Registration Methods Tab Configuration

Introduction

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

This includes 2-Factor Authentication mechanisms enablement and settings, and ID provisioning.

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**, **Data**, and **Workflow** tabs in the Web Admin before configuring the **Registration Methods** tab

Registration Methods Configuration Steps

If the **Authentication Mode** selected in the **Workflow** tab requires 2-Factor Authentication, at least one registration method must be enabled on this page.

Registration Configuration

Phone Settings

Phone Field 1:	Voice and SMS/Text	*telephoneNumber*
Phone Field 2:	Voice Only	*mobile*
Phone Field 3:	SMS/Text Only	*homePhone*
Phone Field 4:	Disabled	*pager*
Phone/SMS Selected:	Voice	
Phone/SMS Visible:	True	
Default Phone Country Code:		
Phone Mask (Regex):		

Email Settings

Email Field 1:	Enabled (HTML)	*mail*
Email Field 2:	Enabled (TEXT)	*wWWHomePage*
Email Field 3:	Disabled	*physicalDeliveryOfficeName*
Email Field 4:	Disabled	*facsimileTelephoneNumber*

Knowledge Based Settings

KB Questions:	Disabled	*info*
KB Format:	Enabled	
Number of Questions:	Disabled	
KB Conversion:	3	
	False	

Help Desk Settings

Help Desk 1:	Disabled	
Phone:	Enabled	
	Disabled	

Email: YourSupport@Company.com

Help Desk 2: Disabled

Phone:

Email:

PIN Settings

PIN Field: Disabled *employeeID*

Open PIN: Enabled / Disabled

One Time Use: False

Show When Empty: False

Time Based Passcodes (OATH)

Time Based Passcodes: Disabled

Passcode Length: Enabled / Disabled

Passcode Change Interval: 60 Second(s)

Passcode Offset: 5 Minute(s)

Cache Lockout Duration: 10 Minute(s) - OATH Service

Mobile Login Requests (Push Notifications)

Request Type: Accept/Deny

Login Request Timeout: Disabled / Passcode (OTP) / Accept/Deny / Passcode (OTP) + Accept/Deny

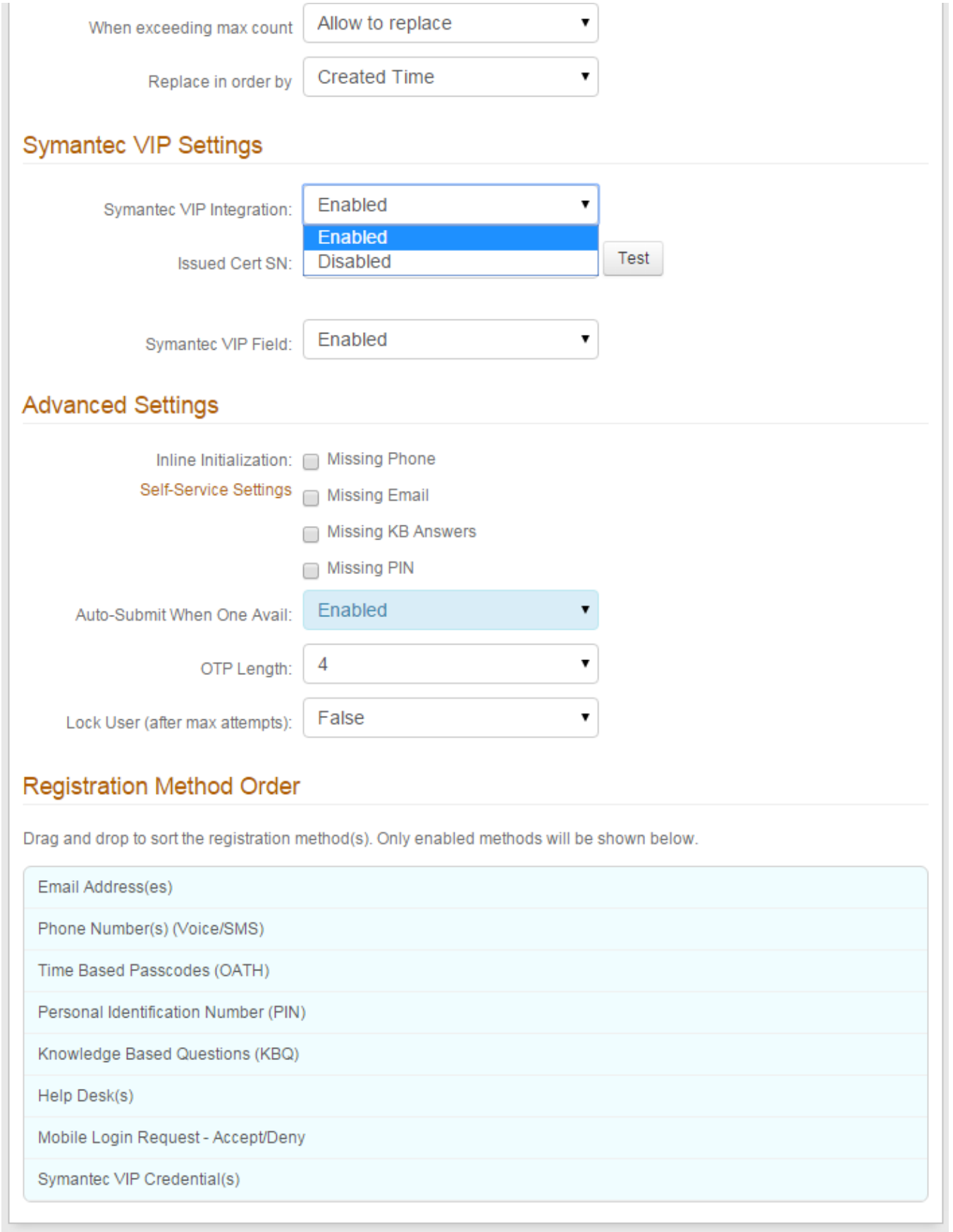
Login Request Content

Company Name

Application Name

Devices Allowed in User Profile

Max Device Count: -1 -1: No limit



1. In the **Registration Configuration** section, under **Phone Settings**, enable **Phone Field 1** by selecting a delivery method of the registration code to **P hone 1** (refer to the **Data** tab for **Profile Property** / data store mapping)

Select **Disabled** from the dropdown if no registration code will be sent to **Phone 1**

2. Enable **Phone Field 2 - Phone Field 4** in the same manner

Select **Disabled** from the corresponding dropdown if no registration code will be sent to **Phone 2**, **Phone 3**, or **Phone 4**

3. Select **Voice** from the **Phone/SMS Selected** dropdown to default the end-user's selection to **Voice** on the login page

4. Select **True** from the **Phone/SMS Visible** dropdown if both **Voice** and **SMS / Text** options are shown, even if both are not available for use

5. Set the **Default Phone Country Code** that will be appended to any user phone numbers in the directory that do not have a country code provided

Leave field empty if there is no default

6. Set the appearance of the end-users' phone numbers by designing a **Phone Mask (Regex)**, e.g. xxx-xx1-2345

SecureAuth IdP automatically displays phone numbers as **xxx-xxx-1234**

Leave field empty if the out-of-the-box display is acceptable

7. Under **Email Settings**, enable **Email Field 1** by selecting a delivery method of the registration code to **Email 1** (refer to the **Data** tab for **Profile Property** / data store mapping)

Select **Disabled** from the dropdown if no registration code will be sent to **Email 1**

8. Enable **Email Field 2 - Email Field 4** in the same manner

Select **Disabled** from the corresponding dropdown if no registration code will be sent to **Email 2**, **Email 3**, or **Email 4**

9. Under **Knowledge Based Settings**, select **Enabled** from the **KB Questions** dropdown to enable the use of knowledge-based questions for 2-Factor Authentication

10. Select the method in which the knowledge-based questions will be formatted from the **KB Format** dropdown

11. Select the **Number of Questions** that will be displayed on the login page from the dropdown

12. Select **True** from the **KB Conversion** dropdown to enable the conversion of knowledge-based questions to certificate-based encryption from Base64 encoding

13. Under **Help Desk Settings**, select **Enabled** from the **Help Desk 1** dropdown to enable the use of Help Desk 1 for 2-Factor Authentication

14. Provide the **Phone** number of the Help Desk that end-users can call for a registration code

15. Provide the **Email** address of the Help Desk that end-users can message for assistance

16. Select **Enabled** from the **Help Desk 2** dropdown to enable the use of Help Desk 2 for 2-Factor Authentication

17. Provide the **Phone** number of the second Help Desk that end-users can call for a registration code

18. Provide the **Email** address of the second Help Desk that end-users can message for assistance

Refer to **Second Help Desk Registration Method Configuration Guide** for more information

19. Under **PIN Settings**, select **Enabled** from the **PIN Field** dropdown to enable the use of static PINs for 2-Factor Authentication

The end-user's Personal Identification Number (PIN) must be contained in the data store and mapped to the SecureAuth IdP **PIN Property**

20. Select **True** from the **Open PIN** dropdown to store the PIN in plain text versus encryption

21. Select **True** from the **One Time Use** dropdown to enable a one-time-use PIN that is immediately cleared from the directory after use

This is typically utilized for first-time users in self-service enrollment processes

22. Select **True** from the **Show When Empty** dropdown if the **One Time Use** PIN is displayed as an option on the login page, but is inactive for use

23. Under **Time-based Passcodes (OATH)**, select **Enabled** from the **Time-based Passcodes** dropdown to enable the use of mobile, browser, desktop, or third-party OATH OTP soft tokens for 2-Factor Authentication

24. Select the number of digits of which a Passcode is compromised from the **Passcode Length** dropdown

25. Set the number of seconds during which a Passcode is displayed in the **Passcode Change Interval** field

26. Set the number of minutes during which a Passcode is valid to make up for time differences between devices in the **Passcode Offset** field

The **Passcode Length** and **Passcode Change Interval** fields must match the values configured in the **Post Authentication** tab of the **SecureAuth App Enrollment Realm**

27. Set the number of minutes during which the account is locked from utilizing Passcodes after too many failed OTP attempts in the **Cache Lockout Duration** field

28. Under **Mobile Login Requests (Push Notifications)**, select the type of Push Notification(s) to be used in this realm for 2-Factor Authentication from the **Push Notification Field** dropdown

- **Passcode (OTP)**: Enable the use of Push Notifications, which are one-time passcodes sent (pushed) directly to an end-user's enrolled mobile device
- **Accept / Deny**: Enable the use of Push-to-Accept requests, which are login requests sent to the **SecureAuth Authenticate App for iOS and Android** that require an end-user to **Accept** or **Deny** the login request
- **Passcode (OTP) + Accept / Deny**: Enable the use of Push Notifications *and* Push-to-Accept requests

29. Select the number of minutes a Push-to-Accept request is valid for response from the **Login Request Timeout** dropdown (if an **Accept / Deny** option is selected in step 28)

30. Set the **Company Name**, which displays on the Push-to-Accept request (optional, and if an **Accept / Deny** option is selected in step 28)

31. Set the **Application Name** to the post-authentication target (e.g. Salesforce, Password Reset, etc.), which displays on the Push-to-Accept request (optional, and if an **Accept / Deny** option is selected in step 28)

32. Limit the number of devices enrolled for Push Notifications / Push-to-Accept requests in the **Max Device Count** field

    Set this to **-1** if there is no limit

33. Select **Allow to replace** from the **When exceeding max count** dropdown to enable device replacement once the limit has been reached

34. Select **Created Time** from the **Replace in order by** dropdown to replace the oldest enrolled device with the new one

    Select **Last Access Time** to replace the least recently used enrolled device with the new one

35. Under **Symantec VIP Settings**, select **Enabled** from the **Symantec VIP Integration** dropdown to initiate the integration of Symantec VIP with SecureAuth IdP

36. Provide the certificate serial number (provided by Symantec) in the **Issued Cert SN** field

37. Select **Enabled** from the **Symantec VIP Field** to enable the use of Symantec VIP tokens for 2-Factor Authentication

38. Under **Advanced Settings**, check **Missing Phone**, **Missing Email**, **Missing KB Answers**, and/or **Missing PIN** from the **Inline Initialization** menu to enable end-users to update or provide missing information and then be redirected back to the login pages

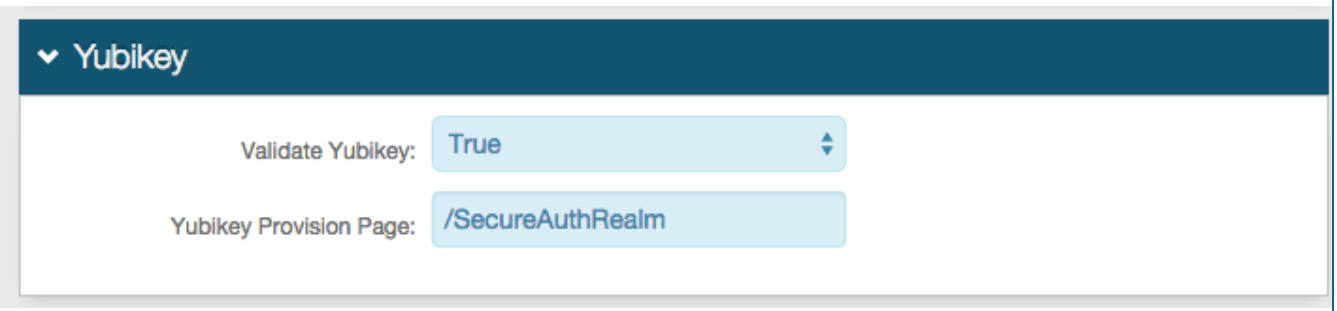
39. Select **Enabled** from the **Auto-Submit When One Avail** dropdown to automatically select the registration method on the login page when only one is available for the user's account

40. Select the number of digits of which the One-time Passwords (OTPs) will be comprised from the **OTP Length** dropdown

41. Select **True** from the **Lock User** to lock an end-user's directory account after so many failed login attempts

42. Under **Registration Method Order**, drag and drop the enabled registration methods on the list to organize their display on the login page

Yubikey

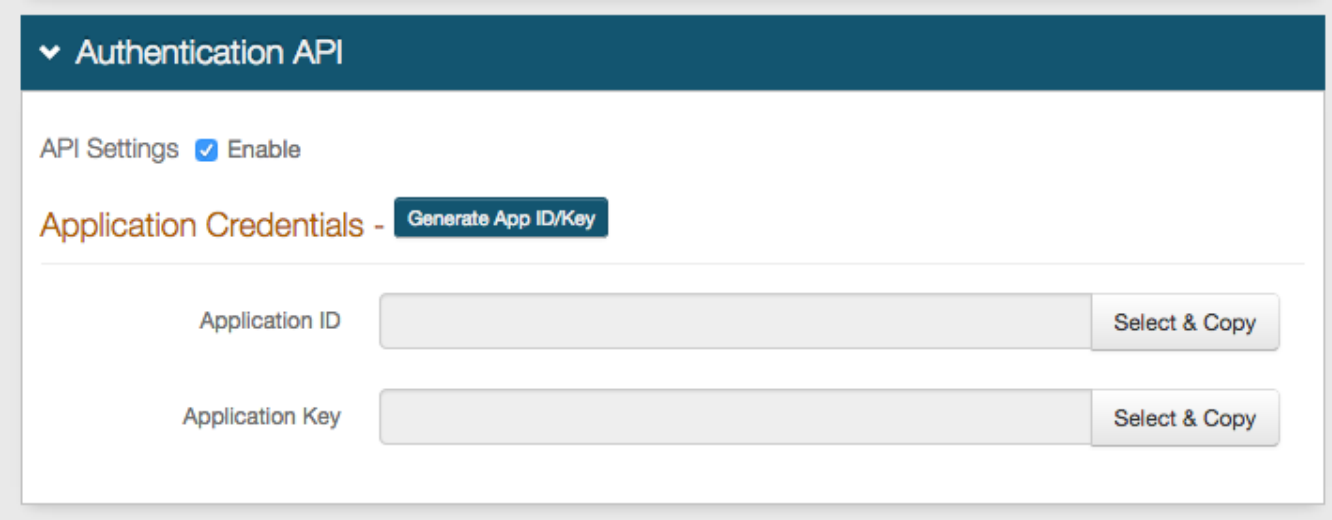


43. Select **True** from the **Validate Yubikey** dropdown to enable the use of Yubikeys for 2-Factor Authentication

44. Provide the **Yubikey Provision Page** URL at which end-users can provision their Yubikeys

    This would be another SecureAuth IdP realm, configured in the **Post Authentication** tab

Authentication API



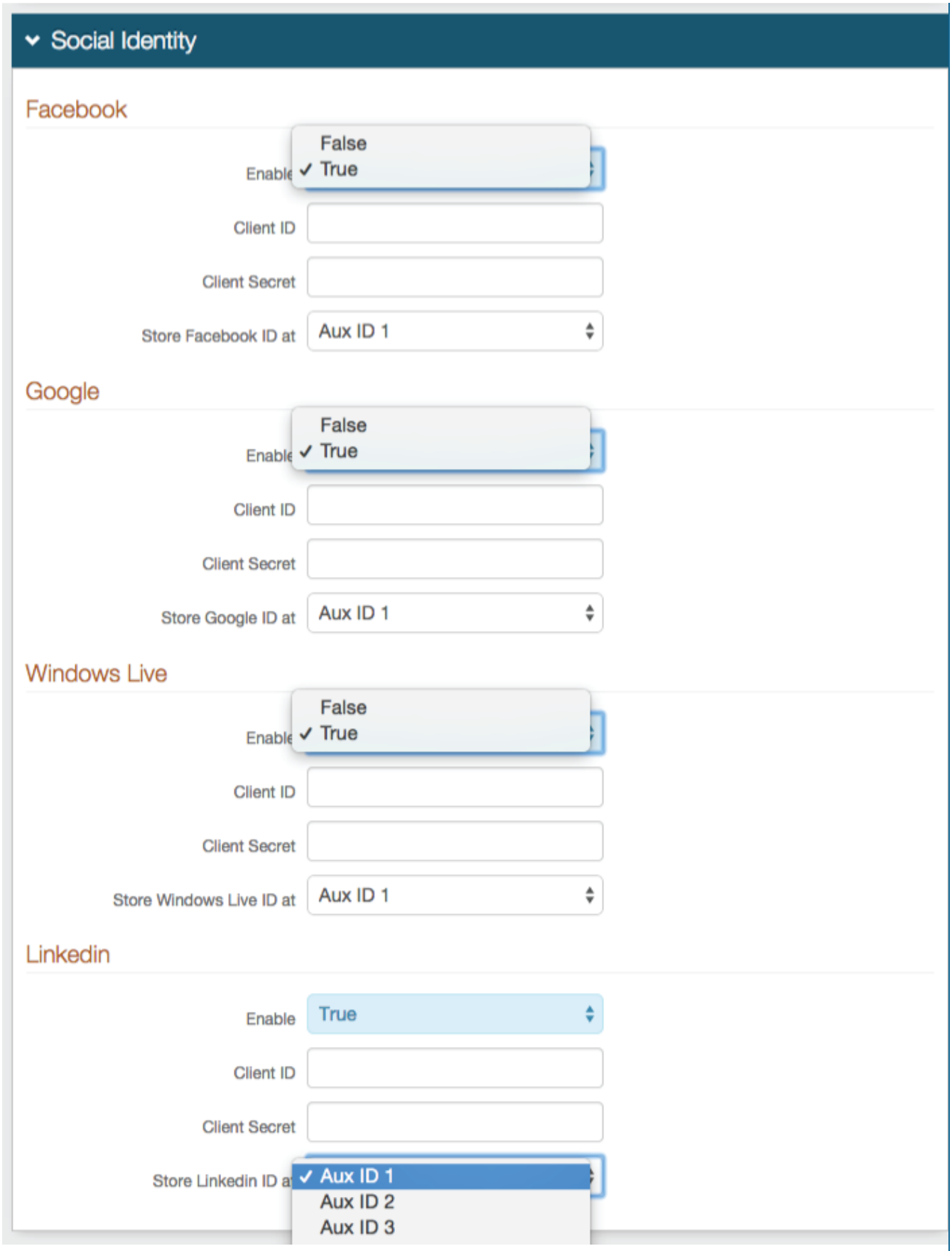
45. Check **Enable** to enable the use of the **Authentication API** in this realm

46. Click **Generate App ID/Key** to generate the Application ID and Application Key to use in the API

    Refer to **Authentication API 8.2 Configuration Guide** for more information

Social Identity

NOTE: Social Identities as second factor mechanisms can only be enabled if an **LDAP directory** is being used as the **Membership Data Store** and the **Profile Provider** (configured in the **Data Tab**)


Social Identity
Facebook
False
Enable
True
Client ID
Client Secret
Store Facebook ID at
Aux ID 1
Google
False
Enable
True
Client ID
Client Secret
Store Google ID at
Aux ID 1
Windows Live
False
Enable
True
Client ID
Client Secret
Store Windows Live ID at
Aux ID 1
Linkedin
Enable
True
Client ID
Client Secret
Store Linkedin ID at
Aux ID 1
Aux ID 2
Aux ID 3

47. Under **Facebook**, select **True** from the **Enable** dropdown to enable the use of Facebook ID for 2-Factor Authentication

48. Provide the **Client ID**, which is provided by Facebook

49. 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

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

51. Under **Google**, select **True** from the **Enable** dropdown to enable the use of Google ID for 2-Factor Authentication

52. Provide the **Client ID**, which is provided by Google

53. 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

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

55. Under **Windows Live**, select **True** from the **Enable** dropdown to enable the use of Windows Live ID for 2-Factor Authentication

56. Provide the **Client ID**, which is provided by Windows Live

57. 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

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

59. Under **LinkedIn**, select **True** from the **Enable** dropdown to enable the use of LinkedIn ID for 2-Factor Authentication

60. Provide the **Client ID**, which is provided by LinkedIn

61. 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

62. Select where to **Store LinkedIn ID at** from the dropdown (e.g. **Aux ID 4**)

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