Post Authentication configuration

Introduction

The Post Authentication tab must be configured on each SecureAuth IdP realm to identify its target resource.

In SecureAuth IdP version 9.3, the Classic Experience user interface – not the New Experience user interface – is used to configure the Post Authentication tab for application integrations, out-of-the-box IdM tools, mobile and VPN integrations, certificate deliveries, and provisioning.

What's new in SecureAuth IdP version 9.3

Updates to Post Authentication configuration for:

- Multi-Factor App Enrollment (QR Code) realm configuration
- Multi-Factor App Enrollment (URL) realm configuration
- OpenID Connect and OAuth 2.0 configuration

Post Authentication guides from the previous release

See the collection of Post Authentication 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
  - Multi-Factor Methods 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.

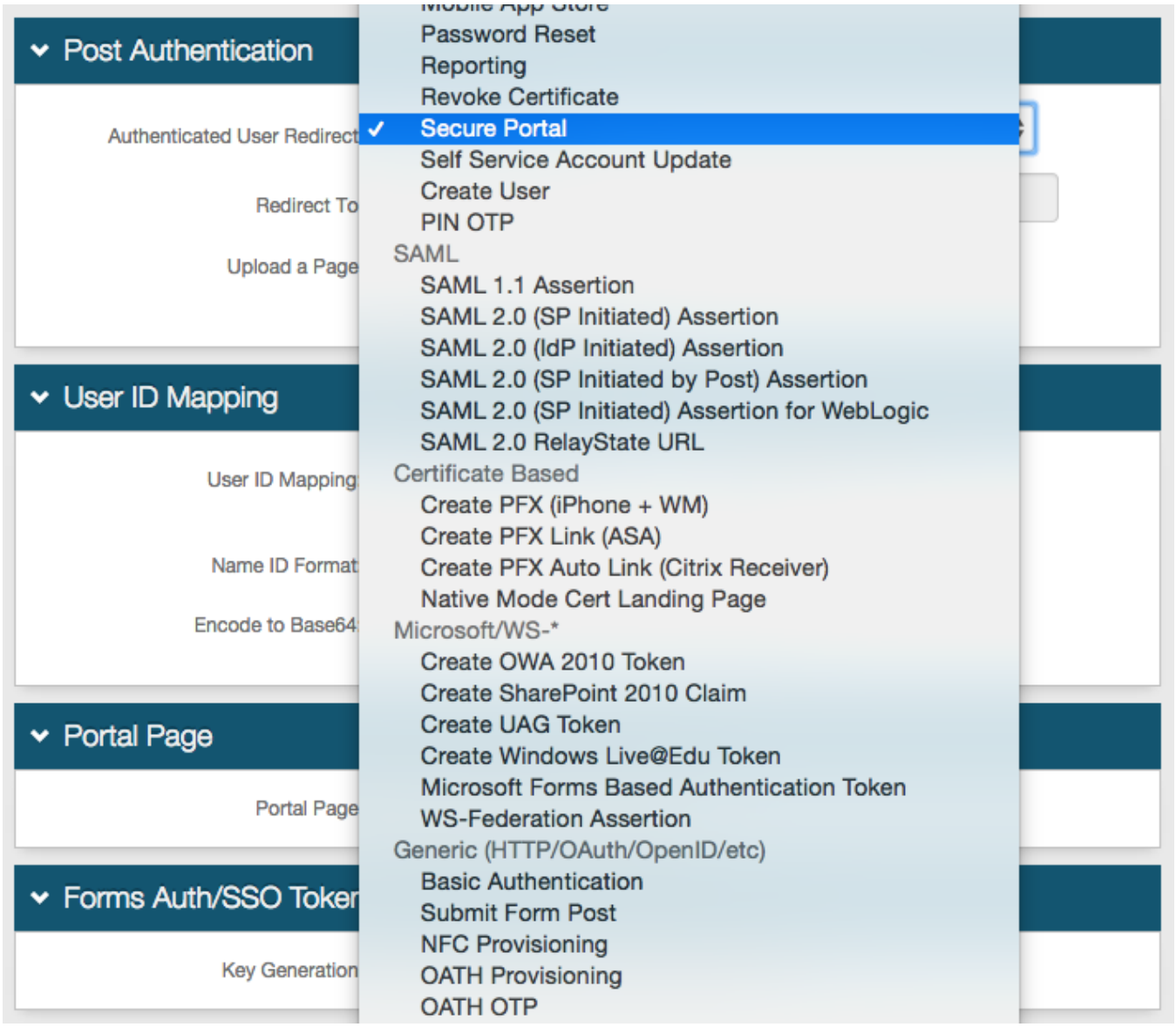
SecureAuth IdP Web Admin - Classic Experience

Post Authentication tab

The Post Authentication tab can be configured in a number of ways, based on the selection made from the Authenticated User Redirect dropdown which dictates the type of content to appear on this tab.

Refer to these guides for the type of post authentication configuration:

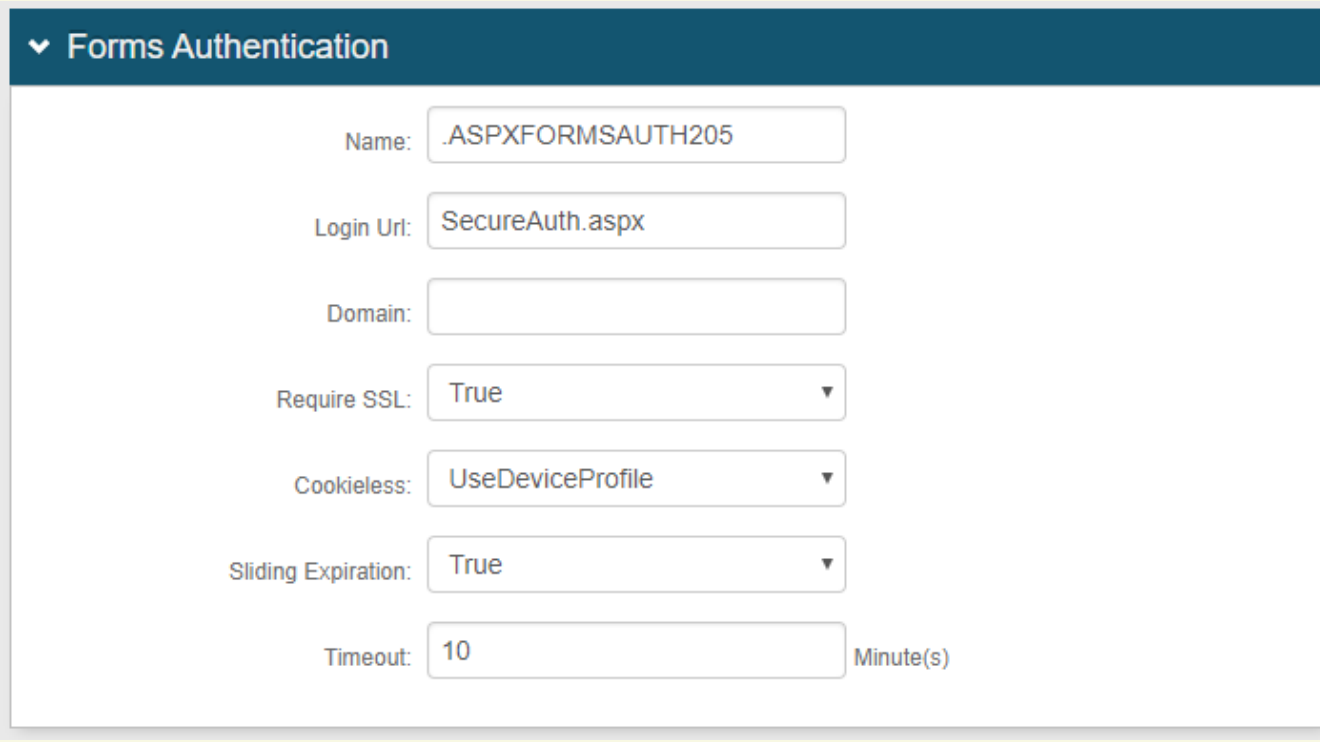
- SecureAuth IdP Out-of-the-box Identity Management Tools for IdM and user self-service configurations, such as Password Reset, Account Update, Reporting, Account Reset, and Forgot Username.
- Third-Party Integration & Configuration Guides for:
  - SaaS and web integration configurations – see also Application Integration Guides (versions 9.1+).
  - VPN and device integration configurations that use SAML, WS-Fed / Trust, OpenID Connect, OAuth 2.0, X.509 certificates – see also VPN and Device Integration Guides (versions 9.1+).
  - Mobile-specific configurations – see also Mobile (versions 9.1+).



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

Post Authentication tab

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



Workflow tab

Session Timeout is configured in the Workflow section on the Workflow tab.