Copyright Information

2017. SecureAuth® is a copyright of SecureAuth Corporation. SecureAuth’s IdP software, appliances, and other products and solutions, are copyrighted products of SecureAuth Corporation.

May, 2017

For information on supporting this product, contact your SecureAuth sales representative:

Email: support@secureauth.com
Phone: +1.949.777.6959 or +1-866- 859-1526
Website: https://www.secureauth.com/Support.aspx
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Getting There</td>
<td>2</td>
</tr>
<tr>
<td>Best Practices for Weighing FP Components</td>
<td>10</td>
</tr>
</tbody>
</table>
Introduction

SecureAuth IdP can collect client-unique information (digital fingerprints) from the end-user’s device or browser in order to authenticate the end-user. Digital fingerprints are a profile of a specific device or browser comprising fourteen distinct attributes. Each of these attributes is given a weight or degree of importance within the whole and only those devices matching the weighted components in the profile are allowed access without additional authentication.

Once the digital fingerprint is collected after a successful Multi-Factor Authentication (MFA), it will be accepted and stored in the user profile in the directory.

When the end-user utilizes the same device or browser to log into SecureAuth IdP again, the current client-unique information (a new digital fingerprint) is collected and compared with the previously registered fingerprint(s) for authentication.

If a requesting digital fingerprint matches the currently stored digital fingerprint (with an acceptable Authentication Threshold score), the end-user will not be required to undergo additional 2-Factor Authentication (2FA).

Device recognition or digital fingerprinting includes the following elements:

+ First-time authentication – register the device or browser digital fingerprint
+ Subsequent authentications – validate the device against a stored digital fingerprint
+ Digital fingerprints include characteristics about a device or browser such as these:
  - Web browser configuration
  - Language
  - Installed fonts
  - Browser plug-ins
  - Device IP address
  - Screen resolution
  - Browser cookie settings
  - Time zone
  - HTML local storage
  - User agent
  - Content-Types
  - Character sets
  - Encodings

**NOTE:** In the next version of SecureAuth IdP, many references to digital fingerprinting will be changed to Device/Browser Recognition.
Getting There

Before we focus on the device recognition parameters, let’s review the steps we take to get there.

1. In SecureAuth IdP Web Admin, create a realm that will be used to handle device recognition.

2. On the Data tab, scroll down to the Membership Connection Settings section and map a directory field to the Fingerprints property.

   ![Membership Connection Settings Section](image)

   FIGURE 1. Membership Connection Settings Section

   In a typical AD deployment, the Data Format is Plain Binary and the audio directory field is utilized as shown in Figure 1.

3. Check the Writable box.

4. Click Save to confirm changes to the Data page.

5. Click the Workflow tab.

6. Scroll down to the Product Configuration section and select Certification Enrollment and Validation from the Integration Method drop-down list.
7. Select **Device/Browser Fingerprinting** from the **Client Side Control** drop-down list.

![Product Configuration Section](image)

**FIGURE 2.** Product Configuration Section

8. Scroll down to the Public/Private Mode field and the fields that follow like the example in Figure 3 on page 4.
FIGURE 3. Product Configuration Section (Continued)

9. Select options or enter information for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public/Private Mode</td>
<td>Select Private and Public Mode or Private Mode Only. Selecting Private and Public Mode or Private Mode Only generates a digital fingerprint in this realm and checks for device recognition.</td>
</tr>
<tr>
<td>Default Public/Private</td>
<td>Select the option designated by default on the client-side page SecureAuth recommends selecting Default Private to ensure that digital fingerprints are generated and checked in the realm.</td>
</tr>
</tbody>
</table>
10. Scroll down to the **Browser/Mobile Device Digital Fingerprinting** section that looks like the example in Figure 4.

![Weights of FP Components](image)

**FIGURE 4.** Weights of FP Components

11. Set the Weights of each component to indicate the significance of that element. The weights of each HTTP Headers and System Components setting together must equal 100%. For more on this, refer to the next section “Best Practices for Weighing FP Components” on page 10.
12. Scroll down to the **Settings** section which looks like the example in Figure 5.

![FP Settings](image)

**FIGURE 5.** FP Settings

Select options or enter information for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Normal Browser Settings</strong></td>
<td></td>
</tr>
<tr>
<td>FP Mode</td>
<td>Select <strong>Cookie</strong> from the drop-down field to enable SecureAuth IdP to deliver a cookie to the browser after authentication. If this option is selected, the Cookie name prefix and Cookie length are activated. Select <strong>No Cookie</strong> if no cookie is to be used.</td>
</tr>
<tr>
<td>Cookie name prefix</td>
<td>If the <strong>Cookie</strong> option is selected in FP Mode, either enter a desired prefix or keep the default value. The cookie name format appears as Cookie Name Prefix + company name + hashed value of user ID.</td>
</tr>
<tr>
<td>Cookie length</td>
<td>If the <strong>Cookie</strong> option is selected in FP Mode, specify how many hours the cookie is valid, such as 72 hours.</td>
</tr>
<tr>
<td>Match FP in cookie</td>
<td>Select <strong>True</strong> to require the digital fingerprint ID to be presented and then matched to a digital fingerprint ID in the directory, with an acceptable Authentication Threshold score. Select <strong>False</strong> to not require ID matching between the cookie and the stored digital fingerprint.</td>
</tr>
</tbody>
</table>
### Authentication Threshold

Determines whether additional 2FA is required (OTP). Set in the range **90-100%** based on preference.

This value must be greater than the Update Threshold value.

For example, if the Authentication Threshold is set to 95 and the Update Threshold is set to 85, then the following evaluation would be done on subsequent authentications:

- If \(<\text{FP-Score}\) > 95, then no additional 2FA is required
- If \(<\text{FP-Score}\) < 95, but > 85, then additional 2FA is required and the existing digital fingerprint is updated with the presented fingerprint information
- If \(<\text{FP-Score}\) < 85, then additional 2FA is required, and a new digital fingerprint will be created

### Update Threshold

Determines whether an existing digital fingerprint is to be updated with new information from the presented digital fingerprint, or if a new digital fingerprint must be created. Set to the range **80-90%** based on preference.

This value must be less than the Authentication Threshold value.

### Mobile Settings

#### FP Mode

Select **Cookie** to deliver a cookie to the mobile device. The Cookie name prefix, Cookie Length, and Match FP ID to cookie fields are activated.

Select **App Mode** to utilize the DR App for further device recognition. The App Mode option requires the SecureAuth Device Recognition (DR) App for iOS and Android.

#### Cookie name prefix

If the **Cookie** option is selected in FP Mode, leave as the default or set it to a preferred name.

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

#### Cookie Length

If the **Cookie** option is selected in FP Mode, set to the amount of hours during which the cookie is valid, such as 72 hours.

#### Match FP ID in cookie

If the **Cookie** option is selected in FP Mode, select **True** to require the digital fingerprint ID to be presented and then matched to a digital fingerprint ID in the directory, with an acceptable Authentication Threshold score.

Select **False** to not require ID matching between the cookie and the stored digital fingerprint.

#### Skip IP Match

Select **True** if an exact IP Address match for device recognition comparison is not required.

Select **False** to require an exact match for device recognition comparison.
Authentication Threshold  
Determines whether additional 2FA is required (OTP). Set in the range 90-100% based on preference.  
The Authentication Threshold value must be greater than the Update Threshold.  
For example, if the Authentication Threshold is set to 95 and the Update Threshold is set to 85, then the following evaluation would be done on subsequent authentications:  
+ If <FP-Score> > 95, then no additional 2FA is required  
+ If <FP-Score> < 95, but > 85, then additional 2FA is required and the existing fingerprint is updated with the presented digital fingerprint information  
+ If <FP-Score> < 85, then additional 2FA is required, and a new digital fingerprint will be created  

Update Threshold  
Determines whether an existing digital fingerprint is to be updated with new information from the presented digital fingerprint, or if a new digital fingerprint must be created. Set in the range 80-90% based on preference.  
The Update Threshold value must be less than the Authentication Threshold.  

FP expiration length  
Set to the number of days the digital fingerprint is valid. Set to 0 for no expiration.  
For example, if this field is set to 10 days, then the user’s fingerprint expires in 10 days, no matter how often it is used.  

FP expiration since last access  
Set to the number of days the digital fingerprint is valid since the last usage. Set to 0 for no expiration.  
For example, if this field is set to 10 days, then the user’s digital fingerprint expires if it is not used during the 10 days since it was last employed.  

Total FP max count  
Set to the maximum number of digital fingerprints that can be stored at a given time. Set to -1 for no maximum entries.  
If a maximum is to be set, a typical configuration would limit digital fingerprint storage to 5-8.  

When exceeding max count  
If a maximum value is specified in Total FP max count, select Allow to replace to enable the replacement of an existing digital fingerprint with a new one, or select Not allow to replace if the digital fingerprints cannot be automatically replaced.  
If Not allow to replace is selected, the user or administrator must manually remove stored fingerprints from the user profile on the Self-service Account Update Page or Account Management (Help Desk) Page.
13. Click **Save** to confirm changes to the **Workflow** page.
14. Click the **System Info** tab.
15. In the **Plugin Info** section, select **False** from the **Java Detection** field drop-down list.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace in order by</td>
<td>If a maximum is specified in Total FP max count and <strong>Allow to replace</strong> is selected above, select <strong>Created Time</strong> to enable the replacement of the oldest stored digital fingerprint with the new one; or select <strong>Last Access Time</strong> to enable the replacement of the least recently used digital fingerprint with the new one.</td>
</tr>
<tr>
<td>FP’s access records max count</td>
<td>Set to the number of access history entries per digital fingerprint stored in the profile. SecureAuth recommends set this value to 5.</td>
</tr>
</tbody>
</table>

16. Click **Save** to confirm changes to the **System Info** page.

For more information on deploying and configuring for digital fingerprinting, refer to [https://docs.secureauth.com/pages/viewpage.action?pageId=40045162](https://docs.secureauth.com/pages/viewpage.action?pageId=40045162).
Best Practices for Weighing FP Components

In order to create unique digital fingerprints for a device or browser, you must specify the number of components on which the profile is based and how each component is weighed.

The Weights for FP Profiles are configured on the Flow page under the Weights of FP Components section as shown in the following example.

As explained in the previous section, the total values designated in these fourteen fields must add up to 100%. It is the way in which these values are prioritized that determines how SecureAuth treats them during the detection process and how the program algorithm
computes the score that determines the profile assigned. This section provides you with recommendations on what weights are best assigned to each component.

<table>
<thead>
<tr>
<th>Weighted Field</th>
<th>Description/Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Agent</strong></td>
<td>The user agent string (identification) of the user agent. This field is a highly important value, indicating the identity of the device to a high degree, and should be assigned up to <strong>30%</strong> of the total.</td>
</tr>
<tr>
<td><strong>Accept</strong></td>
<td>The Content-Types that are acceptable for the response. This field is one of the least important values you will assign. Recommended value for this is <strong>2-3%</strong>.</td>
</tr>
<tr>
<td><strong>Accept Charset</strong></td>
<td>The character sets that are acceptable. The weight you assign to this field depends on the importance you place on the character sets that this device utilizes. For the most part, this cannot be used as an important indication of identity. In general, we recommend assigning this field between <strong>0-2%</strong>.</td>
</tr>
<tr>
<td><strong>Accept Encoding</strong></td>
<td>The list of acceptable encodings. This field cannot normally be used as a fair judge of identity. Normally, this field can only be weighted to <strong>0-2%</strong>.</td>
</tr>
<tr>
<td><strong>Accept Language</strong></td>
<td>The list of acceptable human languages for response. Most devices use an unvarying assortment of languages. Therefore, this field can be reliably assigned a value of <strong>0-2%</strong>.</td>
</tr>
<tr>
<td><strong>Weight for Plugin list</strong></td>
<td>The list of plug-ins on the user’s browser. This value might change frequently on a person’s browser since plug-ins are frequently added, so it is not a particularly good indication of identity. We recommend setting this to <strong>5%</strong>.</td>
</tr>
<tr>
<td><strong>Weight for flash font</strong></td>
<td>The fonts inside of a flash application. This value can change frequently, depending on the flash application being used, so this is not a sensitive detector of identity. We recommend setting this to <strong>5%</strong>.</td>
</tr>
<tr>
<td><strong>Hostaddress/IP</strong></td>
<td>The Host address or IP address for this device. This is a very important factor in detecting identity. We recommend setting this weight to <strong>35-40%</strong>.</td>
</tr>
<tr>
<td><strong>Require exact match</strong></td>
<td>Click to check this box to require an exact match of the address. If enabled, the user will have to perform a different 2FA without an exact match, even if the Authentication Threshold percentage is met. In general, we do not require that this component be checked.</td>
</tr>
<tr>
<td>Weighted Field</td>
<td>Description/Recommendations</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Timezone</td>
<td>The time zone of the user’s browser. Time zones can change as the device is transported from one place to another. Since it is not a particularly good detector of identity, this can be set to 0%, unless the device or browser is know to exist in only one location, in which case the importance of this component can be increased significantly.</td>
</tr>
<tr>
<td>Screen resolution</td>
<td>The screen resolution of the device/browser. If only one screen is used, this can be an important component in determining identity; however, when a double or multiple monitor setup is used for a device, this component becomes problematic since multiple monitors are rarely of the same sort or resolution. In general, we recommend setting this weight to 5%.</td>
</tr>
<tr>
<td>HTML localstorage</td>
<td>The HTML5 local storage. This component should not change greatly and should be assigned some weight: normally, we recommend 5%.</td>
</tr>
<tr>
<td>HTML sessionstorage</td>
<td>The HTML5 session storage. This component should not change greatly and should be assigned some weight: normally, we recommend 5%.</td>
</tr>
<tr>
<td>IE userdata support</td>
<td>The Internet Explorer (IE) user data support. While some devices always use IE, there are many that use other browsers, such as Google or Firefox, or use a variety of browsers during a single session, so this is generally not a reliable indication of identity. For this reason, we recommend assigning a weight of 2.5% or less.</td>
</tr>
<tr>
<td>Cookie enabled/disabled</td>
<td>Based on the user’s settings, whether cookies are enabled or disabled. Cookies can be enabled or disabled indiscriminately, and often in the background. Therefore, this does not indicate a good evaluator of identity. For this reason, we recommend assigning a weight of 2.5% or less.</td>
</tr>
</tbody>
</table>