Device Recognition

Device Recognition is included, out-of-the-box with SecureAuth® Identity Platform. This heuristic-based authentication enables end users to securely access resources without requiring additional one-time passwords (OTPs) for multi-factor authentication (MFA).

While Device Recognition 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 device / browser profiles by successfully authenticating through the Identity Platform realm, and the profiles can be instantly revoked at any time by the administrator or the end user.

Device Recognition 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

The Identity Platform can collect client-unique information (profiles) from the end user's device or browser.

For desktop browsers, there are two options:

<table>
<thead>
<tr>
<th>No Cookie</th>
<th>Information sent from the browser is collected in the Identity Platform, without delivering or registering any information at the client side, such as HTTP headers and cookies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookie</td>
<td>Information sent from the browser is collected in the Identity Platform, in addition to registering a cookie at the client-side to increase security.</td>
</tr>
</tbody>
</table>

For mobile devices (iOS and Android), the Identity Platform has the following method to collect information:

| Cookie | Information sent from the browser is collected in the Identity Platform, in addition to registering a cookie at the client-side to increase security. |

After a successful multi-factor authentication, the profile is created, and then accepted and stored in the user account in the directory.

When the end user logs in again to the Identity Platform using the same device (or browser), the current client-unique information (a new profile) is collected and compared with the previously registered profiles for authentication.

When an existing profile matches the current profile with an acceptable Authentication Threshold score, the end user is not prompted for multi-factor authentication.

When the device recognition cookie is used as part of the device recognition workflow, it restricts the user to have one device profile per browser in which the cookie lives.

Prerequisites

1. Have iOS or Android mobile devices, or desktop devices with a browser
2. Create a New Realm or access existing realm(s) on the Identity Platform Web Admin to which Device Recognition is applied (Realm A in the Identity Platform configuration)
3. Optional. Create a New Realm or access an existing realm in the Identity Platform Web Admin that is configured for the Account Management Page (help desk) to enable administrator device / browser profile revocation (Realm B in the Identity Platform configuration section)
4. Optional. Create a New Realm or access an existing realm in the Identity Platform Web Admin that is configured for the Self-service Account Update (end user self-service) to enable end user device / browser profile self-revocation (Realm C in the Identity Platform configuration section)
5. Configure the following tabs in the Web Admin before configuring for Device Recognition (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 the Identity Platform
   - Workflow – the way in which users access the resource must be defined
   - Multi-Factor Methods – the Multi-Factor Authentication methods that are 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 are enabled or disabled for this realm must be defined

For API configuration information, see Device Recognition Authentication API Guide.
Identity Platform configuration

The following configuration steps are for any and all realms using Device Recognition.

Important! To retain your configurations, be sure to click Save often, before leaving a tab page. Once you leave that tab, any unsaved changes are lost.

Realm A

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

1. Go to the Data tab.

   The following step is for LDAP data stores only (AD and others). If using a different directory (for example, SQL), then the Property needs to be configured as a stored procedure in the data store.

   \textbf{Note:} For SQL, ASP.net, and Oracle data stores, only the \textbf{Plain Binary} Data Format is supported and for ODBC data stores, Device Recognition is \textit{not} supported.

2. In the Profile Fields section, map a directory field to the following Property:

   \begin{tabular}{|l|l|}
   \hline
   \textbf{Fingerprints} & In typical AD deployments, set this field to audio and use the \textbf{Plain Binary} data format. \textbf{Select the Writable} check box. \\
   \hline
   
   \end{tabular}
3. Click **Save**.
4. Go to the **Workflow** tab.
5. In the **Device Recognition Method** section, set the following:
   - **Integration Method**: Set to **Certification Enrollment and Validation**.
   - **Client Side Controls**: Set to **Device/Browser Fingerprinting**.

6. In the **Workflow** section, set the following:
   - **Device** for the directory field
## Default Workflow
Set the login workflow for the end user login.

Then, a persistent token (for example, device / browser profile is required to access the target resource.

To redirect the end user to enroll for a persistent token to gain access, provide the realm URL to another Identity Platform realm. Go to the Workflow tab, in the Workflow > Redirects section and set the realm URL (for example, /Realm#) in the Invalid Persistent Token Redirect field.

### Public / Private Mode
This generates a device / browser profile in this realm and checks for existing profiles.

Set to Private and Public Mode or Private Mode Only.

### Default Public / Private
On the client-side page shown to the end user, select which option is to be selected by default.

To ensure that profiles are generated and checked in the realm, it is recommended to set to Default Private.

### Remember User Selection
On the client-side page shown to the end user, to automatically select the Private or Public option, based on the previous selection by the user, set to True.

### Browser / Mobile Profiles section, set the following:

#### Length – kB minimum per Device / Browser Profile; and if the Total FP Max Count is set to -1, then size must be unlimited

- **FP mode**
  - By default, this is set to Cookie. This indicates whether to deliver a cookie to the browser after authentication – Cookie or No Cookie

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

- **Cookie length**
  - Set the length in time in hours, the cookie is valid. For example, 72 hours.

- **Match FP ID in cookie**
  - By default, this is set to True. This requires the profile ID to presented and then matched to a profile ID in the directory with an acceptable Authentication Threshold score.

  Otherwise, if set to False, it does not require ID matching between the cookie and the stored profile.
<table>
<thead>
<tr>
<th>Mobile App Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile Profile Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>FP mode</strong></td>
<td>Set to Cookie to deliver a cookie to the mobile device after authentication.</td>
</tr>
<tr>
<td><strong>Cookie name prefix</strong></td>
<td>Keep or change the default cookie name. The cookie name appears as <strong>Cookie Name Prefix + company name + hashed value of user ID</strong>.</td>
</tr>
<tr>
<td><strong>Cookie length</strong></td>
<td>Set the length of time in hours, the cookie is valid. For example, 72 hours.</td>
</tr>
<tr>
<td><strong>Match FP ID in cookie</strong></td>
<td>By default, this is set to True. This requires the profile ID to presented and then matched to a profile ID in the directory with an acceptable Authentication Threshold score. Otherwise, if set to False, it does not require ID matching between the cookie and the stored profile.</td>
</tr>
<tr>
<td><strong>Skip IP Match</strong></td>
<td>If an exact IP address match is not required for profile comparison, set to True. Otherwise, to require an exact match, set to False.</td>
</tr>
<tr>
<td><strong>Authentication threshold (%)</strong></td>
<td>Set the Authentication threshold to a percentage number between <strong>90 and 100</strong>.</td>
</tr>
<tr>
<td><strong>Update threshold (%)</strong></td>
<td>Set the Update threshold to a percentage number just below the Authentication threshold. This number <strong>must be less than the number set in the previous field</strong>. For an explanation of thresholds, see the <strong>Profile Comparison Score</strong> information above.</td>
</tr>
<tr>
<td><strong>Other Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>FP expiration length</strong></td>
<td>Set the number of days the profile is valid. For example, when set to 10 days, the user's profile expires in days, no matter how often it is used. Set to 0 for no expiration.</td>
</tr>
<tr>
<td><strong>FP expiration since last access</strong></td>
<td>Set the number of days a profile is not used since the last access; to which the profile no longer valid. For example, when set to 10 days, the user's profile expires when it hasn't been used since it was last employed. Set to 0 for no expiration.</td>
</tr>
<tr>
<td><strong>Total FP max count</strong></td>
<td>Set the maximum number of profiles that can be stored in a user's account at a given time. A typical configuration would limit a profile storage maximum from five to eight profiles. Set to -1 for no limit on profile storage maximum.</td>
</tr>
<tr>
<td><strong>When exceeding max count</strong></td>
<td>If the <strong>Total FP max count</strong> is set to a number other than -1, set to one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Allow to replace</strong> – Enable replacement of an existing profile with a new one.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Allow to replace</strong> – Profiles cannot be automatically replaced. With this option, the user or administrator must manually remove stored profiles from the user profile on the <strong>Self-service Account Update page</strong> or <strong>Account Management (Help Desk) page</strong>.</td>
</tr>
<tr>
<td><strong>Replace in order by</strong></td>
<td>If a maximum is set in the <strong>Total FP max count</strong> and <strong>Allow to replace</strong> is selected when exceeding the maximum count, set to one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Created Time</strong> – Enable replacement of the oldest stored profile with the new one.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last Access Time</strong> – Enable replacement of the most recently used profile with the new one.</td>
</tr>
</tbody>
</table>
Identity Platform 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 no additional Multi-Factor Authentication is required.

When **<Profile-Score>** represents the score of the presented profile, if **<Profile-Score>** is 90, then no additional Multi-Factor Authentication is required.

If **<Profile-Score>** is less than 90, but greater than 79, then no additional Multi-Factor Authentication is required.

FP’s access records max count

Set the number of access history entries stored in each profile. Recommended setting is 5.

### Browser / Mobile Profiles

**Settings**

**Browser Profile Settings**

- FP mode: Cookie
- Cookie name prefix: SecureAuthDFP_
- Cookie length: 168 Hour(s)
- Match FP Id in cookie: True
- 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: No max limitation
When exceeding max count: Allow to replace
Replace in order by: Created Time
FP’s access records max count: 5

8. To modify the Profile Component default weight values, select the **Show Custom Component Weights** check box.

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

- **Off** – Not considered in profile analysis
- **Low** – Profile analysis is low; small changes do not drastically change profile (small changes have low effect)
- **High** – Profile analysis is high; significant change could drastically change profile, requiring new profile for device / browser

< 90, but
As an administrator, you can view mismatched components in the Audit log. For example, if the existing profile is updated with the presented profile information.

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

**NOTE**: If the device recognition cookie is in use and the user login is in the same browser, the existing device profile will be updated with the new profile data.

For specific component information, expand the following link.

### Custom Component Weights...

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

![Profile Components](image)

- Color Depth
- CPU Class
- Local Storage
- Pixel Ratio
- Platform
- Screen Resolution
- Available Screen Resolution
- Touch Start
- Touch End
- Max Touch Points
- User Agent
- User Agent Platform
- Header Accept
- Header Accept Char Set
- Header Accept Language
- Plugins
- Fonts
- Ad Blocker
- Ad Behavior
- Canvas
- Cookies Enabled / Disabled
- Do Not Track
- Host Address / IP
- Indexed DB
- Language
- Open Database
- Session Storage
- Timezone Offset
- WebGL
- User Tamper Browser
- User Tamper Language
- User Tamper Screen Resolution
- User Tamper OS
9. Click Save.
10. Go to the System Info tab.
11. In the Plugin Info section, set the Java Detection field to False.

![Plugin Info screenshot]

12. Click Save.

13. Click Save.

Realm B

These are optional configuration steps to enable administrator (help desk) revocation of user device / browser profiles. This realm must be set up for the Account Management Page post authentication action.

For more information, see Account Management (Help Desk) Page Configuration Guide.

1. Go to the Data tab.
2. For Realm B, follow configuration step 2 as described in the Realm A section above.

The directory attribute used for device / browser profiles (for example, audio) must be the same across all the Identity Platform realms using Device Recognition to ensure consistency.

3. Click Save.
4. Go to the Post Authentication tab.
5. In the Post Authentication section, set the following:

<table>
<thead>
<tr>
<th>Authenticated User Redirect</th>
<th>Set to Account Management.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect To</td>
<td>An unalterable URL Authorized/ManageAccounts.aspx, is auto-populated in this field, which appends to the domain name and realm number in the address bar.</td>
</tr>
</tbody>
</table>

6. In the Identity Management section, click the link for Help Desk to enable or disable help desk functions.

7. On the Help Desk configuration page, set Digital Fingerprints to Show Enabled. This shows the function on the help desk page and to enable changes (revocation).

Example of Help Desk page fingerprint revocation...
These are optional configuration steps to enable end user self-service revocation of device / browser profiles. This realm must be set up for the Self-service Account Update post authentication action.

For more information see Self-service Account Update Page Configuration Guide.

1. Go to the Data tab.
2. For Realm C, follow configuration step 2 as described in the Realm A section above.

The directory attribute used for device / browser profiles (for example, audio) must be the same across all the Identity Platform realms using Device Recognition to ensure consistency.

3. Click Save.
4. Go to the Post Authentication tab.
5. In the Post Authentication section, set the following:
<table>
<thead>
<tr>
<th>Authenticated User Redirect</th>
<th>Set to Self Service Account Update.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect To</td>
<td>An unalterable URL Authorized/AccountUpdate.aspx, is auto-populated in this field, which appends to the domain name and realm number in the address bar.</td>
</tr>
</tbody>
</table>

6. In the Identity Management section, click the link for Self Service to enable or disable help desk functions.

7. On the Self Service configuration page, set Digital Fingerprints to Show Enabled. This shows the function on the self service page and to enable changes (revocation).

Example of Self Service page fingerprint revocation...

<table>
<thead>
<tr>
<th>Digital Fingerprints (Uncheck to revoke)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac OS - 10.12.5 - Chrome: 7/19/2017 9:54:34 AM -07:00</td>
</tr>
<tr>
<td>Windows - 10 - Chrome: 7/19/2017 9:54:47 AM -07:00</td>
</tr>
</tbody>
</table>
8. Click **Save**.