Multi-Factor Methods Tab Configuration

Introduction

Use this guide to configure the Multi-Factor Methods tab in the Web Admin for each SecureAuth IdP realm in SecureAuth IdP version 9.1 or 9.2.

This includes Multi-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 **Multi-Factor Methods** tab

Multi-Factor Methods Configuration Steps

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

When the end-user is presented the page of Multi-Factor Authentication methods from which to choose, the Multi-Factor Authentication method that was last selected and used in a successful login attempt persists as the default method for the next login in each device / browser

Multi-Factor Configuration

Phone Settings

Phone Field 1: One-Time Passcode via Phon ▾ *telephoneNumber*

Phone Field 2:
Phone Field 3:

- Login Request
- One-Time Passcode via Phone Call and SMS
- One-Time Passcode via Phone Call Only
- One-Time Passcode via SMS Only
- Disabled

Phone Field 4: Disabled ▾ *otherTelephone*

Phone/SMS Selected: Voice ▾

Phone/SMS Visible: True ▾

Default Phone Country Code:

Phone Mask (Regex):

Phone Number Blocking

Block phone numbers from the following sources:

- ☐ Cellular Telephones
- ☐ Landlines
- ☐ IP Phones
- ☐ Toll-free Numbers
- ☐ Premium Rate Numbers
- ☐ Pagers
- ☐ Unknown

Block phone numbers that have recently changed carriers:

- ☐ Enable
- ☐ Allow users to approve or delete a phone number that has recently changed carriers

Store carrier information in: Aux ID 2 ▾

Block or allow phone numbers by carrier or country:

- ☐ Enable block/allow list

Define list of blocked/allowed numbers and carriers

Email Settings

Email Field 1: One-Time Passcode via HTM ▾ *mail*

Email Field 2: *ailbox*

Email Field 3: *leTelephoneNumber*

Email Field 4: Disabled ▾ *otherFacsimileTelephoneNumber*

- Login Request via HTML Email
- Login Request via Plain Text Email
- One-Time Passcode via HTML Email
- One-Time Passcode via Plain Text Email
- Disabled

Knowledge Based Settings

KB Questions: Disabled ▾ *info*

KB Format:

- Enabled
- Disabled

Number of Questions: 3 ▾

KB Conversion: 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 ▾

- Enabled

Passcode Length: 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

When exceeding max count: Allow to replace

Replace in order by: Created Time

YubiKey Settings

YubiKey Authentication: Disabled

Enabled
Disabled

Validate Yubikey:

Store YubiKey data in: Hardware Token

Symantec VIP Settings

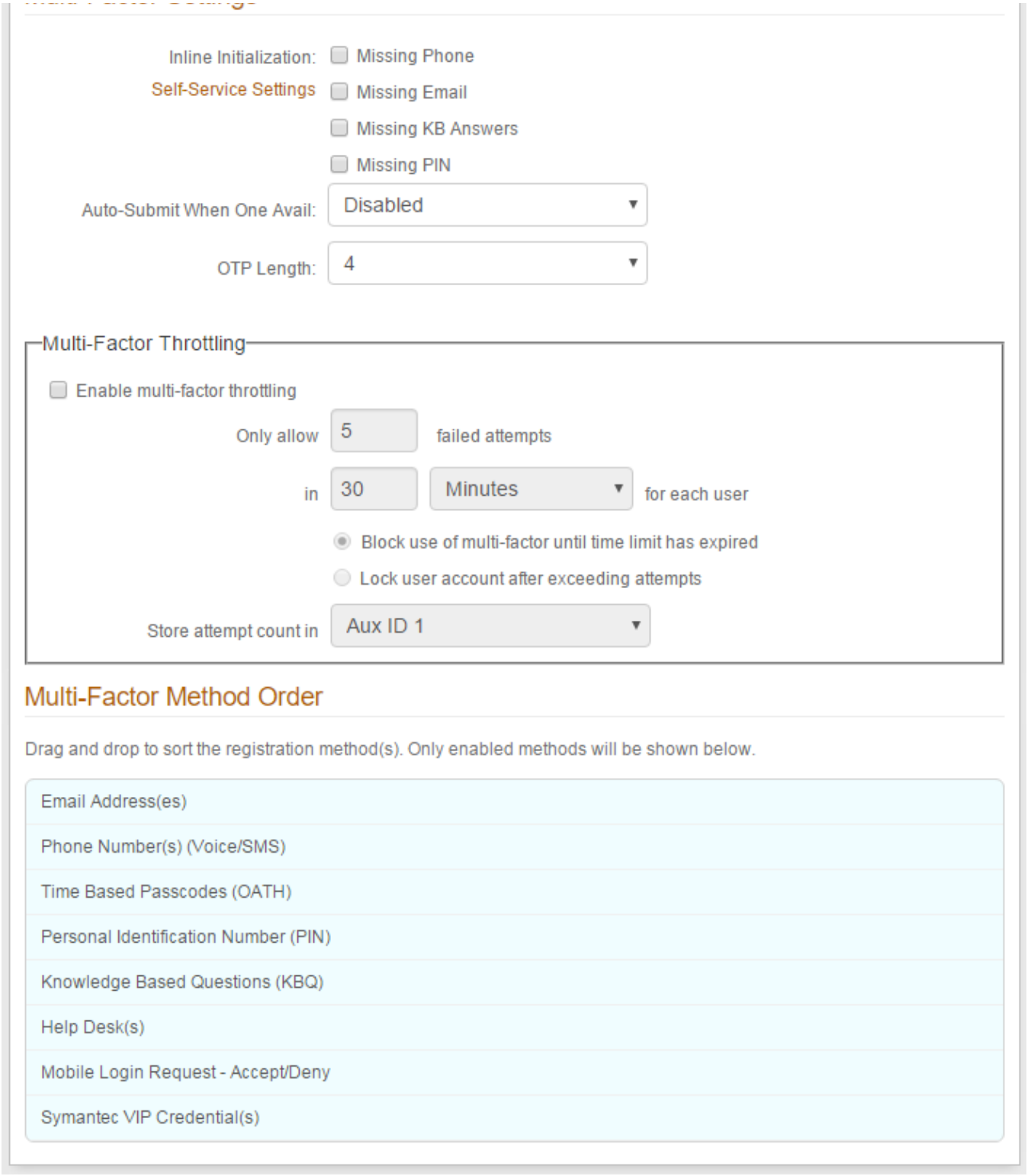
Symantec VIP Integration: Enabled

Enabled
Disabled

Issued Cert SN: Test

Symantec VIP Field: Enabled

Multi-Factor Settings



1. In the **Multi-Factor Configuration** section, under **Phone Settings**, 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

7. In the **Phone Number Blocking** frame, 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

10. 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**

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**

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

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

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

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

16. Under **Help Desk Settings**, select **Enabled** from the **Help Desk 1** dropdown to enable the use of 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 enable the use of 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

22. Under **PIN Settings**, 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 versus encryption

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 utilized for first-time users in self-service enrollment processes

25. 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

26. 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 Multi-Factor Authentication

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

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

29. 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 **Multi-Factor App Enrollment Realm**

30. 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

31. Under **Mobile Login Requests (Push Notifications)**, select the type of Push Notification(s) to be used in this realm for Multi-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 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. 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 31)

33. Set the **Company Name**, which displays on the Push-to-Accept request (optional, and if an **Accept / Deny** option is selected in step 31)

34. 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 31)

35. 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

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

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

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

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

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

41. 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

42. 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

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

44. Under **Multi-Factor 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

45. 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

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

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

    Refer to **Multi-Factor Throttling Configuration Guide** for more information

48. Under **Multi-Factor Method Order**, drag and drop the enabled registration methods on the list to organize their display on the login page