New and Classic Experience Web Admin configuration in SecureAuth IdP v9.3

Introduction

The New Experience Web Admin introduced in SecureAuth IdP version 9.3 lets you configure Active Directory and SQL Server data stores, and then associate these data stores with integrated applications created on the user interface. The newly-architected SecureAuth IdP was launched with minimal features to acquaint you with a new approach in configuring the robust and flexible product. Many tabs on the familiar Web Admin – now called the Classic Web Admin – must still be configured in order to complete the application in version 9.3.

The upcoming software release will provide more robust capabilities to complete your applications in the cloud or on your appliance solely using the New Experience Web Admin user interface.

New Experience Web Admin in v9.3

Supported configuration types

The New Experience user interface lets you configure, save, and edit these integration types:

Integrations	Where the configuration is made	Equivalent Classic Experience configuration
Active Directory data store integration	User Data Stores	Data tab: • Active Directory (sAMAccountName) • Active Directory (UPN)
SQL Server data store directory integration	User Data Stores	Data tab: • SQL Server
SAML Application integration	Application Manager	Post Authentication tab: • see Generic SAML Integration Guide
WS-Federation / WS-Trust application integration	Application Manager	Post Authentication tab: • see Office 365 Integration Guide

Data Store configurations are used by applications created on the New Experience user interface.

Applications are set to use the default Workflow, Multi-Factor Method, and Adaptive Authentication configuration. Go to tabs on the Classic Experience user interface to modify any of these components.

Classic Experience Web Admin in v9.3

Configuration types not yet supported in the New Experience

Use the Classic Experience user interface to configure, save, and edit the following criteria:

- Data Store types outside of Active Directory and SQL Server
- Post Authentication page types outside of SAML application integrations
- Pages for other supported SecureAuth IdP features and functionalities

SecureAuth IdP version 9.3 pages you create with any of these components must be built in the Classic Experience:

Data Store

- Lightweight Directory Services (AD-LDS)

- Lotus Domino
- Novell eDirectory
- Sun ONE
- Tivoli Directory
- Open LDAP
- Other LDAP
- ODBC
- ASPNETDB
- Web Service (Multi-Data Store)
- Microsoft Azure AD
- Oracle
- Custom – directory types not included in the Datastore Type dropdown

Workflow

The Workflow defines how the end-user accesses the configured page / resource.

Device recognition methods

- Tokens
- Certificates

User login options

- 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.

Identity / authentication consumption options

Define any of configuration requirements, if necessary:

- Begin site
  - Basic Authentication
  - Certificate Finder (V1 and V2)
  - Client Side SSL
  - Fingerprint Finder
  - Form Post
  - Multi-Workflow
  - Native Certificate Finder
  - Windows SSO

        - Windows SSO (skip workflow)
        - Cisco ISE
        - YubiKey
        - Custom
- Open ID
- SAML consumer
- Form Post
- Social Identity
- FBA WebService

Adaptive Authentication

The Adaptive Authentication configuration determines how an end-user's login attempt will be handled, based on defined rules:

- User risk
- IP / Country restriction
- SecureAuth Threat Service
- User / Group restriction
- Geo-velocity

Multi-Factor Methods

Configured Multi-Factor Methods define which two-factor methods end-users can select and use to authenticate themselves:

- Phone
- Email
- Knowledge base
- Help desk
- PIN
- Timed passcodes (OATH)
- Mobile login requests (Push Notifications)
- YubiKey
- Symantec VIP

Post Authentication

Post Authentication defines the target resource of the application. Except for SAML and WS-Federation Assertion integrations – which are configured on the New Experience – settings must be made on this tab in the Classic Experience for these types of pages:

Custom

- Use Custom Redirect

Identity Management (IdM)

- Account Management
- Forgot Username
- Mobile App Store
- Password Reset
- Reporting
- Revoke Certificate
- Secure Portal
- Self Service
- Create User
- PIN OTP

Certificate Based

Microsoft/WS-*

Generic (HTTP/OAuth/OpenID/etc)

- Basic Authentication
- Submit Form Post
- Multi-Factor App Enrollment - URL
- Multi-Factor App Enrollment - QR Code
- OATH OTP
- OpenID Connect / OAuth 2.0
- User Handler Web Service

3rd Party App Integrations

- F5 BigIP
- PDP Configuration
- Siteminder Session Token

- WebSphere via Post
- YubiKey Provisioning

Mobile

- Native Mobile App
- Android Transition
- iOS Google Apps Provision
- iOS Exchange Provision

Related topic

New Experience and Classic Experience Web Admin