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)

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)

(OPTIONAL) 3. 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)

(OPTIONAL) 4. 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
The following configuration steps are for **any and all realms** utilizing Device / Browser Fingerprinting

Steps 1 and 2 are required for all realms in this guide (Realm A, Realm B, and Realm C)

### Profile Fields

<table>
<thead>
<tr>
<th>Property</th>
<th>Source</th>
<th>Field</th>
<th>Data Format</th>
<th>Writable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Default Provider</td>
<td>memberOf</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>First Name</td>
<td>Default Provider</td>
<td>givenName</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Last Name</td>
<td>Default Provider</td>
<td>sn</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Phone 1</td>
<td>Default Provider</td>
<td>telephoneNumber</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Phone 2</td>
<td>Default Provider</td>
<td>mobile</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Phone 3</td>
<td>Default Provider</td>
<td>homePhone</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Phone 4</td>
<td>Default Provider</td>
<td>pager</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Default Provider</td>
<td>audio</td>
<td>Plain Binary</td>
<td>✓</td>
</tr>
<tr>
<td>Push Notification Tokens</td>
<td>Default Provider</td>
<td>jpegPhoto</td>
<td>Plain Binary</td>
<td>✓</td>
</tr>
<tr>
<td>OATH Tokens</td>
<td>Default Provider</td>
<td>postalAddress</td>
<td>Plain Binary</td>
<td>✓</td>
</tr>
<tr>
<td>Access Histories</td>
<td>Default Provider</td>
<td>photo</td>
<td>Plain Binary</td>
<td>✓</td>
</tr>
</tbody>
</table>

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

   In typical AD 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**

   This step is for LDAP data stores only (AD and others)

   If using a different directory (e.g. SQL), then the **Property** needs to be configured as a stored procedure in the data store

   **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

---

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

---

Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes
5. 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 browser / device fingerprint in this realm and checks for fingerprints.

6. 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 fingerprints are generated and checked in the realm.

7. 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.

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
10. Set the **Weights** of each component to add or subtract significance to or from specific characteristics that combine to create the fingerprint.

The **HTTP Headers** and **System Components** weights together 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 **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.

12. If **Cookie** is selected in step 11, 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.

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

   **If No Cookie** is selected in step 11, then steps 12 and 13 can be ignored.

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**.
16. 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 fingerprinting validation.

17. 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**.

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

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

   > If **App Mode** is selected in step 16, then steps 17 - 19 can be ignored.

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

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 the number of days the fingerprint is valid.

   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.

   Set to 0 for no expiration.

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

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

   Set to 0 for no expiration.

25. Set the **Total FP max count** to the maximum number 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.

   Set to -1 for no maximum entries.

26. If a maximum is set in step 25, then select **Allow to replace** from the **When exceeding max count** dropdown to enable the replacement of an existing fingerprint with a new one; or select **Not allow to replace** if the fingerprints cannot be automatically replaced.

   If **Not allow to replace** is selected, then 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**.
27. If a maximum is set in step 25 and **Allow to replace** is selected in step 26, then select **Created Time** from the **Replace in order by dropd own** to enable the replacement of the oldest stored fingerprint with the new one; or select **Last Access Time** to enable the replacement of the least recently used fingerprint with the new one.

28. Set the **FP's access records max count** to the number of access history entries per fingerprint stored in the profile. SecureAuth recommends setting this to **5**

---

**System Info**

**Plugin Info**

- **FF Plugin Download:**
- **IE JRE Download:** [https://java.sun.com/update/1.6.0/jinstall-6-windows-i586.cab](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](https://java.sun.com/update/1.6.0/jre-6-windows-i586.xpi)
- **JRE Install Path:** [https://www.java.com/js/deployJava.js](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**

---

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

### Data

1. Follow steps 1-2 in the **Data** configuration steps of **Realm A**

The directory attribute used for Fingerprints (e.g. **audio**) must be the same across all SecureAuth IdP realms utilizing fingerprints to ensure consistency.

### Post Authentication

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

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

### Identity Management

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

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

Click **Save** once the configurations have been completed and before leaving the **Data** 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 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>mobiie</td>
<td></td>
</tr>
<tr>
<td>Phone 3</td>
<td>Hide</td>
<td>homePhone</td>
<td></td>
</tr>
<tr>
<td>Phone 4</td>
<td>Hide</td>
<td>pager</td>
<td></td>
</tr>
<tr>
<td>Email 1</td>
<td>Show Enabled</td>
<td>mail</td>
<td></td>
</tr>
<tr>
<td>Email 2</td>
<td>Show Enabled</td>
<td>wWwHomePage</td>
<td></td>
</tr>
<tr>
<td>Email 3</td>
<td>Show Enabled</td>
<td>physicalDeliveryOfficeName</td>
<td></td>
</tr>
<tr>
<td>Email 4</td>
<td>Show Enabled</td>
<td>faxNumber</td>
<td></td>
</tr>
</tbody>
</table>

| OATH Seed        | Show Enabled   | description                 |                    |

**Digital Fingerprints**: Show Enabled

<table>
<thead>
<tr>
<th>Push Notification Tokens</th>
<th>Hide</th>
<th>jpegPhoto</th>
<th>Digital Fingerprint Devices (Uncheck to remove)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OATH OTP Devices</td>
<td>Show Disabled</td>
<td>postalAddress</td>
<td>Push notification devices (uncheck to remove)</td>
</tr>
</tbody>
</table>

Send Email | Do not send | Email the user on successful update
Redirect  | Do not redirect | Option to redirect the user
5. Select **Show Enabled** from the **Digital Fingerprints** dropdown to show this function on the help desk page and to enable changes (revocation)

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 the **Self-service Account Update Page Configuration Guide** for more information.

---

**Data**

1. Follow steps 1-2 in the **Data** configuration steps of **Realm A**

The directory attribute used for Fingerprints (e.g. `audio`) **must be the same** across all SecureAuth IdP realms utilizing fingerprints to ensure consistency.

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

---

**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 will be auto-populated in the **Redirect To** field, which will append 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.

4. Click **Configure self service page** to enable or disable self-service functions.
<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>mobiie</td>
<td></td>
</tr>
<tr>
<td>Phone 3:</td>
<td>Hide</td>
<td>homePhone</td>
<td></td>
</tr>
<tr>
<td>Phone 4:</td>
<td>Hide</td>
<td>pager</td>
<td></td>
</tr>
<tr>
<td>Email 1:</td>
<td>Show Enabled</td>
<td>mail</td>
<td></td>
</tr>
<tr>
<td>Email 2:</td>
<td>Show Enabled</td>
<td>wWWHomePage</td>
<td></td>
</tr>
<tr>
<td>Email 3:</td>
<td>Show Enabled</td>
<td>physicalDeliveryOfficeName</td>
<td></td>
</tr>
<tr>
<td>Email 4:</td>
<td>Show Enabled</td>
<td>facsimileTelephoneNumber</td>
<td></td>
</tr>
<tr>
<td>OATH Seed:</td>
<td>Show Enabled</td>
<td>description</td>
<td></td>
</tr>
<tr>
<td>Digital Fingerprints:</td>
<td>Show Enabled</td>
<td>audio</td>
<td>Digital Fingerprint (Uncheck to remove)</td>
</tr>
<tr>
<td>Push Notification</td>
<td>Hide</td>
<td>jpegPhoto</td>
<td>Push notification</td>
</tr>
<tr>
<td>Tokens:</td>
<td></td>
<td></td>
<td>devices (uncheck)</td>
</tr>
<tr>
<td>OATH OTP Devices:</td>
<td>Show Disabled</td>
<td>postalAddress</td>
<td></td>
</tr>
<tr>
<td>Send Email</td>
<td>Do not send</td>
<td></td>
<td>Email the user on</td>
</tr>
<tr>
<td>Redirect</td>
<td>Do not redirect</td>
<td></td>
<td>successful update</td>
</tr>
</tbody>
</table>

Digital Fingerprints: **Show Enabled**
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.