Device / Browser Fingerprinting - Heuristic-based Authentication

Introduction

Device / Browser Fingerprinting is included, out-of-the-box with SecureAuth IdP. This heuristic-based authentication enables end-users to securely access resources without requiring additional one-time passwords (OTPs) for 2-Factor Authentication.

While Device / Browser Fingerprinting does not require anything to be stored, it can store a credential in the device, which increases the security as there is now something client-side and something server-side that must match for a successful authentication.

End-users enroll for fingerprints by successfully authenticating through a SecureAuth IdP realm, and the fingerprints can be revoked instantly at any time by the administrator or the end-user him/herself.

Device / Browser Fingerprinting works on any mobile or desktop device and can be configured to ensure that only the actual end-user is obtaining access into the target resource.

Definitions / Descriptions

SecureAuth IdP can collect client-unique information (digital fingerprints) from the end-user's device or browser.

For desktop browsers, there are two options:

- **No Cookie**: SecureAuth IdP collects information sent from the browser itself without delivering or registering any information at the client side, such as HTTP headers and cookies.
- **Cookie**: SecureAuth IdP collects information sent from the browser itself in addition to registering a cookie at the client-side to increase security.

For mobile devices (iOS and Android), SecureAuth IdP has two (2) methods to collect information:

- **Cookie mode**: SecureAuth IdP collects information sent from the browser itself in addition to registering a cookie at the client-side to increase security.
- **App mode**: SecureAuth’s native mobile app is utilized to pull device hardware unique information (UDID, Advertiser ID, and Device ID).
  
  - The App Mode feature is currently unavailable unless the SecureAuth IdP app is already installed on a device; the feature will return in later versions.

Once the fingerprint is collected after a successful 2-Factor Authentication, 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 fingerprint) will be collected and compared with the previously registered fingerprint(s) for authentication.

If one existing fingerprint matches the current fingerprint with an acceptable Authentication Threshold score, then the end-user will not be required to undergo additional 2-Factor Authentication (OTP).

Prerequisites

1. Have iOS or Android mobile devices, or desktop devices with a browser.
2. Create a New Realm or access existing realm(s) in the SecureAuth IdP Web Admin to which Device / Browser Fingerprinting will be applied (Realm A in the SecureAuth IdP Configuration Steps).
3. (OPTIONAL) Create a New Realm or access an existing realm in the SecureAuth IdP Web Admin that is configured for the Account Management Page (help desk) to enable administrator fingerprint revocation (Realm B in the SecureAuth IdP Configuration Steps).
4. (OPTIONAL) Create a New Realm or access an existing realm in the SecureAuth IdP Web Admin that is configured for the Self-service Account Update (end-user self-service) to enable end-user fingerprint self-revocation (Realm C in the SecureAuth IdP Configuration Steps).
5. Configure the following tabs in the Web Admin before configuring for Device / Browser Fingerprinting (and Account Management Page and Self-service Account Update):

   - **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.
   - **Registration Methods** – the 2-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 (see Realm B and Realm C for specific Post Authentication configurations for Account Management Page and Self-service Account Update).
   - **Logs** – the logs that will be enabled or disabled for this realm must be defined.
### SecureAuth IdP Configuration Steps

#### Realm A

<table>
<thead>
<tr>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Property</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td>Groups</td>
</tr>
<tr>
<td>First Name</td>
</tr>
<tr>
<td>Last Name</td>
</tr>
<tr>
<td>Phone 1</td>
</tr>
<tr>
<td>Phone 2</td>
</tr>
<tr>
<td>Phone 3</td>
</tr>
<tr>
<td>Phone 4</td>
</tr>
<tr>
<td>OATH Seed</td>
</tr>
<tr>
<td>One Time OATH List</td>
</tr>
<tr>
<td>Fingerprint</td>
</tr>
<tr>
<td>Push Notification Tokens</td>
</tr>
<tr>
<td>Access Histories</td>
</tr>
</tbody>
</table>

[Add Property]
1. In the **Membership Connection Settings** section, map a directory field to the **Fingerprints Property**

   In typical deployments, the **Data Format** is **Plain Binary** and the **audio** directory field is utilized

2. Check **Writable**

   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 fingerprint information:
   - Length: 8 kB minimum per Fingerprint 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 fingerprint information:
   - Length: No limit / undefined
   - Data Type: DirectoryString
   - Multi-valued

   **NOTE:** For SQL, ASP.net, and Oracle data stores, only the **Plain Binary Data Format** is supported (configured in the **Data tab**); and for ODBC data stores, Fingerprinting is **not supported**

---

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

---

### Workflow

#### Product Configuration

- **Integration Method:** Certification Enrollment and Validation
- **Client Side Control:** Device/Browser Fingerprinting

---

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

4. Select **Device/Browser Fingerprinting** from the **Client Side Control** dropdown
5. Select **Private and Public Mode** from the **Public/Private Mode** dropdown

   Selecting **Private and Public Mode** or **Private Mode Only** will generate a browser / device fingerprint in this realm

6. Select **Default Private** from the **Default Public/Private** dropdown

7. Select **True** from the **Remember User Selection** dropdown

8. Select the preferred workflow from the **Authentication Mode** dropdown

   * If a **Valid Persistent Token** option is selected, a persistent token (e.g. device / browser fingerprint) is required to access the target resource – provide the URL to another SecureAuth IdP realm in which a device / browser fingerprint is generated (/secureauth#) in the **Invalid Persistent Token Redirect** field to appropriately redirect end-users to enroll for a persistent token to gain access in this realm

9. Provide keywords with a comma delimiter to identify mobile devices (browsers) with the user-agent string

---

**Browser / Mobile Device Digital Fingerprinting**
### Browser/Mobile Device digital fingerprinting

#### Weights of FP components

<table>
<thead>
<tr>
<th>Component</th>
<th>Weight (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP headers</strong></td>
<td></td>
</tr>
<tr>
<td>User-Agent</td>
<td>0</td>
</tr>
<tr>
<td>Accept</td>
<td>3</td>
</tr>
<tr>
<td>Accept CharSet</td>
<td>2</td>
</tr>
<tr>
<td>Accept Encoding</td>
<td>5</td>
</tr>
<tr>
<td>Accept Language</td>
<td>5</td>
</tr>
<tr>
<td><strong>System Components</strong></td>
<td></td>
</tr>
<tr>
<td>Weight for plugin list</td>
<td>20</td>
</tr>
<tr>
<td>Weight for flash fonts</td>
<td>15</td>
</tr>
<tr>
<td>Hostaddress/IP</td>
<td>15</td>
</tr>
<tr>
<td>Timezone</td>
<td>15</td>
</tr>
<tr>
<td>Screen resolution</td>
<td>5</td>
</tr>
<tr>
<td>HTML5 localStorage</td>
<td>5</td>
</tr>
<tr>
<td>HTML5 sessionStorage</td>
<td>5</td>
</tr>
<tr>
<td>IE userdata support</td>
<td>0</td>
</tr>
<tr>
<td>Cookie enabled/disabled</td>
<td>5</td>
</tr>
</tbody>
</table>

**Total Weight (%):** 100

#### Settings

**Normal Browser Settings**

- **FP mode:** No Cookie
- **Cookie name prefix:**
- **Cookie length:**
- **Match FP Id in cookie:** False
10. Set the **Weights** of each component to add or subtract significance to or from specific characteristics that will combine to create the fingerprint.

   The **HTTP Headers** and **System Components** weights must equal **100%**.

   Typical configuration is shown in the image, or defaulted in the SecureAuth IdP Web Admin.
11. In the **Normal Browser Settings** section, select **No Cookie** from the **FP Mode** dropdown

   Selecting **Cookie** will enable SecureAuth IdP to deliver a cookie to the browser after authentication

12. Leave the **Cookie name prefix** and **Cookie length** fields default or blank

   If **Cookie** is selected in step 11, provide the name and length, or leave as default

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

13. Select **False** from the **Match FP in cookie** dropdown

   Selecting **True** will require the fingerprint ID to be presented and then matched to a fingerprint ID in the directory, with an acceptable **Authentication Threshold** score

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

15. Set the **Update Threshold** to **80-90%** based on preference

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

---

**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 fingerprint is to be updated with new information from the presented fingerprint, or if a new fingerprint is to be created

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 2-Factor Authentication is required
- If <FP-Score> < 95, but > 85, then additional 2-Factor Authentication is required and the existing fingerprint is updated with the presented fingerprint information
- If <FP-Score> < 85, then additional 2-Factor Authentication is required, and a new fingerprint will be created

---

**HTTP Headers**

- **User-Agent**: The user agent string (identification) of the user agent
- **Accept**: The Content-Types that are acceptable for the response
- **Accept CharSet**: The character sets that are acceptable
- **Accept Encoding**: The list of acceptable encodings
- **Accept Language**: The list of acceptable human languages for response

**System Components**

- **Weight for plugin list**: The list of plugins on the user’s browser
- **Weight for flash font**: The fonts inside of a flash application
- **Hostaddress/IP**: The Host address or IP address
  
  **Require exact match**: Elect to require an exact match of the address. If enabled, then the user will have to perform a different 2-Factor Authentication without an exact match, even if the Authentication Threshold percentage is met.

- **Timezone**: The time zone of the user’s browser
- **Screen Resolution**: The screen resolution of the device / browser
- **HTML5 localstorage**: The HTML5 local storage
- **HTML5 sessionstorage**: The HTML5 session storage
- **IE userdata support**: The Internet Explorer (IE) user data support
- **Cookie enabled/disabled**: Based on the user’s settings, whether cookies are enabled or disabled
16. In the **Mobile Settings** section, select **Cookie** from the **FP Mode** dropdown

   The **App Mode** option can only be utilized if the SecureAuth mobile app is already installed on the app

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

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

18. Set the **Cookie Length** to the amount of hours during which the cookie will be valid, e.g. **72 Hours**

19. Select **True** from the **Match FP in cookie** dropdown

20. Select **True** from the **Skip IP Match** dropdown

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

22. Set the **Update Threshold** to **80-90%** based on preference

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

   See **Fingerprint Comparison Score** information in step 15

23. Set the **FP expiration length** to **0**, unless there will be an expiration on the fingerprint

24. Set the **FP expiration since last access** to **0**, unless there will be an expiration on the fingerprint based on usage

25. Set the **Total FP max count** to **-1**, unless there is a maximum amount of fingerprints that can be stored at a given time

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

26. Select **Allow to replace** from the **When exceeding max count** dropdown if a maximum is set in step 20

   Otherwise, leave as default

27. Select **Created Time** from the **Replace in order by** dropdown if a maximum is set in step 20

   Otherwise, leave as default

28. Set the **FP’s access records max count** to **5**

---

⚠️ **Click** **Save** once the configurations have been completed and before leaving the **Workflow** page to avoid losing changes
29. In the **Plugin Info** section, select **False** from the **Java Detection** dropdown.

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

**Realm B**

These are **optional** configuration steps to enable administrator (help desk) revocation of user fingerprints.

This realm must be set up for the **Account Management Page** post authentication action.

Refer to **Account Management (Help Desk) Page Configuration Guide** for more information.
1. Follow steps 1 - 2 in the **Realm A** configuration steps, mapping the same directory attribute to the **Fingerprints** Property

2. In the **Post Authentication** section, select **Account Management Page** from the **Authenticated User Redirect** dropdown

3. An unalterable URL is auto-populated in the **Redirect To** field, which appends to the domain name and realm number in the address bar (Authorized/ManageAccounts.aspx)

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

4. Click **Configure help desk page** to enable or disable help desk functions
<table>
<thead>
<tr>
<th>SecureAuth Field</th>
<th>Display Type</th>
<th>Datastore Fieldname</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Show Enabled</td>
<td>givenName</td>
<td>Given Name</td>
</tr>
<tr>
<td>Last Name</td>
<td>Show Enabled</td>
<td>sn</td>
<td>Surname</td>
</tr>
<tr>
<td>Phone 1</td>
<td>Show Enabled</td>
<td>telephoneNumber</td>
<td>Phone 1</td>
</tr>
<tr>
<td>Phone 2</td>
<td>Show Enabled</td>
<td>mobile</td>
<td>Phone 2</td>
</tr>
<tr>
<td>Phone 3</td>
<td>Show Enabled</td>
<td></td>
<td>Phone 3</td>
</tr>
<tr>
<td>Phone 4</td>
<td>Show Enabled</td>
<td></td>
<td>Phone 4</td>
</tr>
<tr>
<td>Email 1</td>
<td>Show Enabled</td>
<td>mail</td>
<td>Email 1</td>
</tr>
<tr>
<td>Email 2</td>
<td>Show Enabled</td>
<td>wWWHomePage</td>
<td>Email 2</td>
</tr>
<tr>
<td>Email 3</td>
<td>Show Enabled</td>
<td></td>
<td>Email 3</td>
</tr>
<tr>
<td>Email 4</td>
<td>Show Enabled</td>
<td></td>
<td>Email 4</td>
</tr>
<tr>
<td>Digital Fingerprints</td>
<td>Show Enabled</td>
<td>audio</td>
<td>Digital Fingerprints (unchck to revoke)</td>
</tr>
<tr>
<td>Push Notification Devices</td>
<td>Hide</td>
<td>jpegPhoto</td>
<td>Push notification devices (unchck to remove)</td>
</tr>
</tbody>
</table>
5. Select **Show Enabled** from the **Digital Fingerprints** dropdown to show this function on the help desk page and to enable changes (revocation)

![Digital Fingerprints](image)

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

Realm C

These are *optional* configuration steps to enable end-user self-service revocation of fingerprints

This realm must be set up for the **Self-service Account Update** post authentication action

Refer to **Self-service Account Update page configuration** for more information

Data

1. Follow steps 1 - 2 in the **Realm A** configuration steps, mapping the same directory attribute to the **Fingerprints** Property

Post Authentication
2. Select **Self Service Account Update** from the **Authenticated User Redirect** dropdown in the **Post Authentication** tab in the Web Admin

3. An unalterable URL is auto-populated in the **Redirect To** field, which appends to the domain name and realm number in the address bar (Authorized/AccountUpdate.aspx)

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

**Identity Management**

4. Click **Configure self service page** to enable or disable self-service functions

**Self Service**
<table>
<thead>
<tr>
<th>SecureAuth Field</th>
<th>Display Type</th>
<th>Datastore Filename</th>
<th>Regular Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name:</td>
<td>Show Disabled</td>
<td>givenName</td>
<td></td>
</tr>
<tr>
<td>Last Name:</td>
<td>Show Disabled</td>
<td>sn</td>
<td></td>
</tr>
<tr>
<td>Phone 1:</td>
<td>Show Enabled</td>
<td>telephoneNumber</td>
<td></td>
</tr>
<tr>
<td>Phone 2:</td>
<td>Show Enabled</td>
<td>mobile</td>
<td></td>
</tr>
<tr>
<td>Phone 3:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone 4:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email 1:</td>
<td>Hide</td>
<td>mail</td>
<td></td>
</tr>
<tr>
<td>Email 2:</td>
<td>Hide</td>
<td>WWW HomePage</td>
<td></td>
</tr>
<tr>
<td>Email 3:</td>
<td>Show Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email 4:</td>
<td>Show Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN:</td>
<td>Hide</td>
<td>homePhone</td>
<td></td>
</tr>
<tr>
<td>Digital Fingerprints:</td>
<td>Show Enabled</td>
<td>audio</td>
<td></td>
</tr>
<tr>
<td>Push Notification</td>
<td>Hide</td>
<td>jpegPhoto</td>
<td></td>
</tr>
<tr>
<td>Tokens:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Email:</td>
<td>Do not send</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redirect</td>
<td>Do not redirect</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Select **Show Enabled** from the **Digital Fingerprints** dropdown to show this function on the self-service page and to enable changes (revocation)

Click **Save** once the configurations have been completed and before leaving the **Self-service** page to avoid losing changes.