Workflow configuration

The Workflow tab is configured on a SecureAuth IdP realm to provide the way in which end-users will access a realm. A workflow might include use of any of the following options:

- Device Recognition – this option includes token and certificate properties.
- Workflow – this option includes authentication modes and URL redirection to other realms or pages.
- Identity / Authentication Consumers – this option includes custom tokens and social identities.

What's new in SecureAuth IdP version 9.3

Two new fields – Use Kernel Mode and Use AppPool Credentials – added in the Custom Identity Consumer section can now enable kernel mode authentication and application pool credentials (Active Directory service account) in environments using custom Service Principal Names for Integrated Windows Authentication (Kerberos). In prior versions of SecureAuth IdP, these entries were made in the web.config editor.

Workflow guides from the previous release

See the collection of Workflow configuration guides under this category:

Prerequisites

- SecureAuth IdP v9.3.
- SecureAuth IdP realm or integrated application with the following configured:
    - Overview tab
    - Data tab / Directory integration

> ⓘ On the New Experience user interface in version 9.3, you can configure an Active Directory integration or SQL Server integration to be applied to applications made from App onboarding library templates. Configure the remaining components – for example, Workflow, Multi-Factor Methods, and Adaptive Authentication tabs – on the Classic Experience user interface.

SecureAuth IdP Web Admin - Classic Experience

Device Recognition

Device Recognition Method section

1. Select the **Integration Method** from the dropdown.

    The selection made here alters 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 alters the options for **IE / PFX / Java Cert Type**, and may require additional configuration steps.

Certification enrollment and validation client side control options

- **Java Applet** stores the SecureAuth IdP X.509 certificate in the JRE managed code file set.
- **Browser Plug-ins** stores the certificate in the native key store.
- **Device / Browser Fingerprinting** enables SecureAuth Device Recognition mode. This mode *pulls* unique characteristics from the device or browser and stores these as a profile 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** is set to **Browser Plug-ins / Keygen** (no other option).

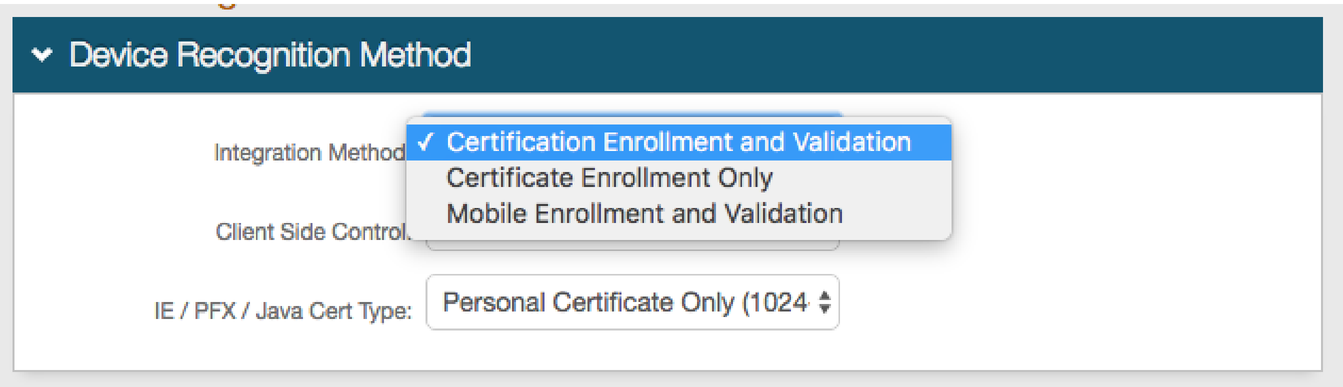
Mobile enrollment and validation client side control options

- **Browser Credential** stores a cookie in the browser.
- **Device / Browser Fingerprinting** enables SecureAuth Device Recognition mode. This mode *pulls* unique characteristics from the device or browser and stores these as a profile 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 selection is based on the security preference.

NOTE: This step is not required if Device / Browser Fingerprinting is selected in step 2.



Device Recognition Method

Integration Method: ✓ Certification Enrollment and Validation

Certificate Enrollment Only

Mobile Enrollment and Validation

Client Side Control:

IE / PFX / Java Cert Type: Personal Certificate Only (1024

Certificate / Token Properties section

4. Select **Password Expiration Date** from the Certificate Expiration dropdown for the certificate to expire on the same day the password expires.

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

5. Select **Cert Expiration Date** from the Certificate Valid Until dropdown for the certificate to remain valid up until the expiration date.

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

6. If Private Mode Cert Length was selected in step 4 or 5, make an entry in the **Private Mode Cert Length** field to set the number of days a certificate will remain valid and will not expire.

7. If **Certificate Enrollment** was selected from the Integration Mode dropdown in the Device Recognition Method section, make an entry in the **Public Mode Cert Length** field to set the number of hours during which the Public Mode Certificate is valid.

8. Make an entry in the **Mobile Credential Length** field (browser credential) to set the number of hours a cookie delivered to a mobile device remains valid.

9. OPTIONAL: Make an entry in the **Global Cert Limit** field to set the maximum number of certificates a user can have at a time.

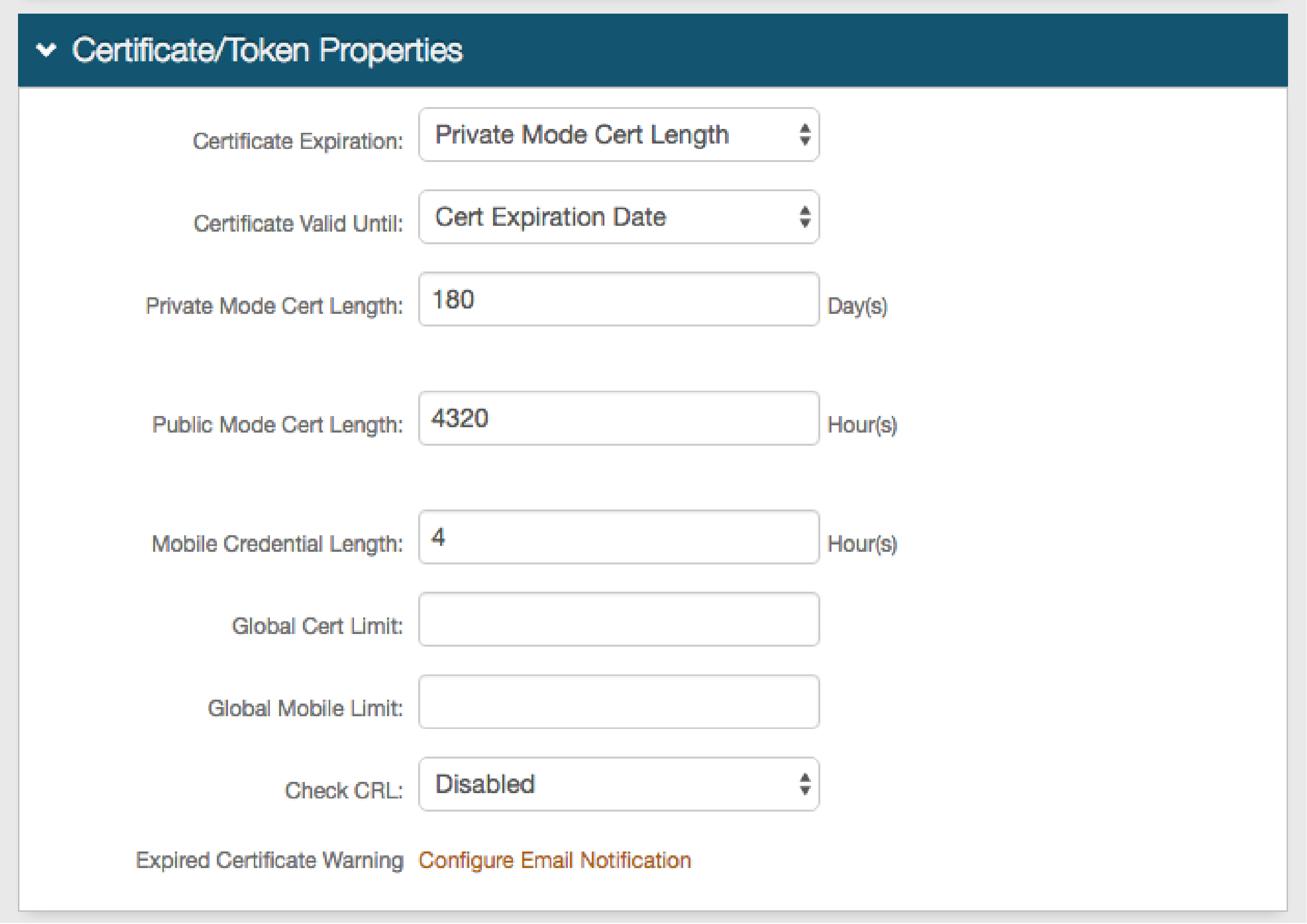
10. OPTIONAL: Make an entry in the **Global Mobile Limit** field to set the maximum number of mobile cookies a user can have at a time.

11. OPTIONAL: To have SecureAuth IdP check the Certificate Revocation List, select **Fall Back to 2nd Factor** or **Display Error Message** from the Check CRL dropdown.

Select **Disabled** to opt out of checking the CRL.

12. OPTIONAL: Click **Configure Email Notification** to enable and set up Expired Certificate Warning emails.

13. **Save** the configuration.



Certificate/Token Properties

Certificate Expiration: Private Mode Cert Length

Certificate Valid Until: Cert Expiration Date

Private Mode Cert Length: 180 Day(s)

Public Mode Cert Length: 4320 Hour(s)

Mobile Credential Length: 4 Hour(s)

Global Cert Limit:

Global Mobile Limit:

Check CRL: Disabled

Expired Certificate Warning Configure Email Notification

Expired Certificate Warning

Configure Email Notification

1. Select **Enabled** from the Email Notification dropdown to enable the warning notifications.

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

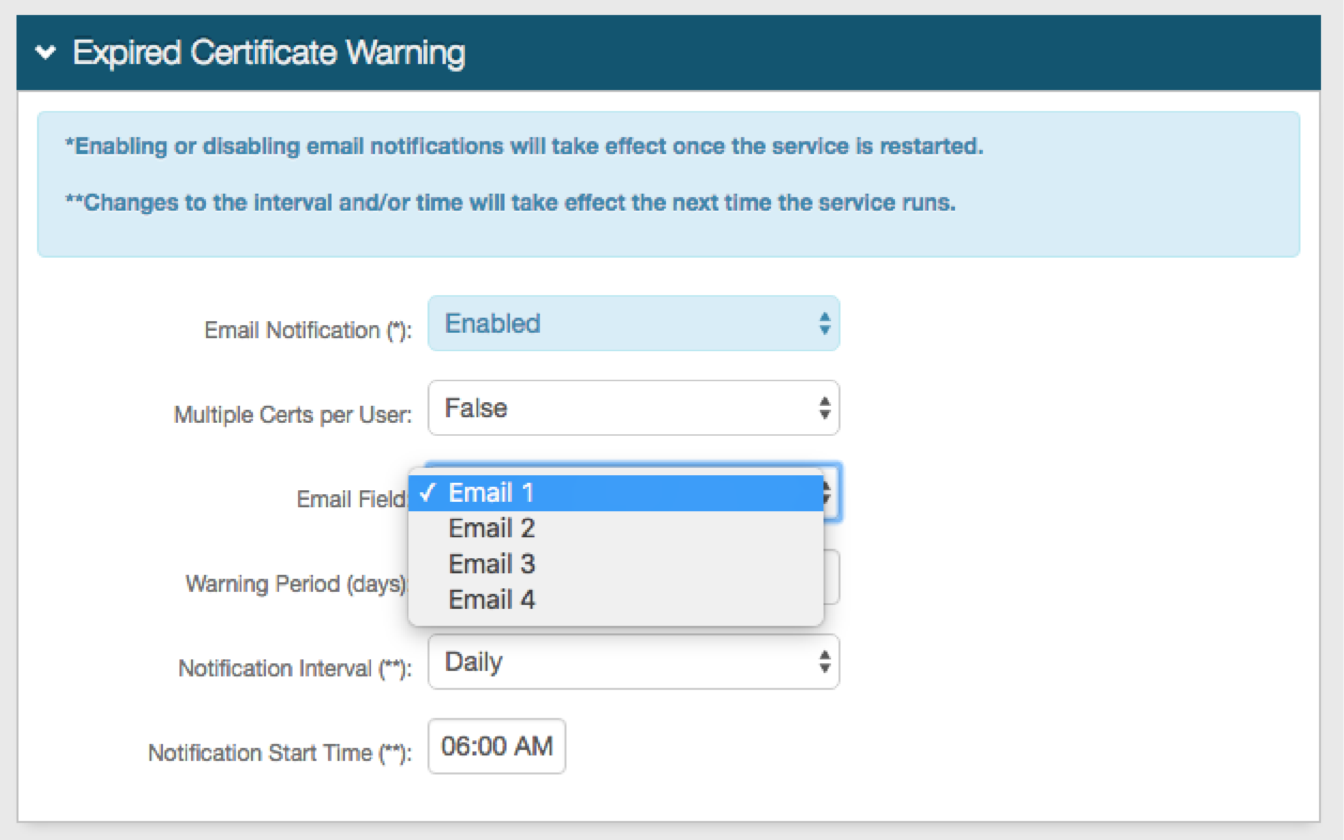
3. Make a selection from the Email Field dropdown to select the **Email Property** corresponding to the data store field containing the user's email address for receiving notifications.

4. Make an entry in the **Warning Period** field to set the number of days before the expiration date on which notifications will be sent.

5. Select **Daily** from the **Notification Interval** dropdown to send an email notification once per day.

6. Set the **Notification Start Time** for sending email notifications.

7. **Save** the configuration.



Expired Certificate Warning

*Enabling or disabling email notifications will take effect once the service is restarted.

**Changes to the interval and/or time will take effect the next time the service runs.

Email Notification (*): Enabled

Multiple Certs per User: False

Email Field

Warning Period (days)

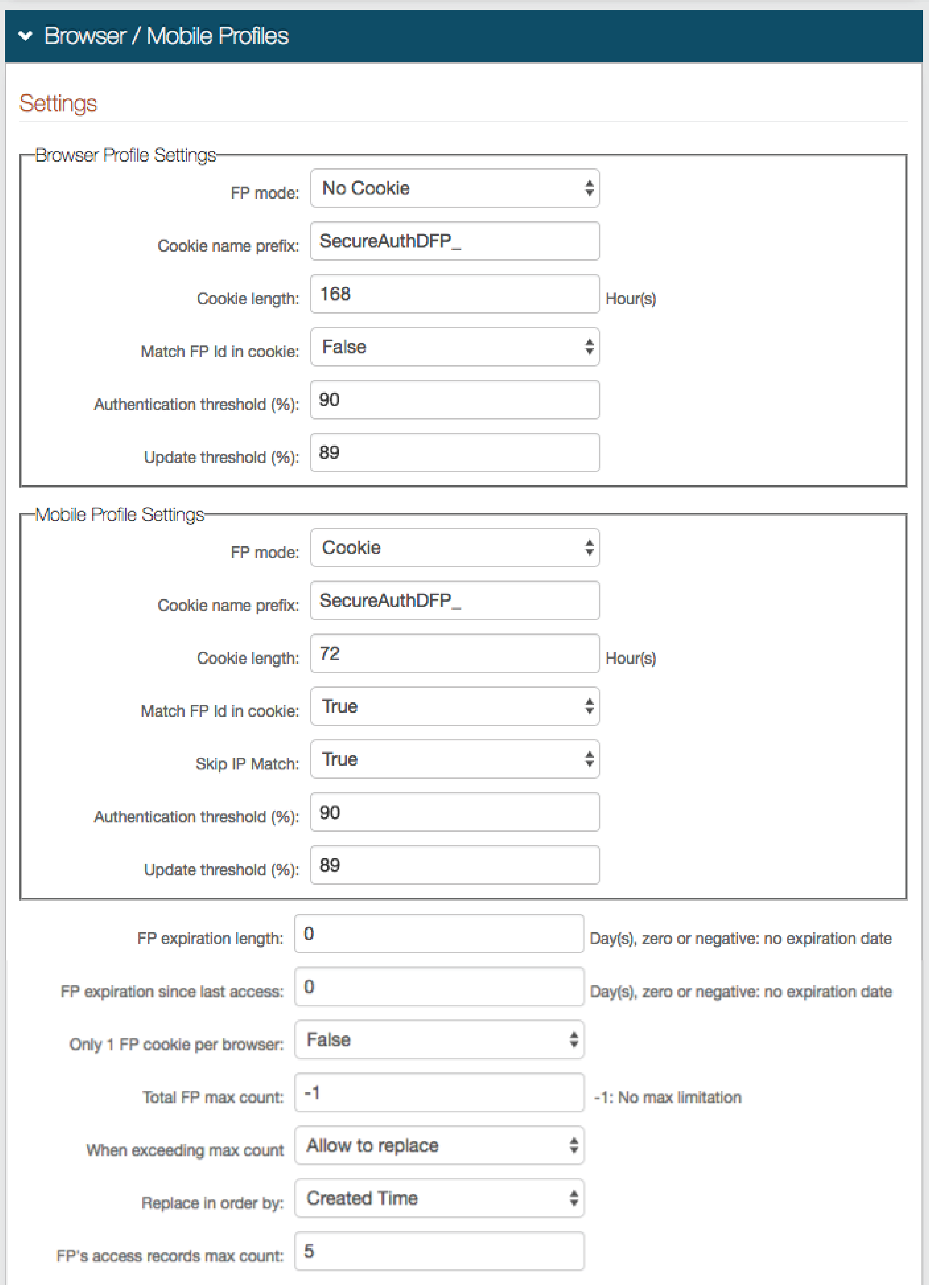
Notification Interval (**): Daily

Notification Start Time (**): 06:00 AM

Browser / Mobile Profiles section

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

14. Configure Device Recognition settings for the realm.



Browser / Mobile Profiles

Settings

Browser Profile Settings

FP mode: No Cookie

Cookie name prefix: SecureAuthDFP_

Cookie length: 168 Hour(s)

Match FP Id in cookie: False

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

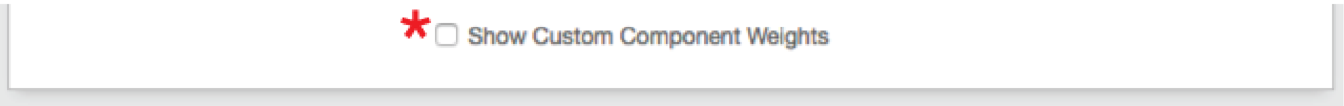
Only 1 FP cookie per browser: False

Total FP max count: -1 -1: No max limitation

When exceeding max count Allow to replace

Replace in order by: Created Time

FP's access records max count: 5


* □ Show Custom Component Weights

Workflow

Workflow section

Login Screen Options

15. Select the **Default Workflow**, which is the workflow for users to access the realm's resource.

User provides username only (no password or second factor required).

This option is usually selected only for specific configurations, such as Windows Desktop SSO.

User provides username on one page, and then undergoes two-factor authentication on a subsequent page.

This options requires configuration and enablement of at least one registration method on the **Multi-Factor Methods** tab.

User presents a valid persistent token in lieu of a username only (no password of second factor required).

This option requires a different realm in which the **Client Side Control** token/certificate/fingerprint is generated for use on this realm.

User provides username and password on one page (no second factor).

User provides username and password on the page, and then undergoes two-factor authentication on a subsequent page.

This options requires configuration and enablement of at least one registration method on the **Multi-Factor Methods** tab.

User provides username on one page, and then provides password on a subsequent page (no second factor).

User provides username on one page, undergoes two-factor authentication on next page, and then provides password on a subsequent page (standard workflow, recommended by SecureAuth).

This options requires configuration and enablement of at least one registration method on the **Multi-Factor Methods** tab.

User presents a valid persistent token in lieu of a username on one page, and then provides password on a subsequent page (no second factor).

This option requires a different realm in which the **Client Side Control** token/certificate/fingerprint is generated for use on this realm.

User presents a valid persistent token in lieu of a username on one page, and then undergoes two-factor authentication on a subsequent page.

This option requires a different realm in which the **Client Side Control** token/certificate/fingerprint is generated for use on this realm, and configuration and enablement of at least one registration method is made on the **Multi-Factor Methods** tab.

User presents a valid persistent token in lieu of a username on one page, undergoes two-factor authentication on next page, and then provides password on a subsequent page.

This option requires a different realm in which the **Client Side Control** token/certificate/fingerprint is generated for use on this realm, and configuration and enablement of at least one registration method is made on the **Multi-Factor Methods** tab.

16. 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 / device profile, or delivers a certificate / token to the browser or pull information to create a device / browser profile for subsequent access attempts.

17. If **Private and Public Mode** is enabled, make a selection from the **Default Public / Private** dropdown for the option that appears by default on the end-user login page.

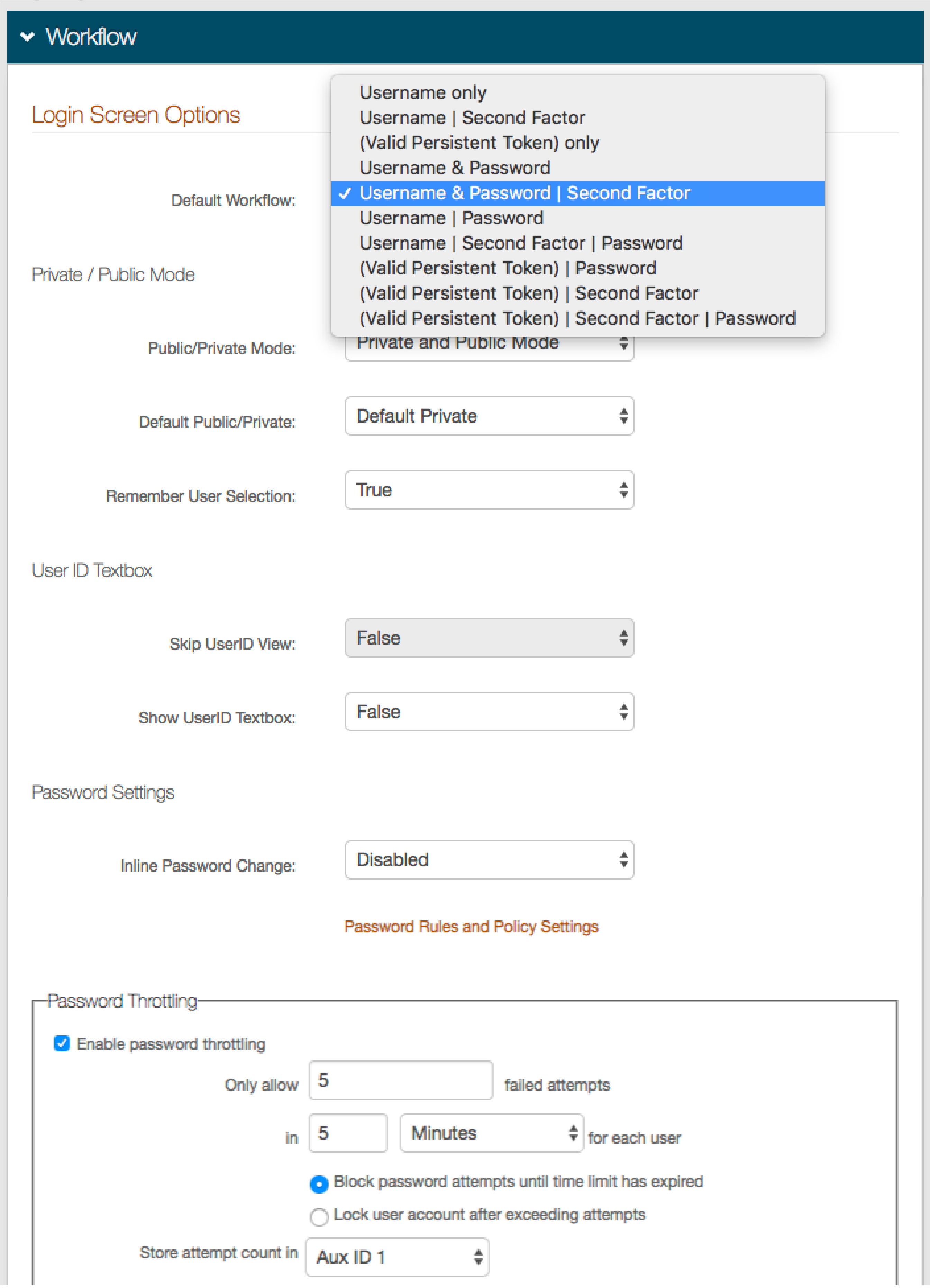
18. Select **True** from the **Remember User Selection** dropdown if the user's last **Private / Public Mode** selection is defaulted for subsequent access attempts.

19. Select **False** (default) from the **Skip UserID View** dropdown if the username input field should not appear on login pages.

20. Select **False** (default) from the **Show UserID Textbox** dropdown if the username input field should not appear on the login pages for Certificate Enrollment and / or Cisco ASA integrations when the user ID is not provided by Cisco.

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

22. OPTIONAL: Configure the realm for Password Throttling.



Workflow
Username only
Username | Second Factor
(Valid Persistent Token) only
Username & Password
✓ Username & Password | Second Factor
Username | Password
Username | Second Factor | Password
(Valid Persistent Token) | Password
(Valid Persistent Token) | Second Factor
(Valid Persistent Token) | Second Factor | Password

Login Screen Options

Default Workflow: Username & Password | Second Factor

Private / Public Mode

Public/Private Mode: Private and Public Mode

Default Public/Private: Default Private

Remember User Selection: True

User ID Textbox

Skip UserID View: False

Show UserID Textbox: False

Password Settings

Inline Password Change: Disabled

Password Rules and Policy Settings

Password Throttling

☑ Enable password throttling

Only allow 5 failed attempts

in 5 Minutes for each user

● Block password attempts until time limit has expired

○ Lock user account after exceeding attempts

Store attempt count in Aux ID 1

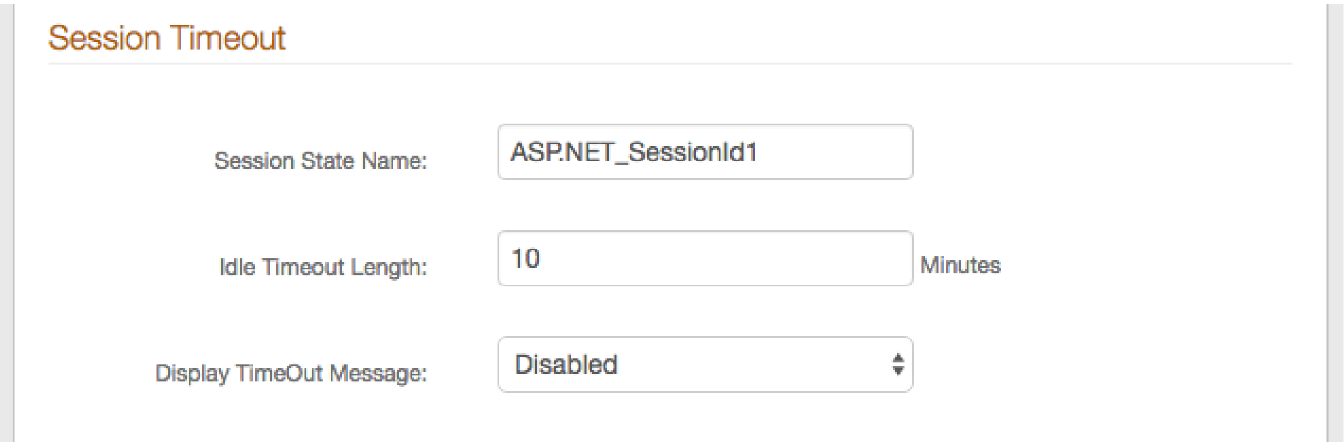
Session Timeout

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

23. Set the **Session State Name** or leave the default value.

24. Set the number of minutes in the **Idle Timeout Length** field to the length of time until the session expires.

25. Make a selection from the **Display Timeout Message** dropdown to specify the action after the session expires.



Session Timeout

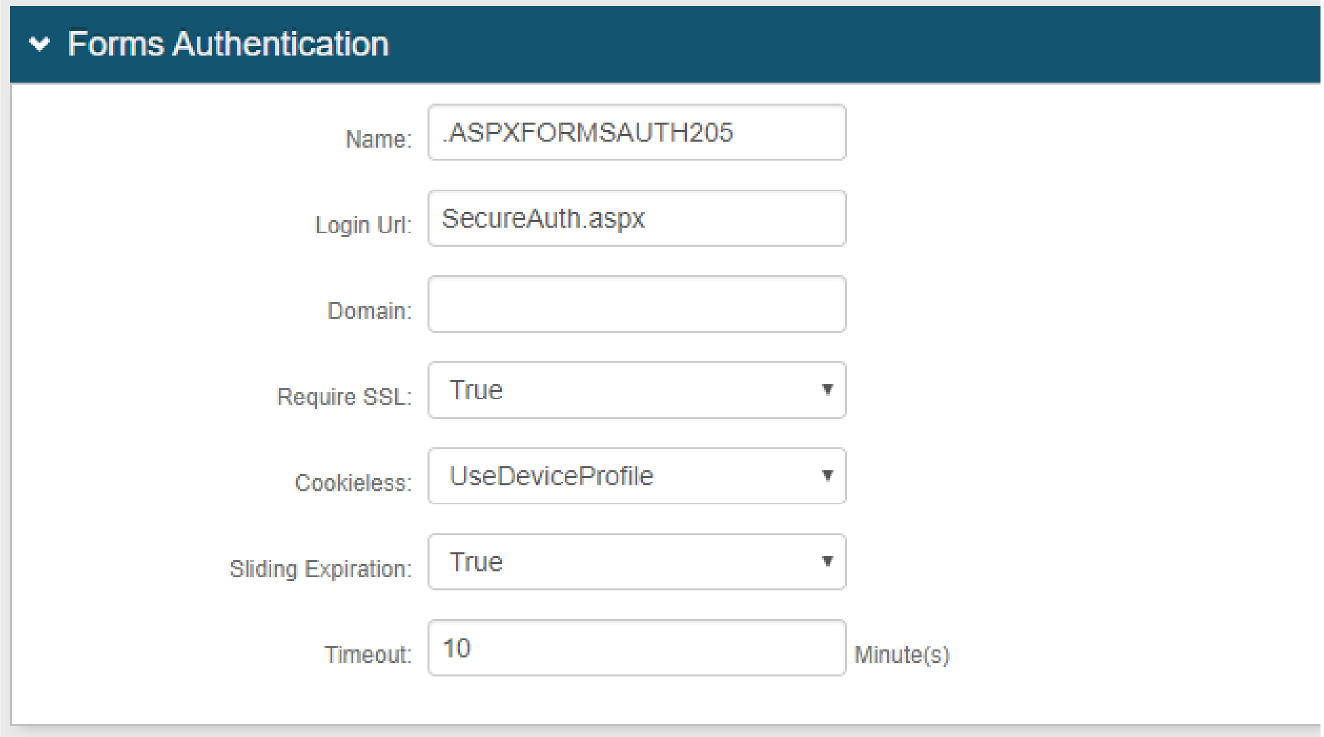
Session State Name: ASP.NET_SessionId1

Idle Timeout Length: 10 Minutes

Display TimeOut Message: Disabled

IMPORTANT: To prevent time synchronization errors in the SecureAuth0 realm, set the **Idle Timeout Length** to the same value as the **Timeout** Minute (s) configured on the Forms Authentication section of the Post Authentication tab.

> Access the Forms Authentication section from the **View and Configure FormsAuth keys / SSO token** link in the Forms Auth / SSO Token section on the Post Authentication tab.



Forms Authentication

Name: .ASPXFORMSAUTH205

Login Url: SecureAuth.aspx

Domain:

Require SSL: True

Cookieless: UseDeviceProfile

Sliding Expiration: True

Timeout: 10 Minute(s)

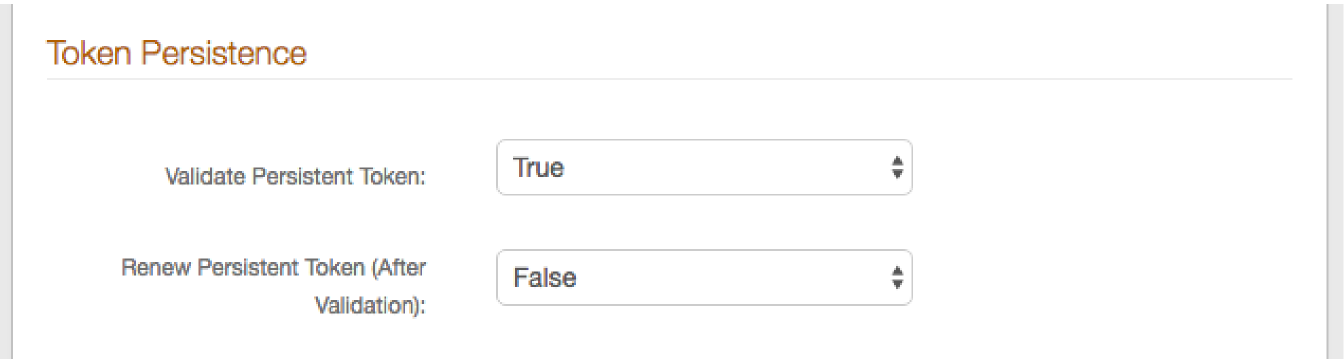
Token Persistence

Steps 26 - 27 apply to the **Client Side Control** option selected in step 2 – that is the Device / Browser Profile, Native Cert, Java Cert, or UBC is the persistent token that can be validated and / or renewed through the workflow.

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

Select **False** if this realm will *only* deliver certificates or create a profile, but not validate or renew the token.

27. Select **True** from the **Renew Persistent Token (After Validation)** if the persistent token should be renewed after SecureAuth IdP checks the validity (applicable only if **True** is selected in step 26).



Token Persistence

Validate Persistent Token: True

Renew Persistent Token (After Validation): False

Redirects

Redirects are **optional** and may not be relevant for every realm configuration.

28. Set the **Invalid Persistent Token Redirect** field so that users are directed to acquire a new / valid persistent token – example: 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.

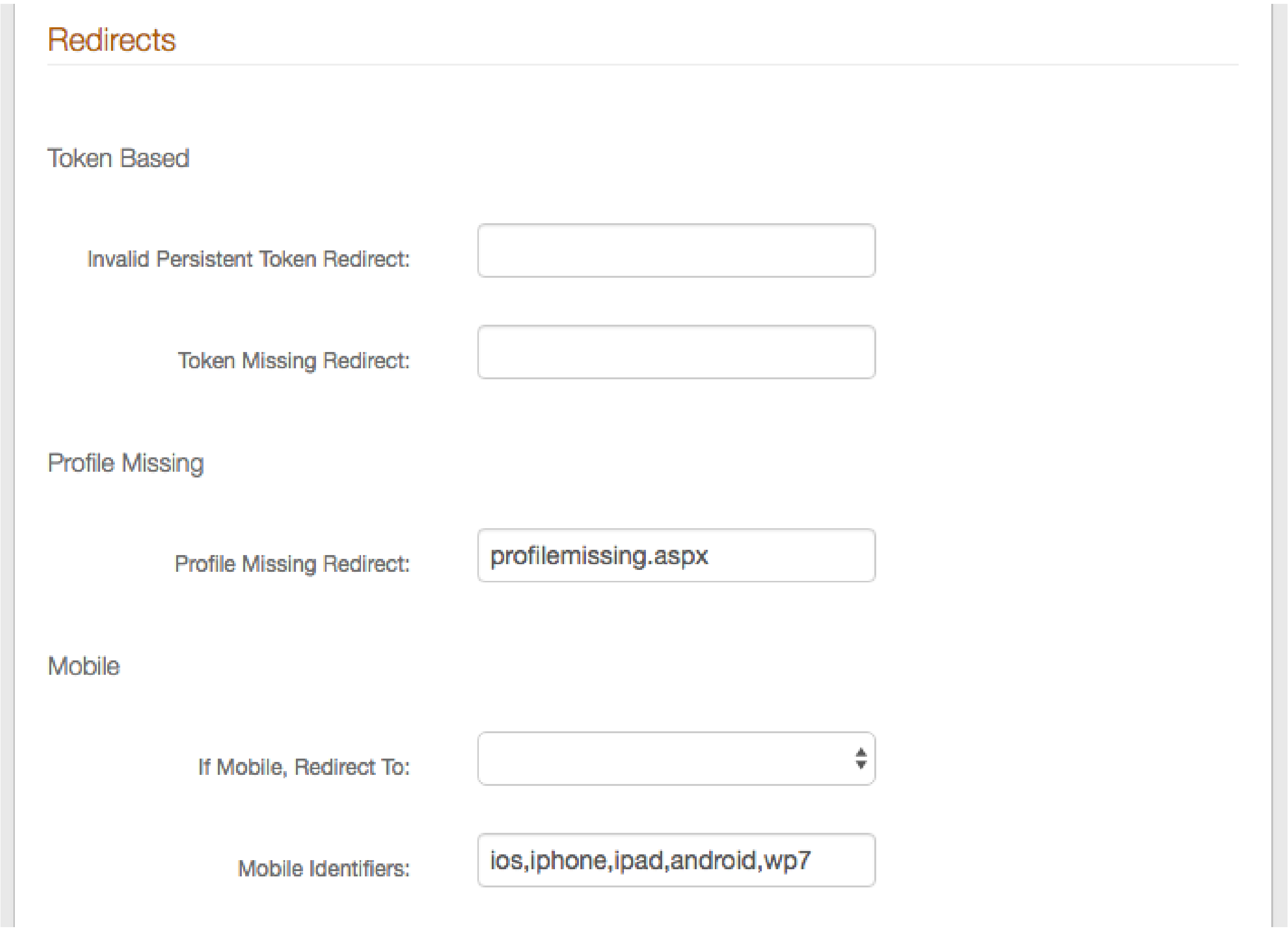
29. Set the **Token Missing Redirect** field so that users are directed to acquire a new token – example: enrollment or provisioning realm.

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

30. Set the **Profile Missing Redirect** field (or leave as default) so that users are directed to retrieve a missing profile – example: profilemissing.aspx

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

32. Set the **Mobile Identifiers** to common keywords that can be used to detect mobile devices and browsers, which trigger the mobile redirect to the realm specified in step 31.



Redirects

Token Based

Invalid Persistent Token Redirect:

Token Missing Redirect:

Profile Missing

Profile Missing Redirect: profilemissing.aspx

Mobile

If Mobile, Redirect To:

Mobile Identifiers: ios,iphone,ipad,android,wp7

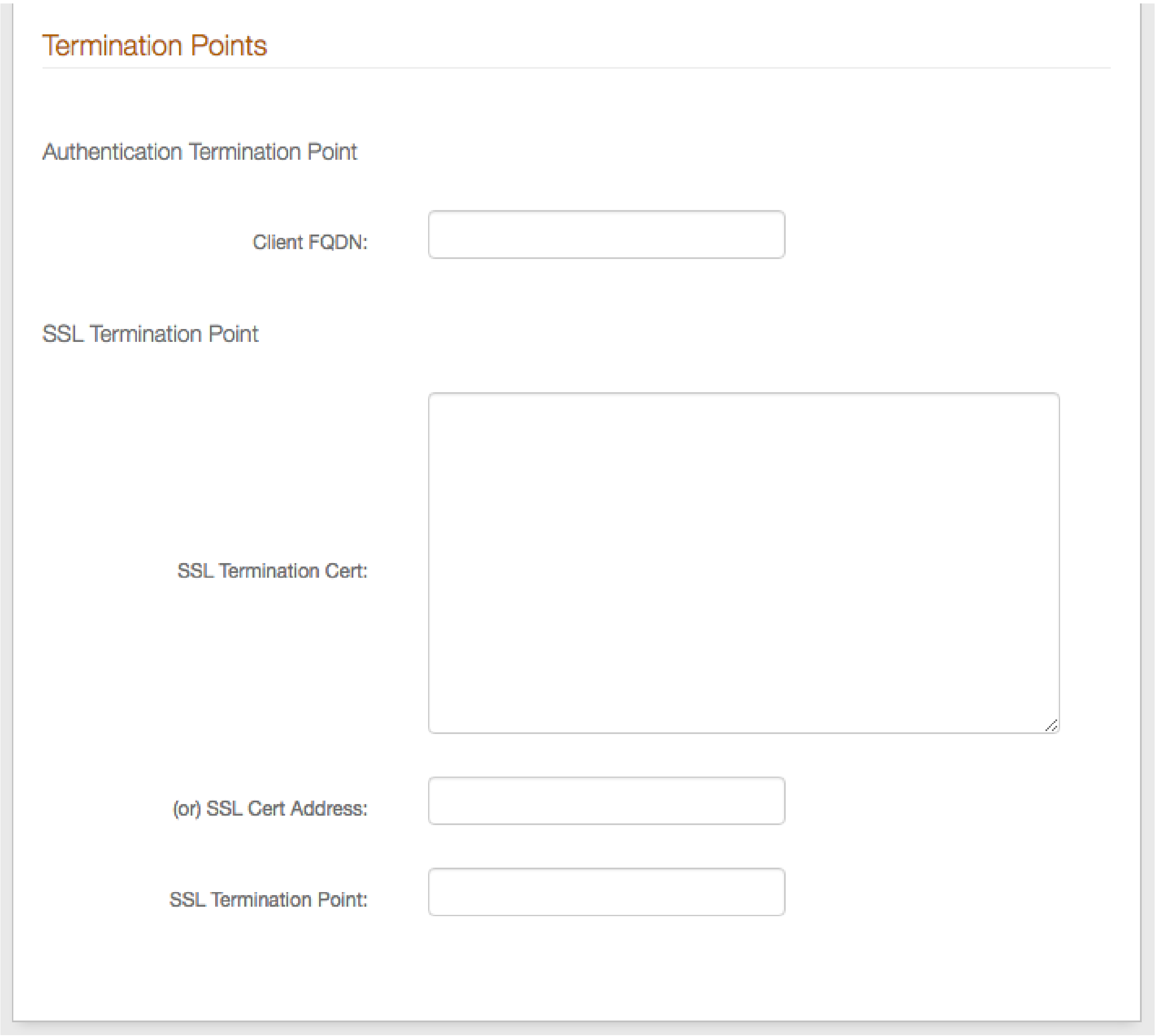
Termination Points

33. Set the **Client FQDN** to the Fully Qualified Domain Name (FQDN) of the client termination point used by SecureAuth IdP to validate the information.

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

35. If the **SSL Termination Cert** (step 34) can't be provided, then set the **(or) SSL Cert Address** to the FQDN or IP Address of the (typically) Load Balancer to which the SSL connection is being terminated, enabling SecureAuth IdP to retrieve the SSL certificate.

36. Set the **SSL Termination Point** to the FQDN of the site where the SSL certificate is terminated – this is communicated to SecureAuth IdP to validate the information.



Termination Points

Authentication Termination Point

Client FQDN:

SSL Termination Point

SSL Termination Cert:

(or) SSL Cert Address:

SSL Termination Point:

Java

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

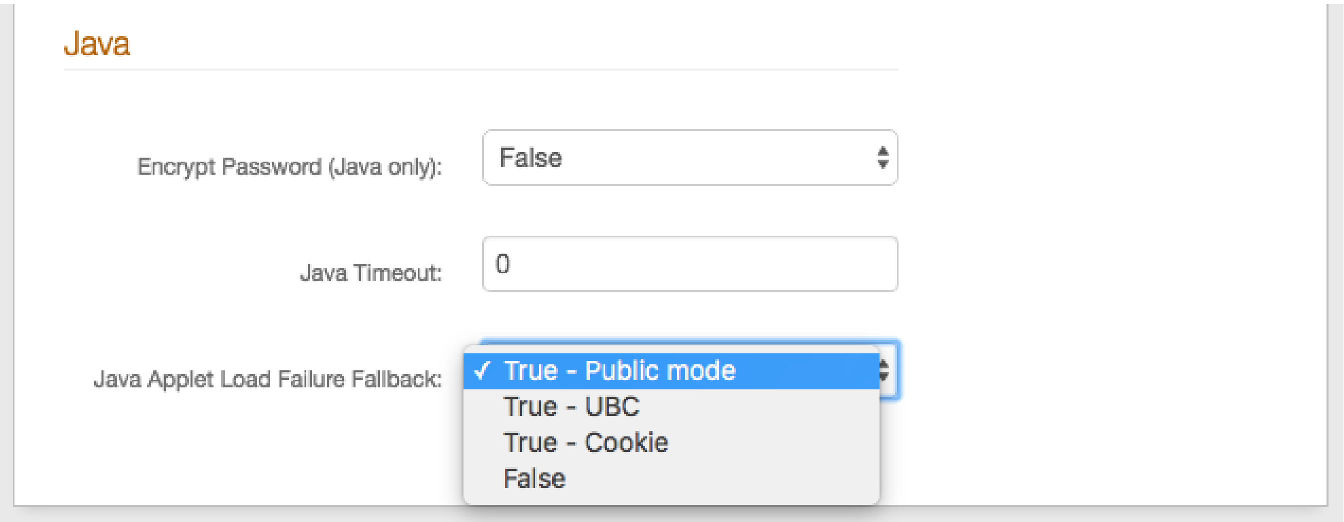
37. Select **True** from the Encrypt Password (Java only) dropdown to encrypt (rather than send in plain text) the end-user's password during login to the SecureAuth IdP server for validation.

38. Set the **Java Timeout** to the set amount of time in which Java can respond.

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

39. Make a selection from the **Java Applet Load Failure Fallback** dropdown to specify what happens if SecureAuth IdP fails to launch the Java Applet:

- **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 the Help Desk.



Java

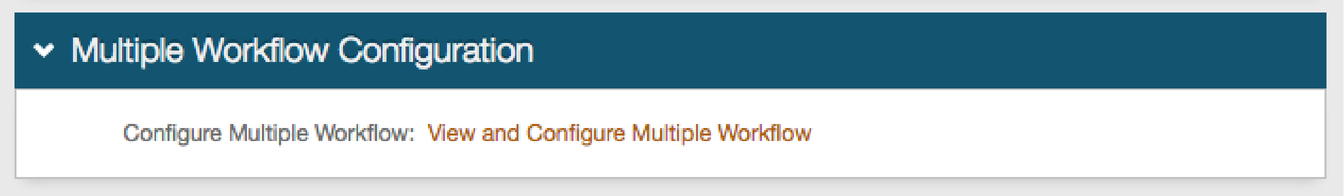
Encrypt Password (Java only): False

Java Timeout: 0

Java Applet Load Failure Fallback:

Multiple Workflow Configuration section

Click **View and Configure Multiple Workflow** *only if* this realm enables multiple data store integrations that lead to distinct workflows.



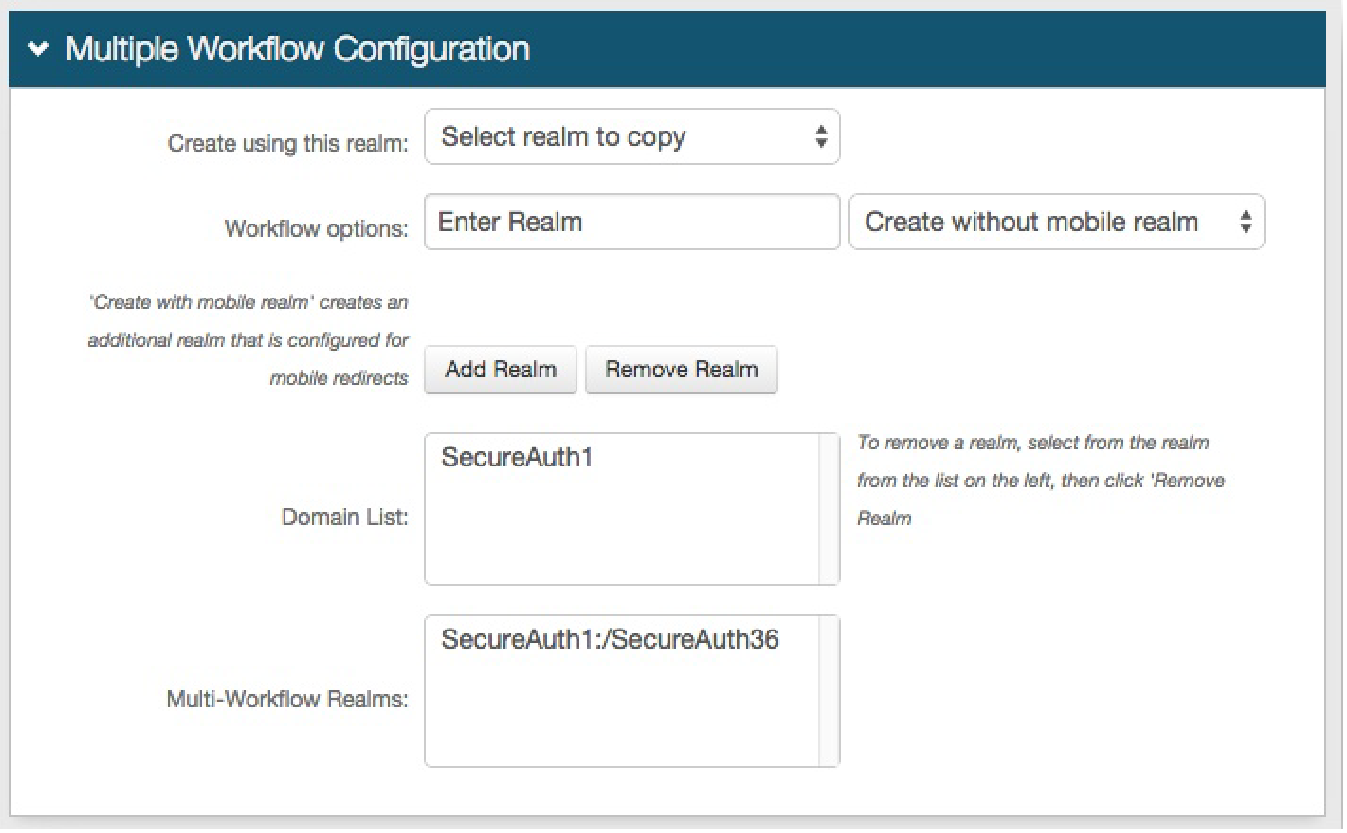
Configure Multiple Workflow: View and Configure Multiple Workflow

OPTIONAL: Multiple workflow configuration settings

Multiple Workflow Configuration sub-section

1. Refer to Multiple Workflow Configuration Guide for this feature's configuration steps.

2. **Save** the configuration.



Multiple Workflow Configuration

Create using this realm: Select realm to copy

Workflow options: Enter Realm | Create without mobile realm

'Create with mobile realm' creates an additional realm that is configured for mobile redirects

Domain List: SecureAuth1

To remove a realm, select from the realm from the list on the left, then click 'Remove Realm

Multi-Workflow Realms: SecureAuth1:/SecureAuth36

Identity / Authentication Consumers

Custom Identity Consumer section

> The Custom Identity Consumer configuration is **optional** and may not be relevant for every realm configuration.

40. Make a selection from the **Receive Token** dropdown to specify the type of token SecureAuth IdP can receive on the realm being configured.

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

42. Make a selection for the type of **Begin Site** used on this realm – this information auto-populates the Begin Site URL field (unless **Custom** is selected).

    Refer to the specific Begin Site Configuration Guide for full configuration steps.

    See Windows desktop SSO configuration for the latest configuration guide for this begin site.

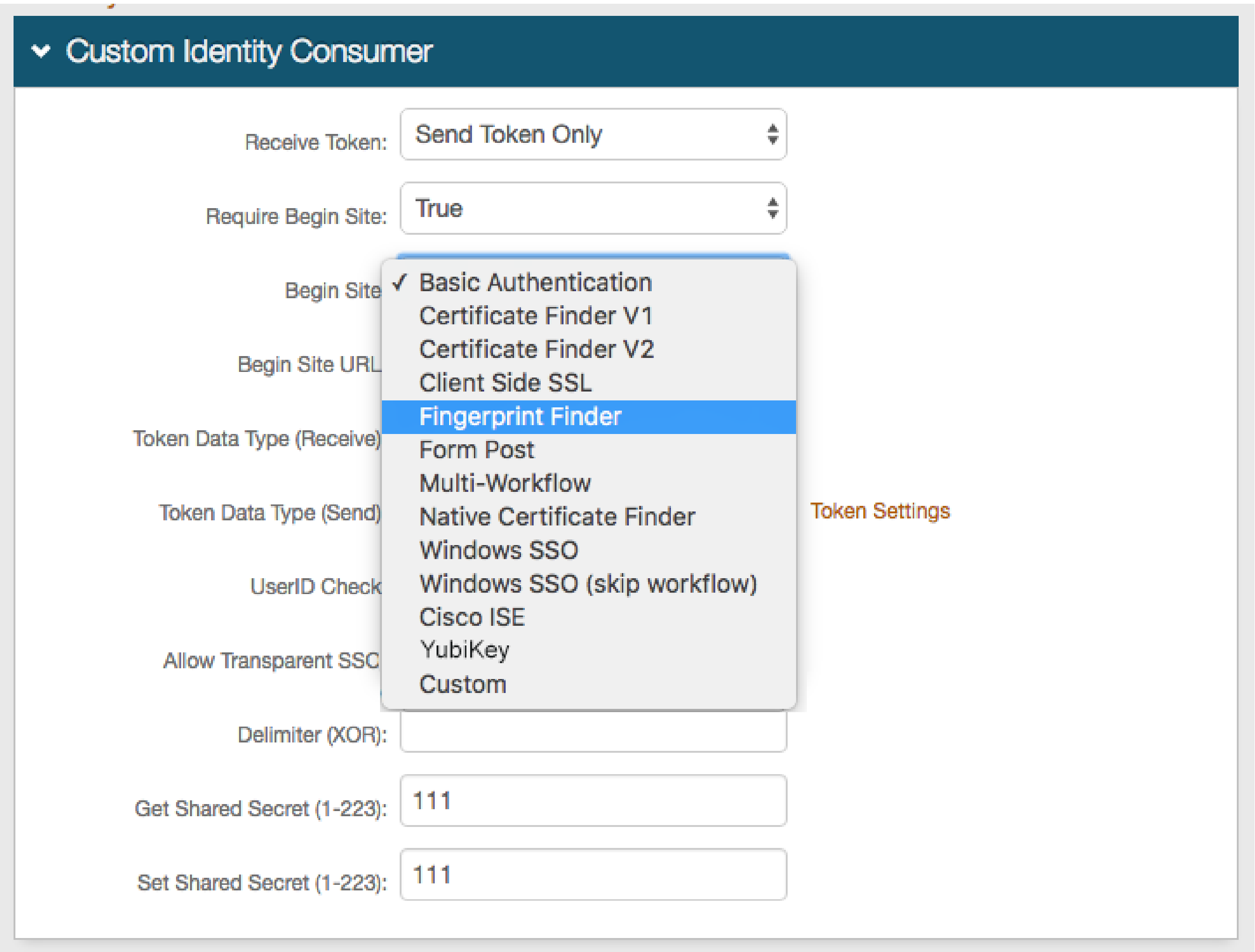
43. Make a selection from the **Token Data Type (Receive)** dropdown to specify where the User ID is stored in the token SecureAuth IdP receives.

44. Make a selection from the **Token Data Type (Send)** dropdown to specify where the User ID is stored in the token sent to the SP.

45. Select **False** from the Allow Transparent SSO dropdown.

    Select **True** if this realm uses SecureAuth IdP SSO, and enables SP-initiated or Secure Portal SSO.

> **NOTE**: Also refer to the specific Integration Guide to view the distinct configuration steps.
>
> Save the configuration on the Workflow tab after completing all necessary steps for the workflow.



Receive Token: Send Token Only

Require Begin Site: True

Begin Site

Begin Site URL

Token Data Type (Receive)

Token Data Type (Send)

UserID Check

Allow Transparent SSO

Delimiter (XOR):

Get Shared Secret (1-223): 111

Set Shared Secret (1-223): 111

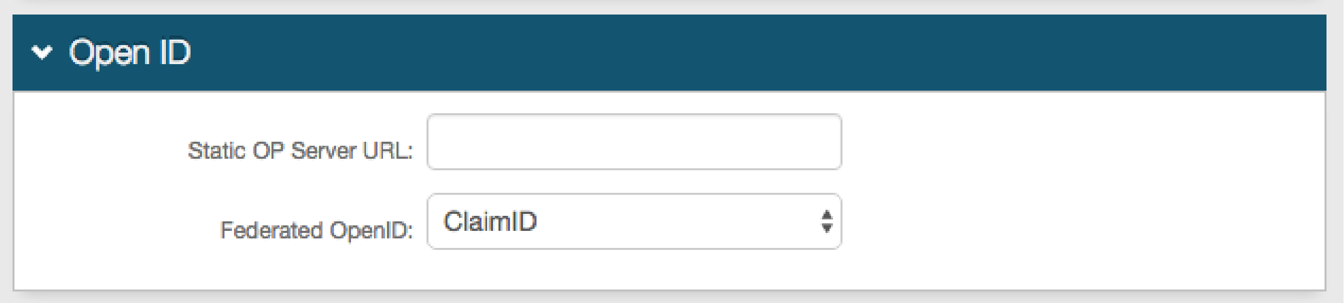
Open ID section

An Open ID configuration is only necessary if using Open ID on the realm.

Open ID configuration

1. Set the Open ID Provider URL in the **Static OP Server URL** field.

2. Make a selection from the **Federated OpenID** dropdown for the type of identifying claim to be used in Open ID.



Static OP Server URL:

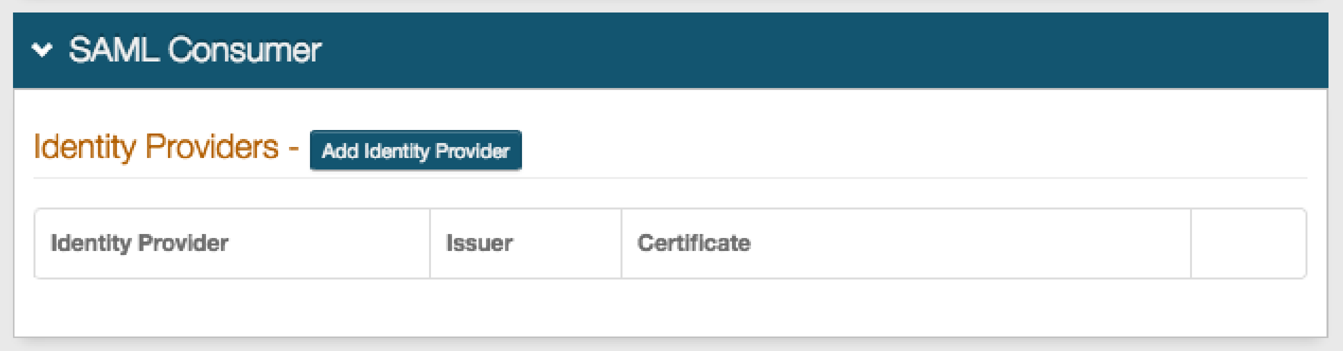
Federated OpenID: ClaimID

SAML Consumer section

A SAML Consumer configuration is only necessary if SecureAuth IdP is accepting a SAML assertion from one or multiple Identity Providers.

SAML Consumer configuration

Refer to SAML Multi-tenant Consumer Configuration Guide and SAML attribute consumption configuration for more information about these features.



SAML Consumer

Identity Providers -

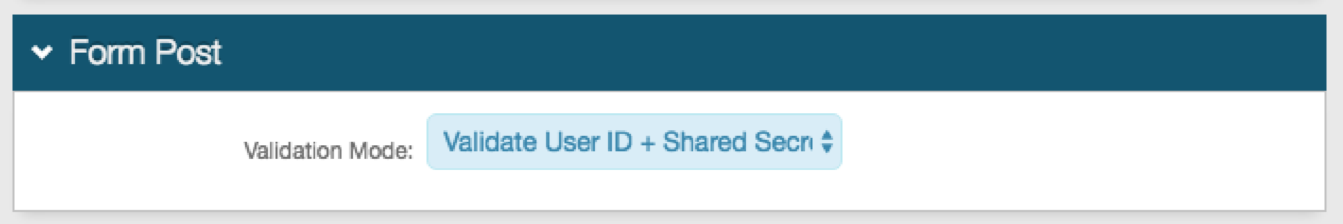
Identity Provider	Issuer	Certificate	

Form Post section

A Form Post configuration is only necessary if SecureAuth IdP is accepting a Form Post.

Form Post configuration

1. Make a selection from the **Validation Mode** dropdown to specify the type of user information to be sent to SecureAuth IdP for Form Post validation.



Form Post

Validation Mode: Validate User ID + Shared Secr

Social Identity section

A Social Identity configuration is only necessary if Social IDs are being consumed by SecureAuth IdP for use in two-factor authentication.

Social Identity configuration

Facebook

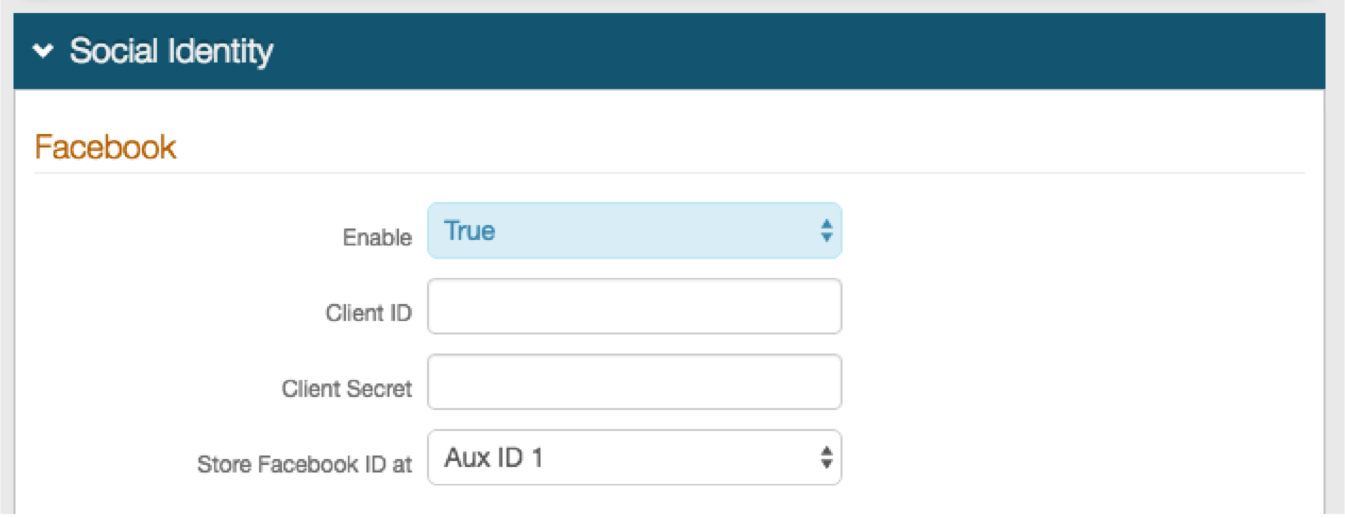
1. Select **True** from the Enable dropdown to enable the use of Facebook ID for two-factor authentication.

2. Set the **Client ID** which is provided by Facebook.

3. Set the **Client Secret** which is provided by Facebook.

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

4. Specify where to **Store Facebook ID at** from the dropdown (example: **Aux ID 1**)



Social Identity

Facebook

Enable: True

Client ID:

Client Secret:

Store Facebook ID at: Aux ID 1

Google

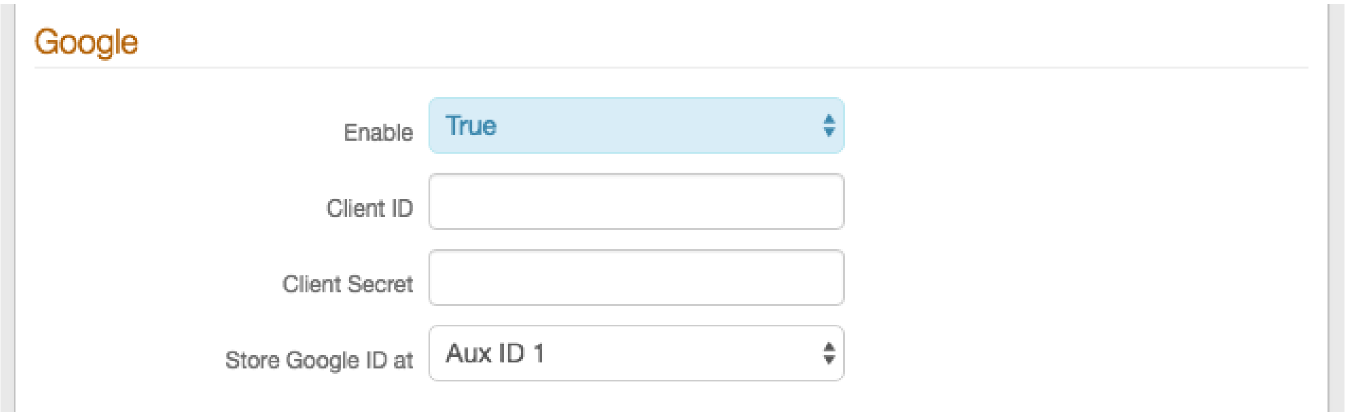
5. Select **True** from the Enable dropdown to enable the use of Google ID for two-factor authentication.

6. Set the **Client ID**, which is provided by Google.

7. Set the **Client Secret**, which is provided by Google.

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

8. Specify where to **Store Google ID at** from the dropdown (example: **Aux ID 2**).



Google

Enable: True

Client ID:

Client Secret:

Store Google ID at: Aux ID 1

Windows Live

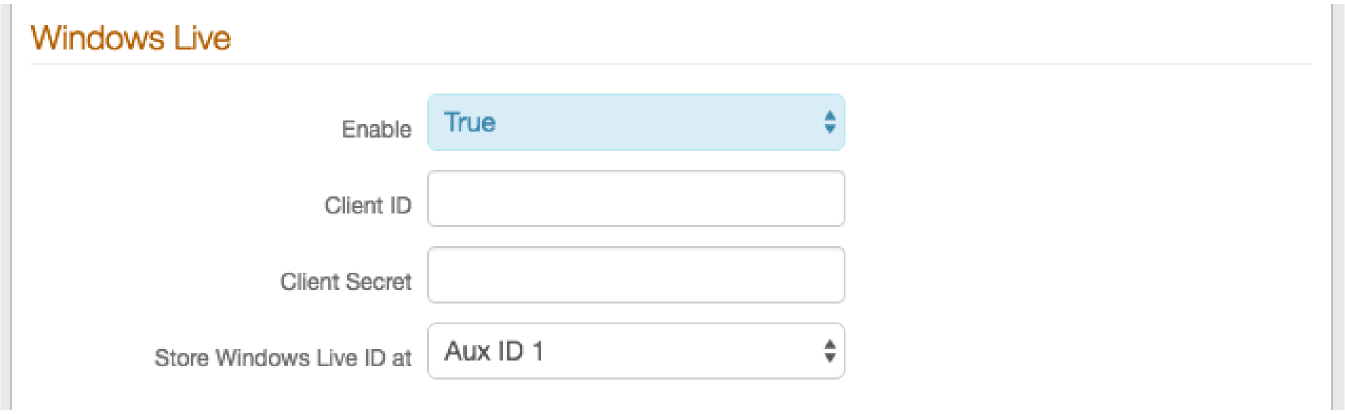
9. Select **True** from the Enable dropdown to use Windows Live ID for two-factor authentication.

10. Set the **Client ID**, which is provided by Windows Live.

11. Set 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.

12. Specify where to **Store Windows Live ID at** from the dropdown (example: **Aux ID 3**).



Windows Live

Enable: True

Client ID

Client Secret

Store Windows Live ID at: Aux ID 1

LinkedIn

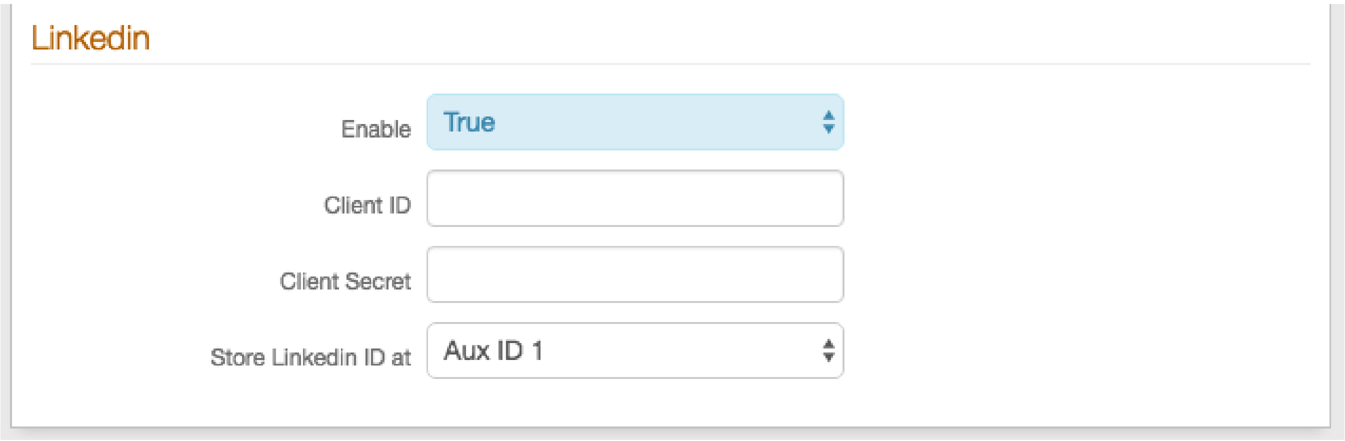
13. Select **True** from the Enable dropdown to use LinkedIn ID for two-factor authentication.

14. Set the **Client ID**, which is provided by LinkedIn.

15. Set the **Client Secret**, which is provided by LinkedIn.

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

16. Specify where to **Store LinkedIn ID at** from the dropdown (example: **Aux ID 4**).



Linkedin

Enable: True

Client ID

Client Secret

Store Linkedin ID at: Aux ID 1

FBA WebService section

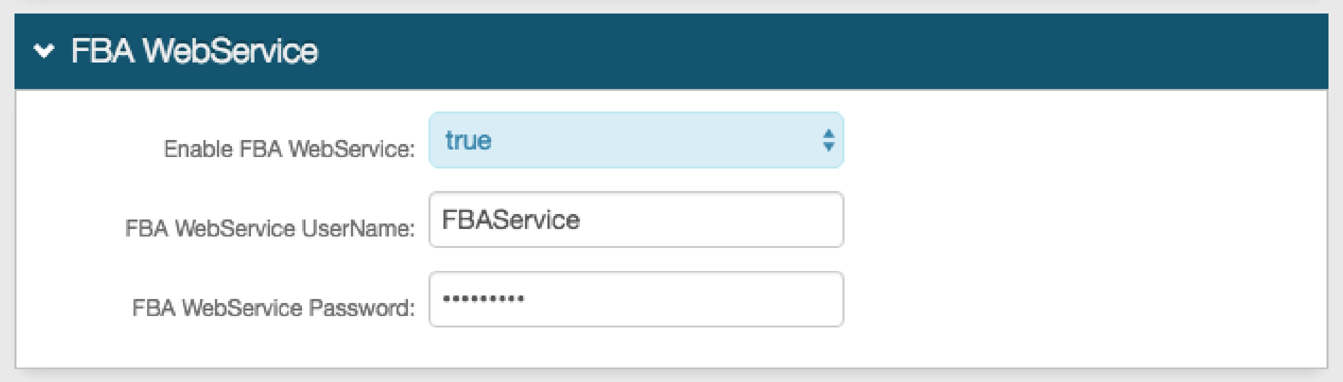
> An FBA WebService configuration is only necessary if using SecureAuth IdP Web Service Multi-data Store, and if required by the SP.

FBA WebService configuration

1. Select **True** from the Enable FBA WebService dropdown.

2. Set the **FBA WebService UserName**, which is the same as the **Webservice Username** on the Data tab.

3. Set the **FBA WebService Password** which corresponds to the username.



Enable FBA WebService: true

FBA WebService UserName: FBAService

FBA WebService Password: ••••••••••

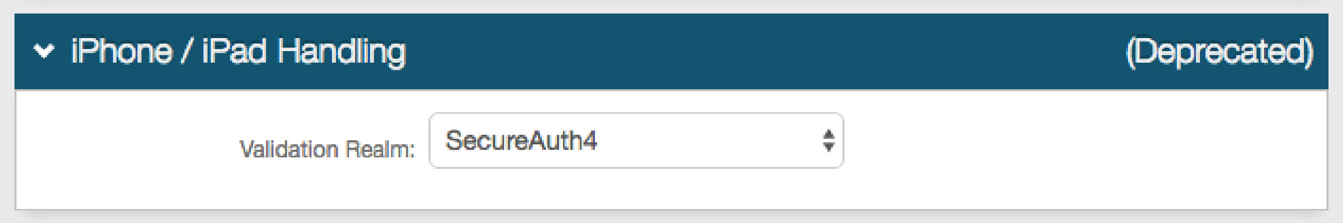
iPhone / iPad Handling section (Deprecated)

An iPhone / iPad Handling configuration is only necessary if users with an iPhone or iPad require redirection.

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

iPhone / iPad configuration

1. Make a selection from the **Validation Realm** dropdown for the SecureAuth IdP realm to which iPhone / iPad users will be redirected.



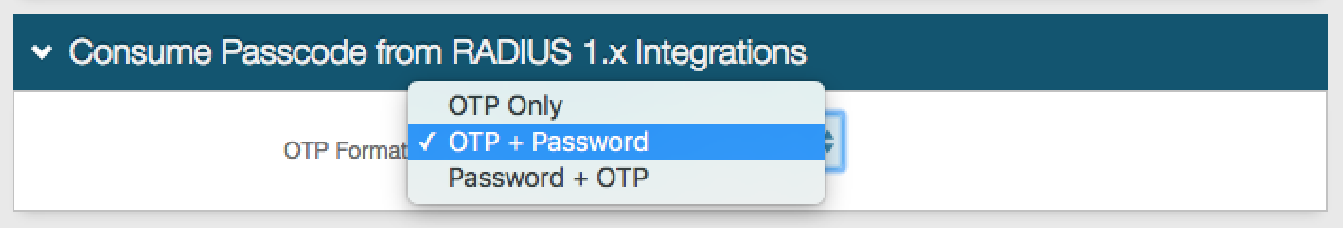
Validation Realm: SecureAuth4

Consume Passcode from RADIUS 1.x Integrations section

This type of configuration is only necessary if using **SecureAuth RADIUS 1.0.x** to make RADIUS web service calls to validate user information.

Consume Passcode from RADIUS 1.x configuration

1. Make a selection from the **OTP Format** dropdown for the type of information to be validated by SecureAuth IdP via the RADIUS web service call.



OTP Format ✓ OTP + Password