Multi-Factor Methods configuration

Introduction

The Multi-Factor Methods tab is configured on a SecureAuth IdP realm to provide the method(s) end-users can select and use for authentication. If the Authentication Mode selected on the Workflow tab requires user authentication, at least one authentication method must be enabled on the Multi-Factor Methods tab.

Authentication methods available for configuring on this tab include:

- Phone
- Phone Number Blocking
- Email
- Knowledge Based Questions and Answers
- Help Desk
- PIN
- Timed Passcodes
- Mobile Login Requests
- YubiKey
- Symantec VIP
- Inline Initialization
- Multi-Factor Throttling

What's new in SecureAuth IdP version 9.3

Inline Initialization - Self-service has been enhanced to enable setting a maximum of four different types of phone numbers and four different types of email addresses to be required in a user's profile.

Multi-Factor Methods guides from the previous release

See the collection of Multi-Factor Methods 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
  - Workflow tab

> 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

Multi-Factor Methods tab

Multi-Factor Configuration section

Phone Settings

1. Enable **Phone Field 1** by selecting a delivery method of the registration code to **Phone 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)** which SecureAuth IdP will automatically display for the end-user. Or leave this field empty if the out-of-box display is acceptable.

If setting a value in this field, then the user's phone number must contain the *exact* number of digits defined. Any dash or character other than "x" and "n" will appear in its appropriate place in the user's phone number.

For example, if the Regex value is xxx-xxn-nnnn, and the phone number entered is 1234567890, then this number will appear as xxx-xx6-7890

To accommodate a country code, the Regex value must contain a pipe character (|) between the country code and the start of the phone number. For example, if the Regex value is x|xxx-xxn-nnnn, and the phone number is +1 123-456-7890, then this number will appear as xxxx-xx6-7890

Note that more than one Regex value can be entered in this field, if more than one phone number format is required, as in the previous two scenarios described. For this configuration, each Regex value must be separated by a comma (,). In this example, the Regex values would be entered as: xxx-xxn-nnnn,x|xxx-xxn-nnnn

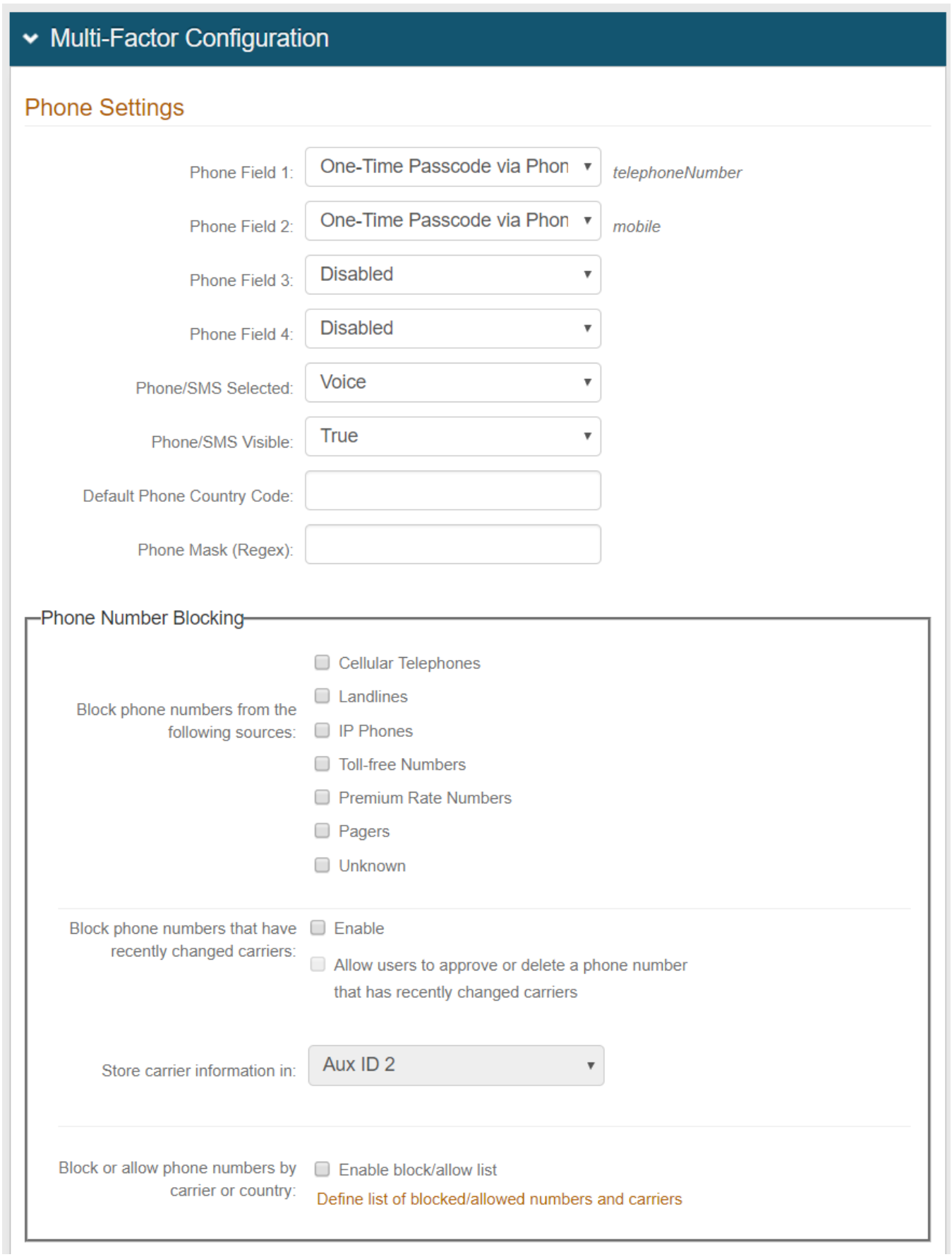
Phone Number Blocking

7. Select types of phone numbers to block from the **Block phone numbers from the following sources** options.

8. Check **Enable** to **Block phone numbers that have recently changed carriers**, then select a directory attribute to **Store carrier information in**.

9. Check **Enable block/allow list** to **Block or allow phone numbers by carrier or country**, then click **Define list of blocked/allowed numbers and carriers**.

Refer to Phone Number Profiling Service Configuration Guide for more information on configuring **Phone Number Blocking** settings.



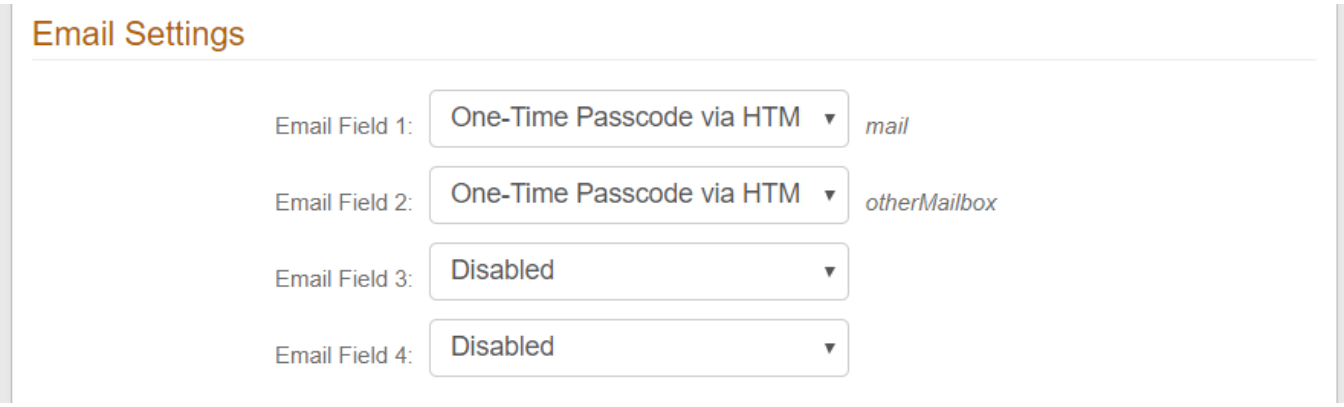
Email Settings

10. Enable **Email Field 1** by selecting a delivery method to send 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**.

11. 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**.



Knowledge Based Settings

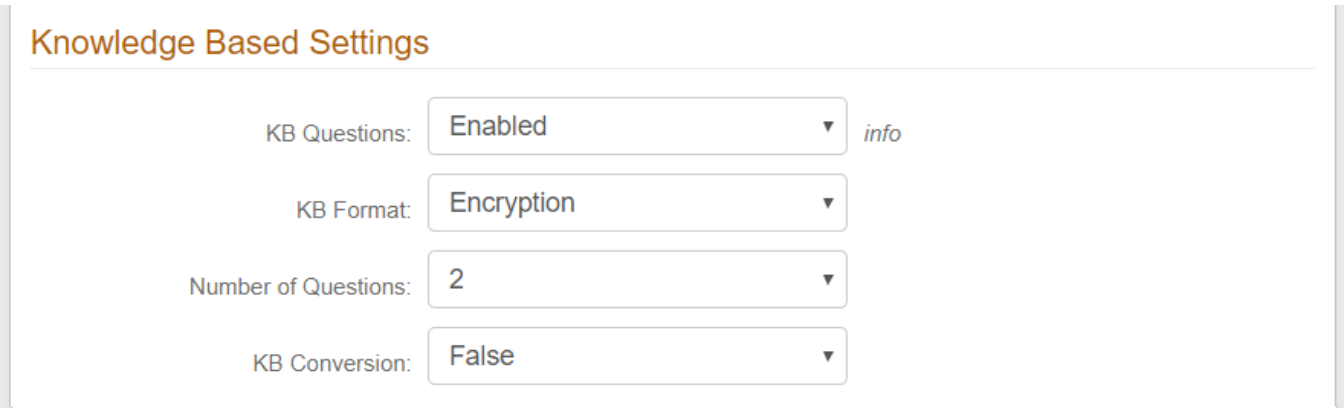
12. Select **Enabled** from the **KB Questions** dropdown to use of knowledge based questions for Multi-Factor Authentication.

13. Select the **KB Format** to specify the method to use for formatting knowledge based questions:

    Encryption for maximum security during the end-user's login process, or **Base 64** encoding algorithm.

14. Select the **Number of Questions** to appear on the login page.

15. Select **True** from the **KB Conversion** dropdown only if knowledge based questions should be converted to certificate-based encryption via Base64 encoding.



Help Desk Settings

16. Select **Enabled** from the **Help Desk 1** dropdown to use Help Desk 1 for Multi-Factor Authentication.

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

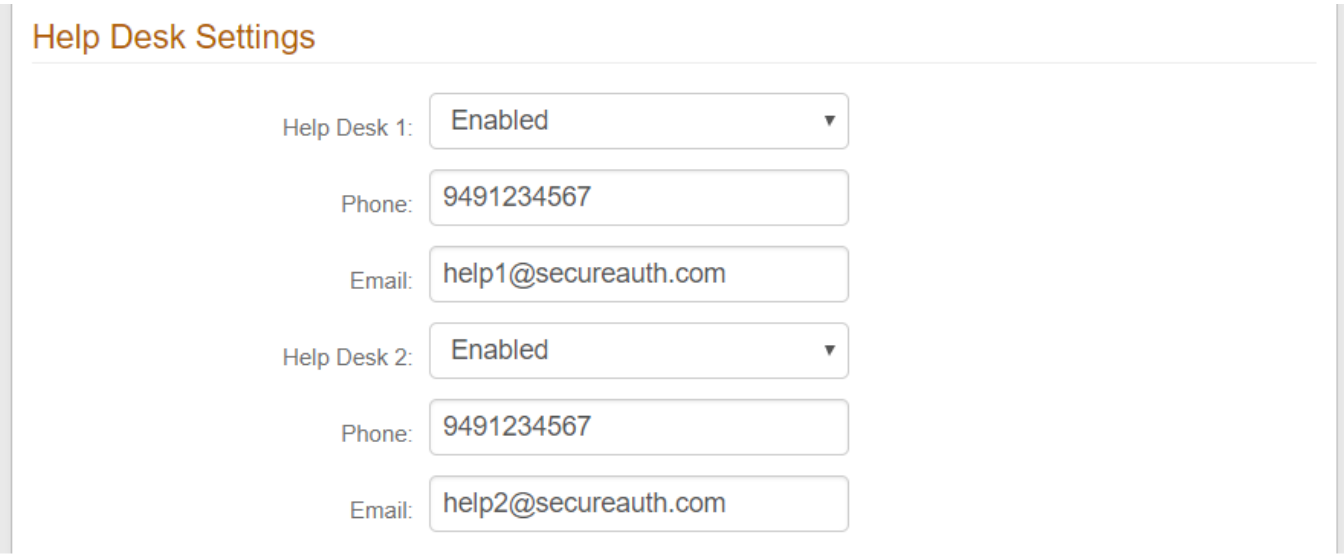
18. Provide the **Email** address of the Help Desk that end-users can message for assistance.

19. Select **Enabled** from the **Help Desk 2** dropdown to use Help Desk 2 for Multi-Factor Authentication.

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

21. 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.



PIN Settings

22. Select **Enabled** from the **PIN Field** dropdown to enable the use of static PINs for Multi-Factor Authentication.

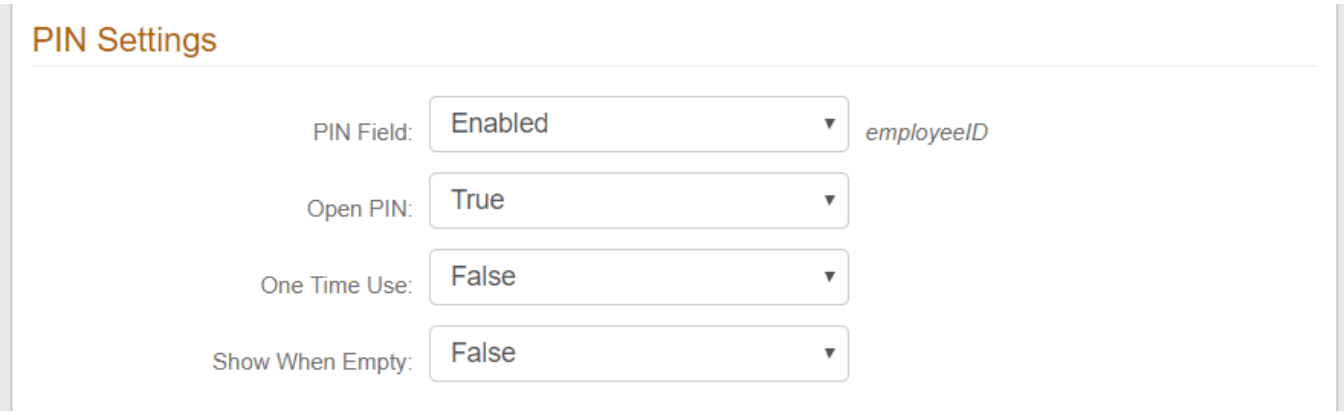
    The end-user's Personal Identification Number (PIN) must be contained in the data store and mapped to the SecureAuth IdP **PIN Property**.

23. Select **True** from the **Open PIN** dropdown to store the PIN in plain text format versus encrypted format.

24. 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 used by first-time users in self-service enrollment processes.

25. Select **True** from the **Show When Empty** dropdown if the **One Time Use** PIN will appear as an option on the login page, but be inactive for use.



Time-based Passcodes (OATH)

26. Select **Enabled** from the **Time-based Passcodes** dropdown to use mobile, browser, desktop, or third-party OATH OTP soft tokens for Multi-Factor Authentication.

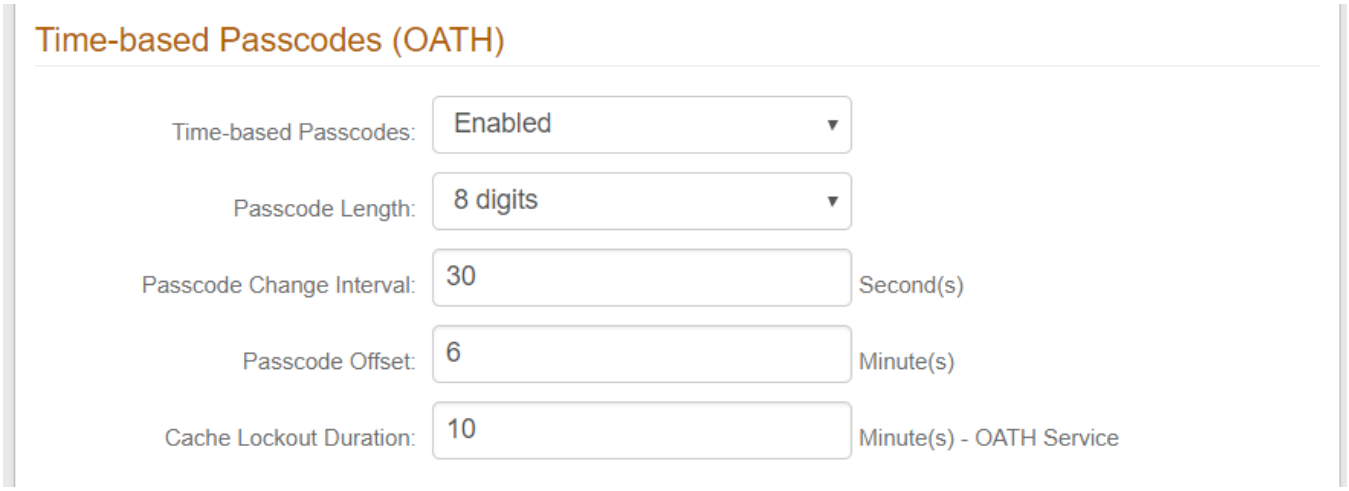
27. Select the number of digits in the passcode from the **Passcode Length** dropdown.

28. Make an entry in the **Passcode Change Interval** field to set the number of seconds a passcode is available.

29. Make an entry in the **Passcode Offset** field to set the number of minutes between devices for the passcode to remain valid.

    The **Passcode Length** and **Passcode Change Interval** fields must match the values configured in the **Post Authentication** tab of the Multi-Factor App Enrollment (URL) realm.

30. Make an entry in the **Cache Lockout Duration** field to set the number of minutes an account remains locked after using passcodes for too many failed OTP attempts.



Mobile Login Requests (Push Notifications)

31. Make a selection from the **Push Notification Field** dropdown for the type of Push Notification(s) to be used for Multi-Factor Authentication on this realm:

- **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 Android and iOS 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.

32. Make a selection from the **Login Request Timeout** dropdown for the number of minutes a Push-to-Accept request is valid for response – if **Accept / Deny** is selected in step 31.

33. Set the **Company Name** that appears on the Push-to-Accept request – this optional setting is only needed if **Accept / Deny** is selected in step 31.

34. Set the **Application Name** to the post-authentication target (for example: Salesforce, Password Reset, etc.) that appears on the Push-to-Accept request – this optional setting is only needed if **Accept / Deny** is selected in step 31.

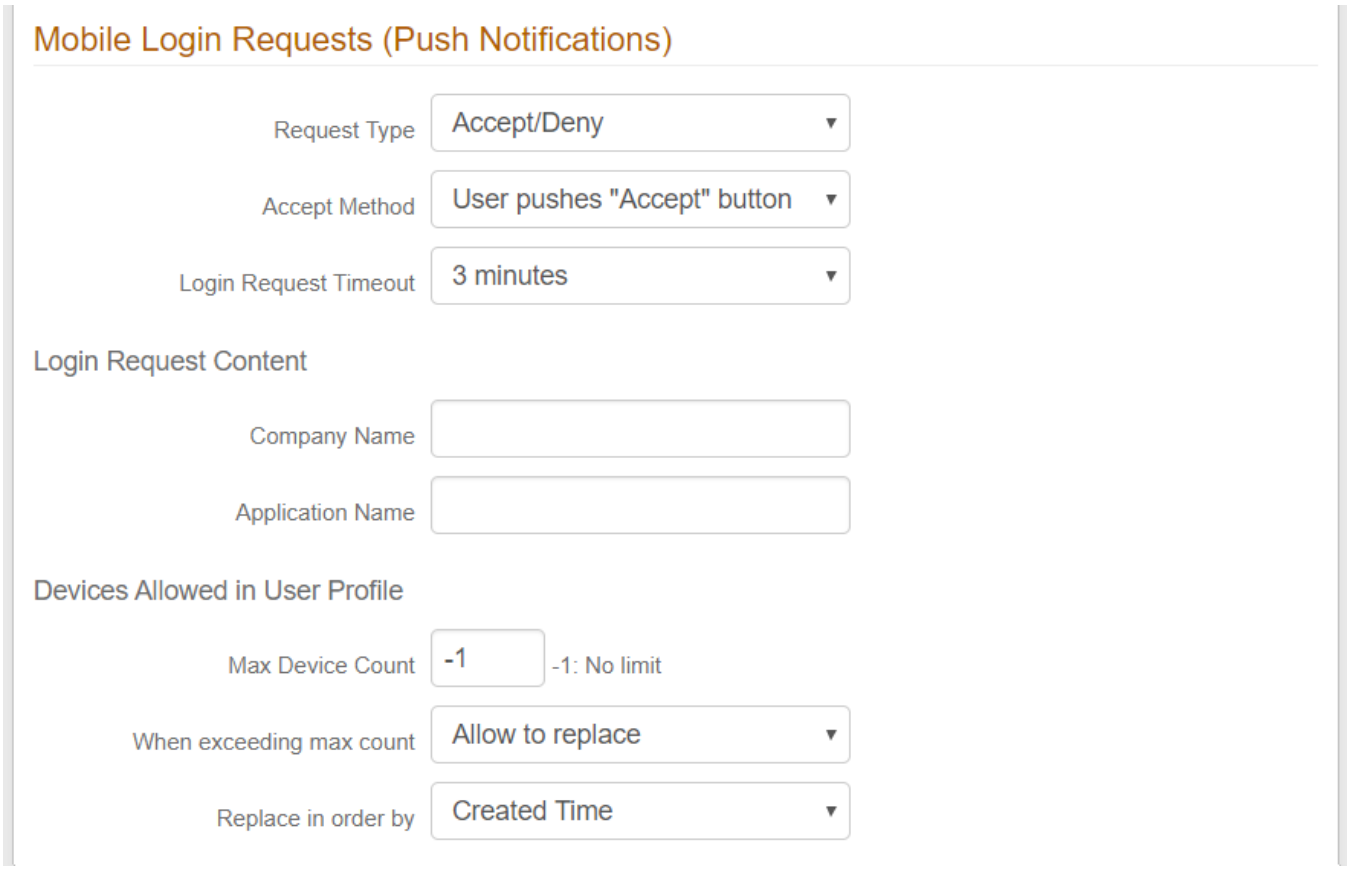
35. Make an entry in the **Max Device Count** field to limit the number of devices enrolled for Push Notifications / Push-to-Accept requests.

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

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

37. 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.



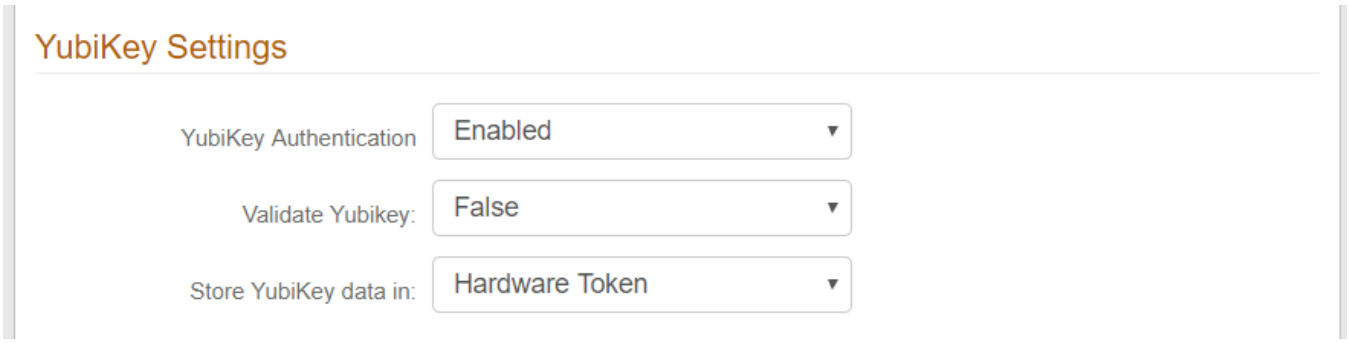
YubiKey Settings

38. Select **Enabled** from the **YubiKey Authentication** dropdown to let end-users use a YubiKey device for Multi-Factor Authentication.

    Refer to YubiKey Multi-Factor Authentication Configuration Guide for more information.

39. Select **True** from the **Validate Yubikey** dropdown if a One-time Passcode (OTP) is required in addition to the YubiKey device to validate the end-user.

40. Select the property (Hardware Token, or Aux ID 1 - Aux ID 10) from the **Store YubiKey data in** dropdown – this must be the same property configured on the Data tab for storing YubiKey data.

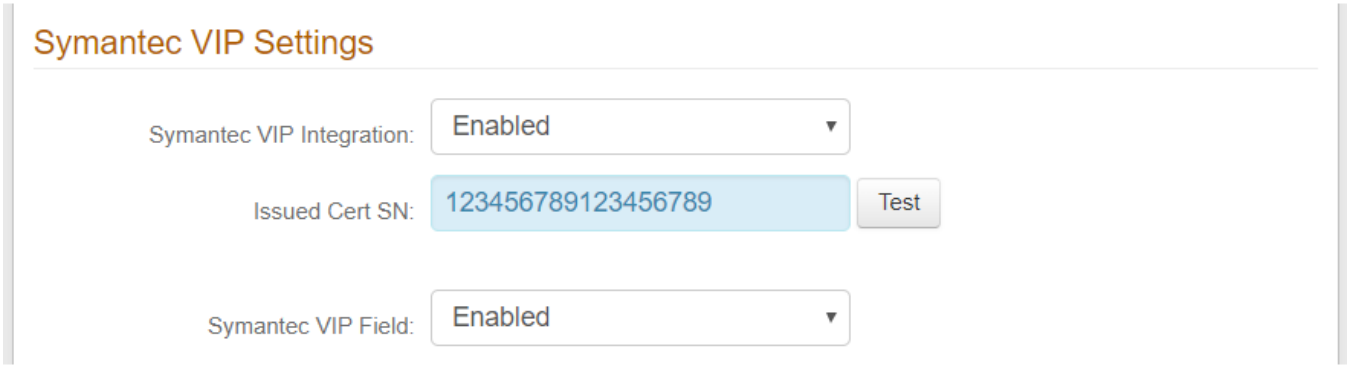


Symantec VIP Settings

41. Select **Enabled** from the **Symantec VIP Integration** dropdown to initiate the integration of Symantec VIP with SecureAuth IdP.

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

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



Multi-Factor Settings

44. 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 profile information and then be redirected back to the login pages.

45. If Missing Phone or Missing Email are selected, then you can specify up to four different types of phone numbers or email addresses that are required for entry in the user profile.

> Refer to Inline Initialization - Self-service profile update for more information.

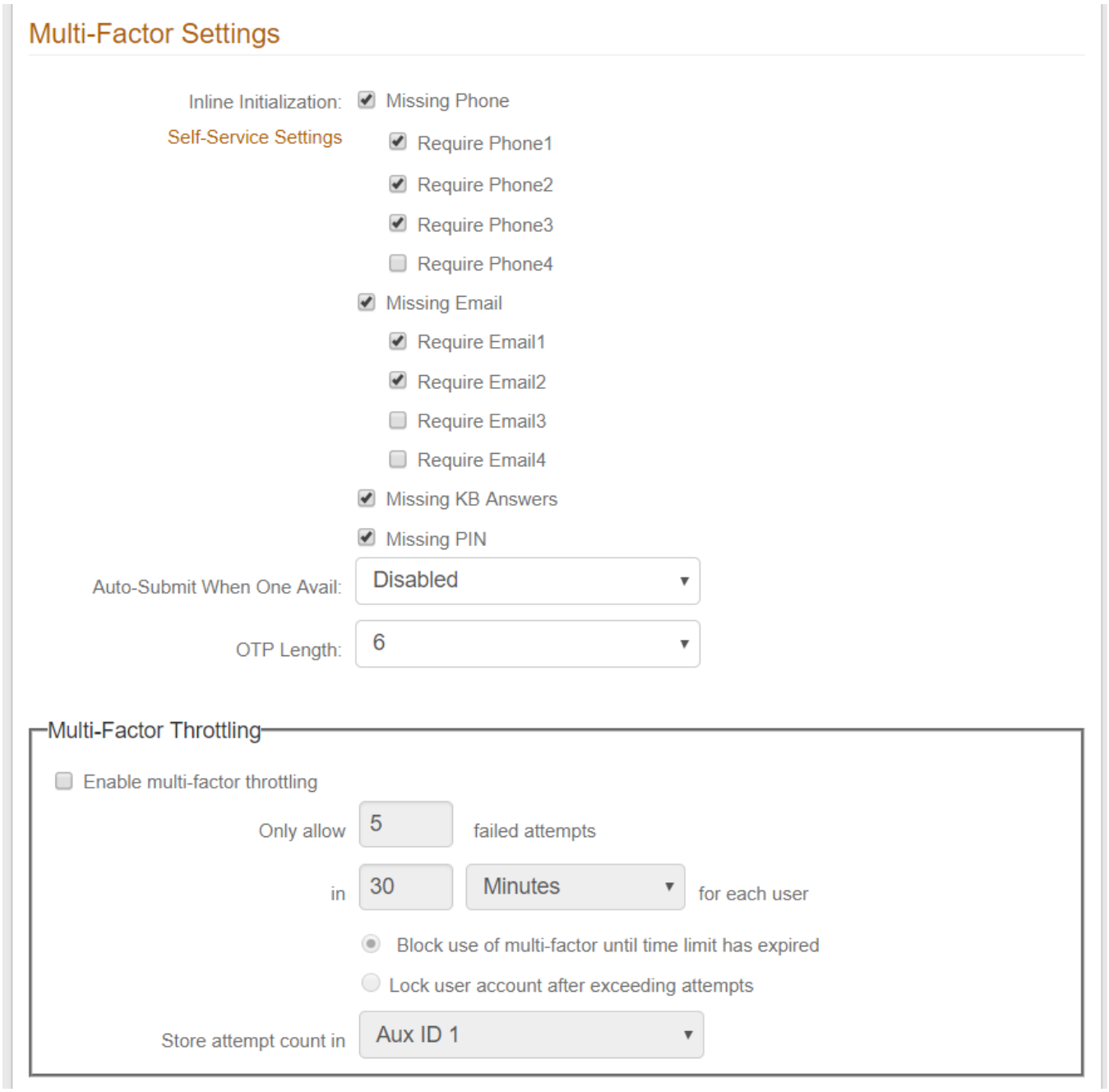
46. Select **Enabled** from the **Auto-Submit When One Avail** dropdown to automatically select the registration method on the login page when only one is available for the user's account.

47. Make a selection from the **OTP Length** dropdown to set the number of digits to be used in One-time Passwords (OTPs) for a configured PIN OTP page.

> Refer to PIN OTP Page Configuration Guide for more information.

48. Check **Enable multi-factor throttling** to limit the number of multi-factor authentication attempts allowed within a rolling time period (specified below).

> Refer to Multi-Factor Throttling Configuration Guide for more information.



Multi-Factor Method Order

49. Drag and drop the enabled registration methods on the list to order their appearance on the login page.

Multi-Factor Method Order

Drag and drop to sort the registration method(s). Only enabled methods will be shown below.

- Email Address(es)
- Phone Number(s) (Voice/SMS)
- Knowledge Based Questions (KBQ)
- Personal Identification Number (PIN)