Self-service Account Update page configuration

Use this guide to configure the Self-service Account Update page, which enables end-users to modify and update their own profiles.

Once end-users securely log into the tool, they can enter new information (mobile number, personal email address); update existing information (new home address, last name change); and update Multi-Factor Authentication information, including setting PIN numbers, selecting Knowledge-based Questions, resetting Device Recognition information, and revoking devices / browsers provisioned for Time-based Passcode generation.

Depending on the configured directory permissions, all of the changes made on the Self-service Account Update page are written to and updated in the corporate data store. This significantly reduces directory management time and costs.

Prerequisites

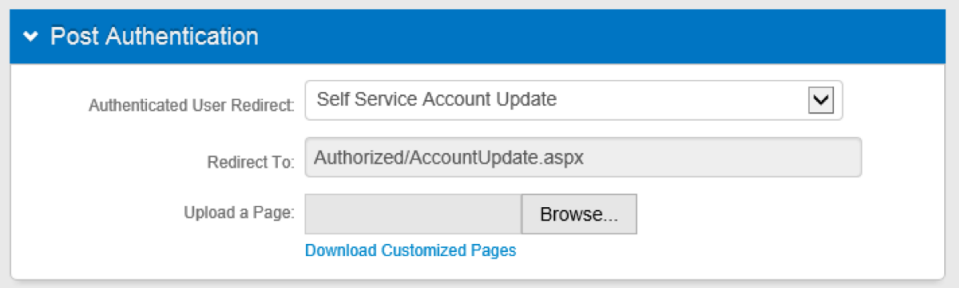
- The SecureAuth IdP directory Service Account must have the write privileges in order to change/add user information
- SecureAuth IDP **new realm** for the Self-service Account Update page with the following tabs configured ***before*** you configure the **Post Authentication** tab:
  - **Overview** – the description of the realm and SMTP connections must be defined
  - **Data** – an enterprise directory must be integrated with SecureAuth IdP
  - **Workflow** – the way in which users will access this application must be defined
  - **Registration Methods** – the 2-Factor Authentication methods that will be used to access this page (if any) must be defined

---

SecureAuth IdP configuration

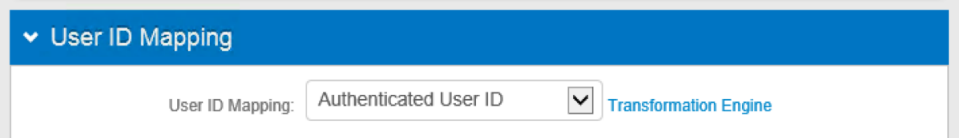
1. Go to the **Post Authentication** tab.
2. In the **Post Authentication** section set the following:

Authenticated User Redirect	Set to **Self Service Account Update**.
Redirect To	This field is auto-populated with an URL, which appends to the domain name and realm number in the address bar. For example, Authorized/AccountUpdate.aspx.
Upload a Page	Optionally, you can upload a customized post authentication page.



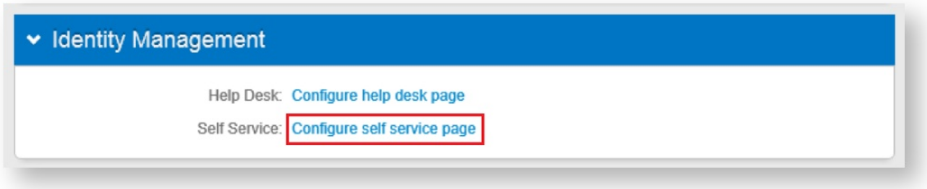
3. In the User ID Mapping section, set the following:

User ID Mapping	Set to the type of User ID that will be asserted to the Self-Service Account Update page. For example, Authenticated User ID.

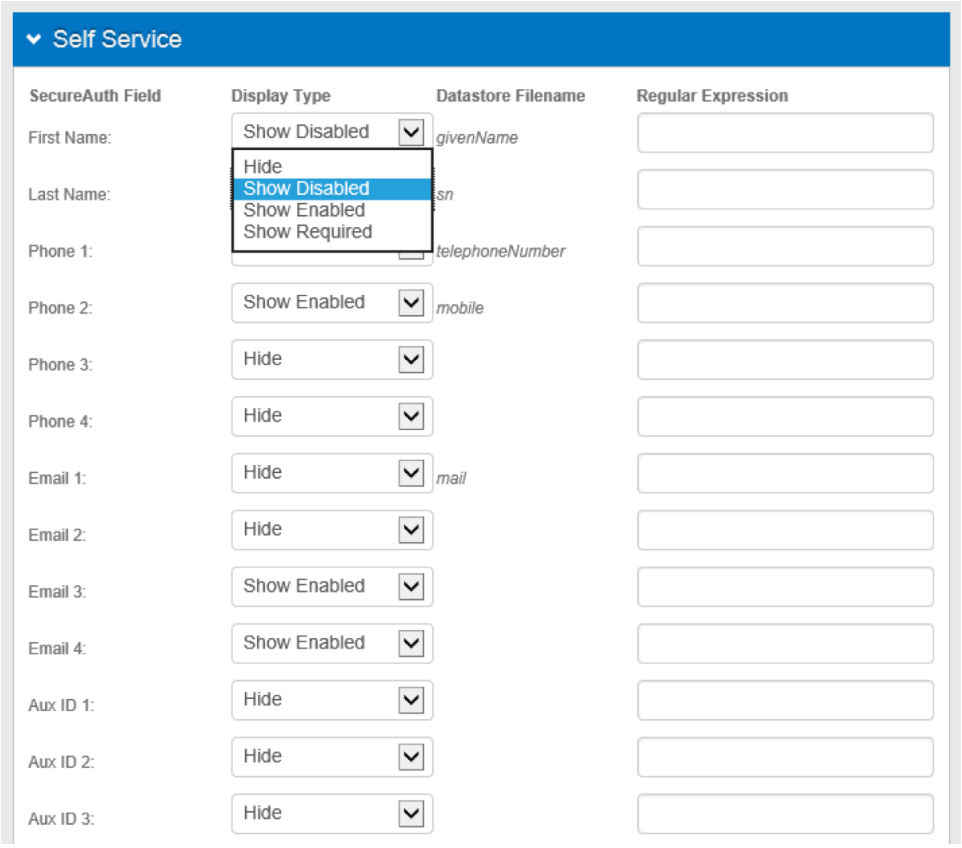


4. **Save** your changes.

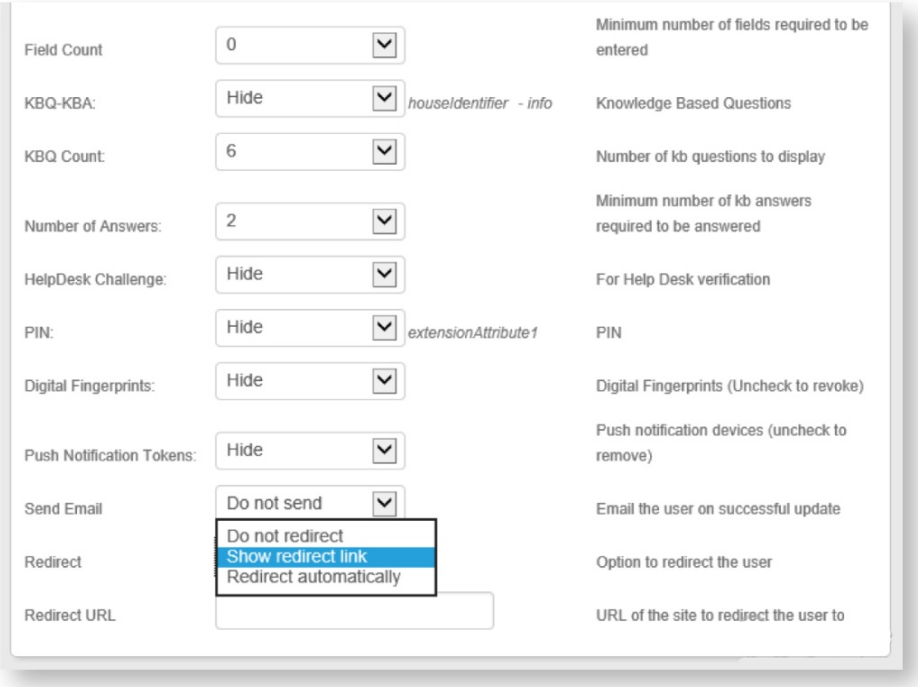
5. In the **Identity Management** section, click the **Configure self service page** link and set the following:



SecureAuth Field	For each SecureAuth field, indicate how the field is to display on the Self-service Account Update page. Choose from the following options: • **Hide** – Do not show the field on the self-service page • **Show Disabled** – Show the field as disabled on the self-service page • **Show Enabled** – Show and allow the user to edit information for this field • **Show Required** – Show and require the user to edit information for this field
Regular Expression	For more information about limiting the type of information that can be submitted on the self-service page, see the Restrict allowed information in employee Self Service page knowledge base article.



Send Email	Indicate whether to send an email when a change is made.
Redirect	Indicate whether to redirect the user after changes are successfully completed. If you choose **Show redirect link** or **Redirect automatically**, provide the URL in the **Redirect URL** field.



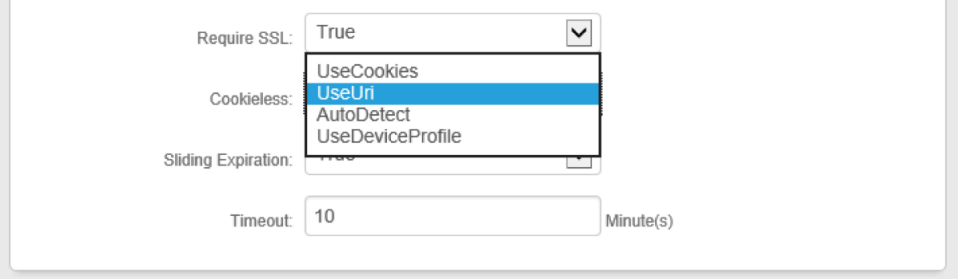
6. **Save** your changes.
7. Optionally, in the **Forms Auth / SSO Token** section, click the **View and Configure FormsAuth keys/SSO token** link to configure the token /cookie settings and configure this realm for SSO.

To configure token/cookie settings for this realm, expand this panel and do the following...

a. In the **Forms Authentication** section, set the following:

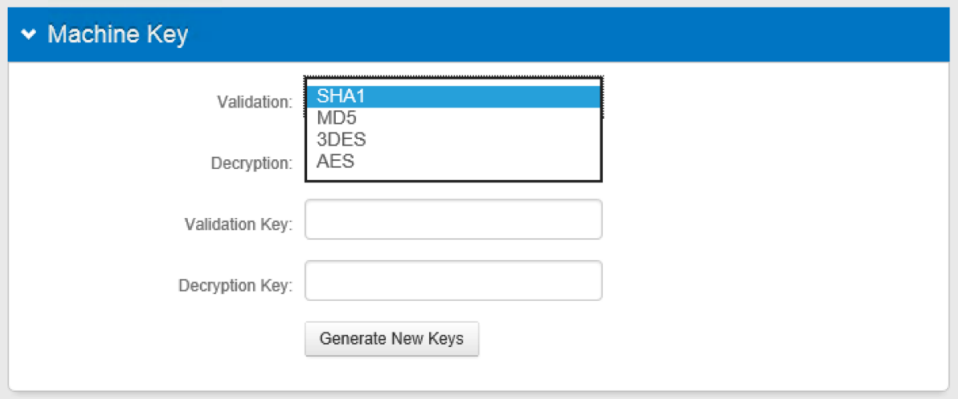
Require SSL	If the SSL is required to view the token, set to **True**.
Cookieless	Indicate whether SecureAuth IdP will deliver the token in a cookie to the user's browser or device: • **UseCookies** – Always deliver a cookie • **UseUri** – Do not deliver a cookie, deliver the token in a query string • **AutoDetect** – Deliver a cookie if the user's settings allow it. • **UseDeviceProfile** – Deliver a cookie if the browser settings allow it, regardless of the user's settings
Sliding	For the cookie to remain valid as long as the user is interacting with the page, set to **True**.

Expiration	
Timeout	Set the length of time in minutes the cookie is valid.



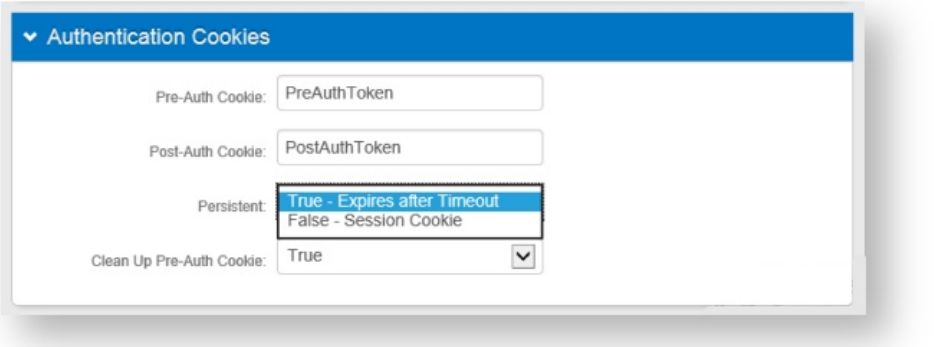
b. In the **Machine Key** section, set the following:

Validation	If the default value does not match your organization's requirements, choose another value.
Decryption	If the default value does not match your organization's requirements, choose another value.



c. In the **Authentication Cookies** section, set the following:

Persistent	Set one of the following values: • **True - Expires after Timeout** – Allow the cookie to be persistent • **False - Session Cookie** – Allow the cookie to be valid as long as the session is open, and expires when the browser is closed or the session expires



d. **Save** your changes.

To configure this realm for **SSO**, see SecureAuth IdP Single Sign-on Configuration.

To configure this realm for **Windows Desktop SSO**, see Windows desktop SSO configuration.