Java Detection** dropdown

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

End-user Experience