Workflow Tab Configuration (version 9.0.1+)

Introduction

NOTE: This guide is for SecureAuth IdP versions 9.0.1+; for IdP 9.0.0 configuration, refer to Workflow Tab Configuration Guide (9.0.0), and for previous versions' configurations, refer the appropriate IdP documentation space.

Use this guide to configure the Workflow tab in the Web Admin for each SecureAuth IdP realm.

This includes Device Recognition (token and certificate properties), Workflow options (authentication modes, realm redirects, etc.), and consumption options (custom tokens, social identities, etc.).

Prerequisites

1. Create a New Realm for the target resource for which the configuration settings will apply, or open an existing realm for which configurations have already been started

2. Configure the Overview and the Data tabs in the Web Admin before configuring the Workflow tab

Workflow Configuration Steps

Device Recognition

Device Recognition Method

1. Select the Integration Method from the dropdown

   The selection made here will alter the options for Client Side Control and IE / PFX / Java Cert Type

   • Select Certification Enrollment and Validation for web-based authentication (used most frequently for majority of application integrations)
   • Select Certificate Enrollment Only for X.509 VPN authentication
   • Select Mobile Enrollment and Validation for mobile browser authentication or enrollment (e.g. native mobile apps, OATH enrollment)

2. Select the Client Side Control option from the dropdown

   The selection made here will alter the options for IE / PFX / Java Cert Type, and may require additional configuration steps
Certification Enrollment and Validation Client Side Control Options

- Select **Java Applet** to store the SecureAuth IdP X.509 certificate in the JRE managed code file set
- Select **Browser Plug-ins** to store the certificate in the native key store
- Select **Device / Browser Fingerprinting** to enable SecureAuth IdP's Fingerprinting mode, which pulls unique characteristics from the device or browser and stores them as a value in the user directory rather than storing a cookie or certificate on the client

The **Universal Browser Credential (UBC)** has been deprecated for IdP versions 9.0+, but is still supported for earlier product versions

Certificate Enrollment Only Client Side Control Options

The **Client Side Control** will be set to **Browser Plug-ins / Keygen** (no other option)
Mobile Enrollment and Validation Client Side Control Options

- Select **Browser Credential** to store a cookie in the browser
- Select **Device / Browser Fingerprinting** to enable SecureAuth IdP’s Fingerprinting mode, which pulls unique characteristics from the device or browser and stores them as a value in the user directory rather than storing a cookie or certificate on the client

The Universal Browser Credential (UBC) has been deprecated for IdP versions 9.0+, but is still supported for earlier product versions

3. Select the **IE / PFX / Java Cert Type** from the dropdown
   This is based on the security preference

Step 3 is not required if **Device / Browser Fingerprinting** is selected in step 2, but the **Browser / Mobile Device Digital Fingerprinting** section appears and requires configuration

Certificate / Token Properties
4. Select **Password Expiration Date** from the **Certificate Expiration** dropdown if the certificate is to expire when the password expires.

   Select **Private Mode Cert Length** if the certificate is to expire after a designated number of days.

5. Select **Cert Expiration Date** from the **Certificate Valid Until** if the certificate is to remain valid up until the expiration.

   Select **Private Mode Cert Length** if the certificate is to remain valid during a designated number of days.

6. Set the number of days during which a certificate does not expire and remains valid in the **Private Mode Cert Length** field if **Private Mode Cert Length** was selected in step 4 or 5.

7. Set the number of hours during which the Public Mode Certificate is valid in the **Public Mode Cert Length** field.

   This is only for realms in which **Certificate Enrollment** is selected from the **Integration Mode** dropdown in the **Device Recognition Method** section.

8. Set the number of hours during which the cookie delivered to a mobile device is valid in the **Mobile Credential Length** field (browser credential).

9. Provide a maximum amount of certificates that a user can have at a time in the **Global Cert Limit** field (optional).

10. Provide a maximum amount of mobile cookies that a user can have at a time in the **Global Mobile Limit** field (optional).

11. Select **Fall Back to 2nd Factor** or **Display Error Message** from the **Check CRL** dropdown for SecureAuth IdP to check the Certificate Revocation List.

   Select **Disabled** to opt out of checking the CRL as it is not necessary with SecureAuth IdP.

12. Click **Configure Email Notification** to enable and set up **Expired Certificate Warning** emails (optional).
13. Select **Enabled** from the **Email Notification** dropdown to enable the warning notifications.

14. Select **True** from the **Multiple Certs per User** dropdown to notify users of all certificate expirations, rather than just one.

15. Select the **Email Property** that corresponds to the data store field that contains the user's email address to which the notifications are sent from the **Email Field** dropdown.

16. Set the number of days before the expiration on which the notifications begins in the **Warning Period** field.

17. Select **Daily** from the **Notification Interval** dropdown if an email notification is to be sent once a day.

18. Set the **Notification Start Time** at which the email is sent.

---

**Browser / Mobile Device Fingerprinting**

The following configuration steps are only required if **Device / Browser Fingerprinting** is selected in step 2 as the **Client Side Control** option.

Refer to **Device / Browser Fingerprinting - Heuristic-based Authentication** for more configuration information.

---

**Weights of FP Components**

The image shows the weights of different components for browser/mobile device fingerprinting. The total weight is calculated as 100%. The components include:
- **User Agent**: 15%
- **Accept**: 2%
- **Accept-Charset**: 2%
- **Accept-Encoding**: 9%
- **Accept-Language**: 5%
- **Screen-Resolution**: 6%
- **HTML5 Environment**: 9%
- **HTML2 Environment**: 5%
- **Flash**: 2.5%
- **Cors-enabled-Status**: 2.5%

The image also includes a more detailed breakdown of each component's weight.
19. 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

---

**SecureAuth IdP Heuristic-based Parameters**

**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

---

**Settings**

**Normal Browser Settings**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF mode</td>
<td></td>
</tr>
<tr>
<td>Cookie name prefix</td>
<td></td>
</tr>
<tr>
<td>Cookie length</td>
<td></td>
</tr>
<tr>
<td>Mask FF to lower</td>
<td></td>
</tr>
<tr>
<td>Authentication threshold</td>
<td></td>
</tr>
<tr>
<td>Update threshold</td>
<td></td>
</tr>
</tbody>
</table>
20. 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.

21. If **Cookie** is selected in step 20, 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.

22. 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 20, then steps 21 and 22 can be ignored.

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

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

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

---

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

---

**Fingerprint Comparison Score**

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:

- **<FP-Score>** represents the score of the presented fingerprint.

  - 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.
Mobile Settings

25. 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.

26. 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.

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

28. 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 25, then steps 26 - 28 can be ignored.

29. 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.

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

31. 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 24.

General Settings
32. 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

33. 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

34. 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

35. If a maximum is set in step 34, 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

36. If a maximum is set in step 34 and Allow to replace is selected in step 35, then select Created Time from the Replace in order by dropdown 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

37. 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

---

**Workflow**

**Login Screen Options**
38. Select the **Default Workflow**, which is the workflow through which users go to obtain access to the realm's resource:

<table>
<thead>
<tr>
<th>Workflow Type</th>
<th>Description</th>
<th>Required Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username only</strong></td>
<td>User provides username only (no password or second factor required)</td>
<td>This option is usually selected only for specific configurations, such as Windows Desktop SSO</td>
</tr>
<tr>
<td>**Username</td>
<td>Second Factor**</td>
<td>User provides username on one page, and then undergoes 2-Factor Authentication on subsequent page</td>
</tr>
<tr>
<td><strong>(Valid Persistent Token) only</strong></td>
<td>User presents a valid persistent token in lieu of a username only (no password of second factor required)</td>
<td>This option requires a different realm in which the Client Side Control token/certificate/fingerprint is generated to use in this realm</td>
</tr>
<tr>
<td><strong>Username &amp; Password</strong></td>
<td>User provides username and password on one page (no second factor)</td>
<td></td>
</tr>
<tr>
<td>**Username &amp; Password</td>
<td>Second Factor**</td>
<td>User provides username and password on page, and then undergoes 2-Factor Authentication on subsequent page</td>
</tr>
<tr>
<td>**Username</td>
<td>Password**</td>
<td>User provides username on one page, and then provides password on subsequent page (no second factor)</td>
</tr>
<tr>
<td>**Username</td>
<td>Second Factor</td>
<td>Password**</td>
</tr>
<tr>
<td>**(Valid Persistent Token)</td>
<td>Password**</td>
<td>User presents a valid persistent token in lieu of a username on one page, and then provides password on subsequent page (no second factor)</td>
</tr>
<tr>
<td>**(Valid Persistent Token)</td>
<td>Second Factor**</td>
<td>User presents a valid persistent token in lieu of a username on one page, and then undergoes 2-Factor Authentication on subsequent page</td>
</tr>
<tr>
<td>**(Valid Persistent Token)</td>
<td>Second Factor</td>
<td>Password**</td>
</tr>
</tbody>
</table>

39. Select **Private and Public Mode** from the **Public/Private Mode** dropdown to enable both modes during the login process.
If the end-user selects **Private Mode** on the login page, then SecureAuth IdP checks for a certificate / token / fingerprint, or delivers a certificate / token to the browser or pull information to create a fingerprint for subsequent access attempts.

40. Select which option is selected by default (if **Private and Public Mode** is enabled) on the end-user login page from the **Default Public / Private** dropdown.

41. Select **True** from the **Remember User Selection** dropdown if the user’s last **Private / Public Mode** selection is defaulted for subsequent access attempts.

42. Select **False** (default) from the **Skip UserID View** dropdown, which provides a username input field on the login pages.

43. Select **False** (default) from the **Show UserID Textbox** dropdown, which provides a username input field on the login pages for Certificate Enrollment and / or Cisco ASA integrations when the user ID is not provided by Cisco.

44. Select **Enabled** from the **Inline Password Change** dropdown to allow users to change their password during the workflow process.

**Session Timeout**

These configuration steps are only required if session timeout occurs automatically after a set period of time.

45. Set the **Session State Name** or leave it as the default value.

46. Set the number of minutes after which the session is expired in the **Idle Timeout Length** field.

47. Select the action to take after the session has been expired from the **Display Timeout Message** dropdown.

**Token Persistence**

48. Select **True** from the **Validate Persistent Token** dropdown if SecureAuth IdP is to check the validity of the persistent token during the authentication process.

    Select **False** for this realm to only deliver certificates or create a fingerprint, but not validate or renew the token.

49. Select **True** from the **Renew Persistent Token (After Validation)** if the persistent token is to be renewed after SecureAuth IdP checks the validity (applicable only if **True** is selected in step 48).

**Steps 48 - 49 apply to the Client Side Control option selected in step 2, i.e. the Device Fingerprint, Native Cert, Java Cert, or UBC is the persistent token that can be validated and / or renewed through the workflow.**

**Redirects**
50. Set the **Invalid Persistent Token Redirect** field to where users are directed to acquire a new / valid persistent token, e.g. another SecureAuth IdP realm

   This is especially useful in realms using (Valid Persistent Token) workflows as a valid token is required to access the resource

51. Set the **Token Missing Redirect** field to where users are directed to acquire a new token, e.g. enrollment or provisioning realm

   This is used for Near Field Communications (NFC) tokens only

52. Set the **Profile Missing Redirect** field (or leave as default) to where users are directed to retrieve a missing profile, e.g. profilemissing.aspx

53. Set the **If Mobile, Redirect To** field to a SecureAuth IdP realm specifically configured for mobile access

54. Set the **Mobile Identifiers** to common keywords that can be used to detect mobile devices and browsers, which then triggers the mobile redirect to the realm selected in step 53

**Termination Points**

Termination Points are **optional** and may not be relevant for every realm configuration
55. Set the **Client FQDN** to the Fully Qualified Domain Name (FQDN) of the client point of termination for SecureAuth IdP validation.

56. Provide the **SSL Termination Cert** if enabling bi-lateral authentication and if not using SecureAuth IdP as the termination point.

57. If the **SSL Termination Cert** (step 56) cannot be provided, then set the (or) **SSL Cert Address** to the FQDN or IP Address of the (typically) Load Balancer at which the SSL connection is being terminated to enable SecureAuth IdP to retrieve the SSL certificate.

58. Set the **SSL Termination Point** to the FQDN of where the SSL certificate is terminated, which is communicated to SecureAuth IdP to validate the information.

**Java**

The following configuration steps are only required if **Java Applet** is selected in step 2 as the **Client Side Control** option.

59. Select **True** from the **Encrypt Password (Java only)** dropdown to encrypt the end-user’s password (provided during login) being sent to the SecureAuth IdP server for validation (rather than in plain text).

60. Set the **Java Timeout** to the number of X during which Java can respond.

   If no response during the configured time, then an error is presented.

61. Select the action to take if SecureAuth IdP fails to launch the Java Applet from the **Java Applet Load Failure Fallback** dropdown:

   - **True - Public Mode**: The user goes through an out-of-band one-time password.
   - **True - UBC**: The Universal Browser Credential (UBC) is used instead.
   - **True - Cookie**: A cookie is used instead.
   - **False**: The user is denied access and is asked to contact Help Desk.
62. Click **View and Configure Multiple Workflow** only if this realm enables multiple data store integrations that lead to distinct workflows (optional).

Refer to **Multiple Workflow Configuration Guide** for the configuration steps of this feature.
63. Select the type of token SecureAuth IdP receives in the realm from the Receive Token dropdown.

64. Select True from the Require Begin Site dropdown if users are to acquire tokens / other information from a different site before logging in with SecureAuth IdP; or select False (default) if no begin site is required.

65. Select the type of Begin Site from the dropdown that is used in this realm, which auto-populates the Begin Site URL field (unless Custom is selected). Refer to the specific Begin Site Configuration Guide for full configuration steps.

66. Select where the User ID is stored in the received token from the Token Data Type (Receive) dropdown.

67. Select where the User ID is stored in the token sent to the SP from the Token Data Type (Send) dropdown.

68. Select False from the Allow Transparent SSO dropdown. Select True if this realm utilizes SecureAuth IdP SSO, and enables SP-initiated or Secure SSO Portal SSO. Also refer to the specific Integration Guide to view the distinct configuration steps.

69. Provide the Open ID Provider URL in the Static OP Server URL field.

70. Select the type of identifying claim that will be used in Open ID from the Federated OpenID dropdown.
SAML Consumer

SAML Consumer configurations are only necessary if SecureAuth IdP is accepting a SAML assertion from one or multiple Identity Providers

Refer to SAML Multi-tenant Consumer Configuration Guide and SAML Attribute Consumption Configuration Guide for more information on these features

Form Post

Form Post configurations are only necessary if SecureAuth IdP is accepting a Form Post

71. Select what user information is being sent for SecureAuth IdP validation in the Form Post from the Validation Mode dropdown

Social Identity

Social Identity configurations are only necessary if Social IDs are being consumed by SecureAuth IdP for use in multi-factor authentication

Facebook

72. Select True from the Enable dropdown to enable the use of Facebook ID for 2-Factor Authentication
73. Provide the Client ID, which is provided by Facebook
74. Provide the Client Secret, which is provided by Facebook

The Client ID and the Client Secret must match exactly here and on Facebook's side

75. Select where to Store Facebook ID at from the dropdown (e.g. Aux ID 1)

Google
76. Select True from the Enable dropdown to enable the use of Google ID for 2-Factor Authentication
77. Provide the Client ID, which is provided by Google
78. Provide the Client Secret, which is provided by Google

The Client ID and the Client Secret must match exactly here and on Google's side

79. Select where to Store Google ID at from the dropdown (e.g. Aux ID 2)

Windows Live

80. Select True from the Enable dropdown to enable the use of Windows Live ID for 2-Factor Authentication
81. Provide the Client ID, which is provided by Windows Live
82. Provide the Client Secret, which is provided by Windows Live

The Client ID and the Client Secret must match exactly here and on Windows Live's side

83. Select where to Store Windows Live ID at from the dropdown (e.g. Aux ID 3)

LinkedIn

84. Select True from the Enable dropdown to enable the use of LinkedIn ID for 2-Factor Authentication
85. Provide the Client ID, which is provided by LinkedIn
86. Provide the Client Secret, which is provided by LinkedIn

The Client ID and the Client Secret must match exactly here and on LinkedIn's side

87. Select where to Store LinkedIn ID at from the dropdown (e.g. Aux ID 4)
88. Select **True** from the **Enable FBA WebService** dropdown.

89. Provide the **FBA WebService UserName**, which is the same as the **Webservice Username** in the **Data** tab.

90. Provide the **FBA WebService Password** that corresponds to the username.

---

### iPhone / iPad Handling (Deprecated)

iPhone / iPad Handling configurations are only necessary if users utilizing an iPhone or iPad require redirection.

This functionality has been deprecated. Previous deployments of the feature continue to be supported, but no new configurations are accepted.

91. Select the SecureAuth IdP realm to which iPhone / iPad users will be redirected from the **Validation Realm** dropdown.

---

### Consume Passcode from RADIUS 1.x Integrations

These configurations are only necessary if using **SecureAuth RADIUS 1.0.x** to make RADIUS web service calls to validate user information.

92. Select what information is to be validated by SecureAuth IdP via the RADIUS web service call from the **OTP Format** dropdown.