Create User Page Configuration Guide

Introduction

The Create User function is for administrators to establish new users in the enterprise directory and the SecureAuth IdP environment.

Prerequisites

1. Create a **New Realm** for the Create User function

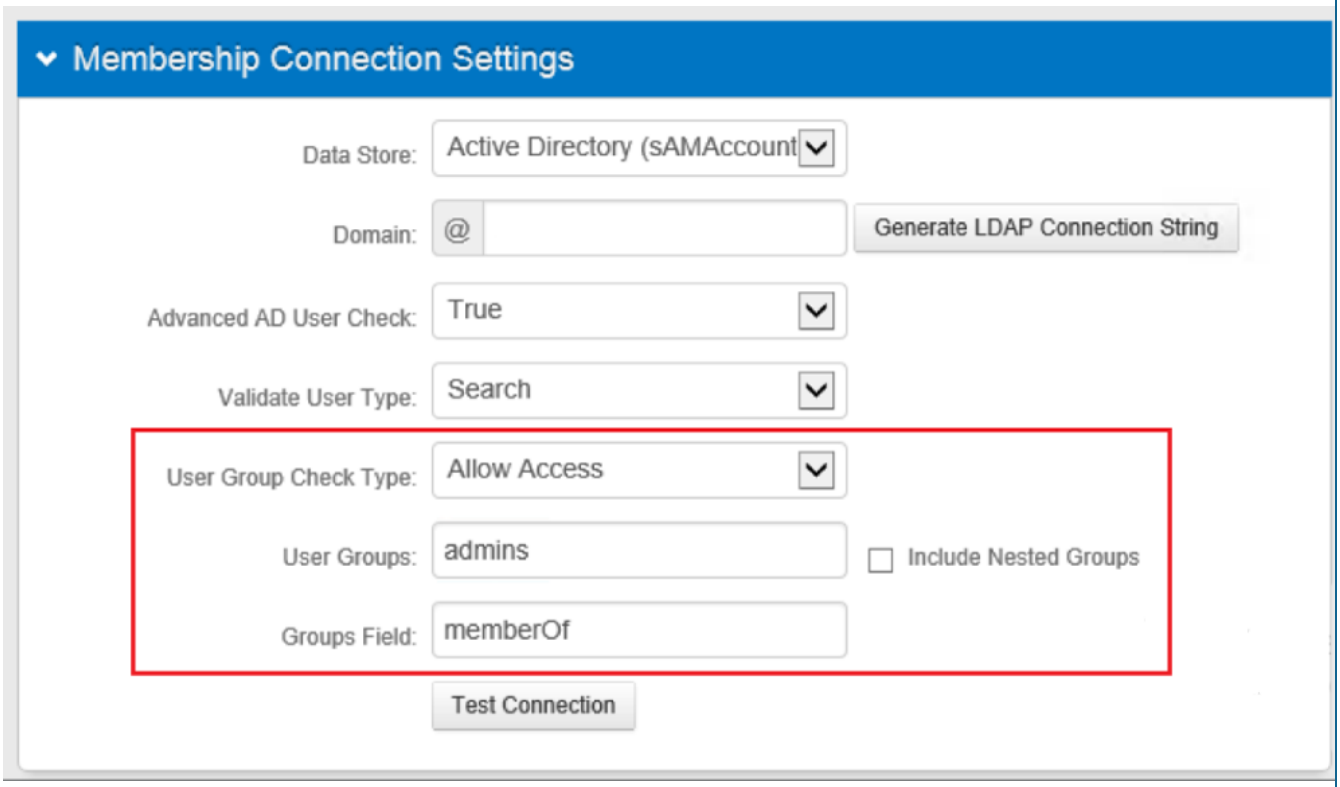
2. The SecureAuth IdP directory Service Account must have the write privileges to **add** users

3. Configure the following tabs in the Web Admin before configuring 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

Configuration Steps

Data

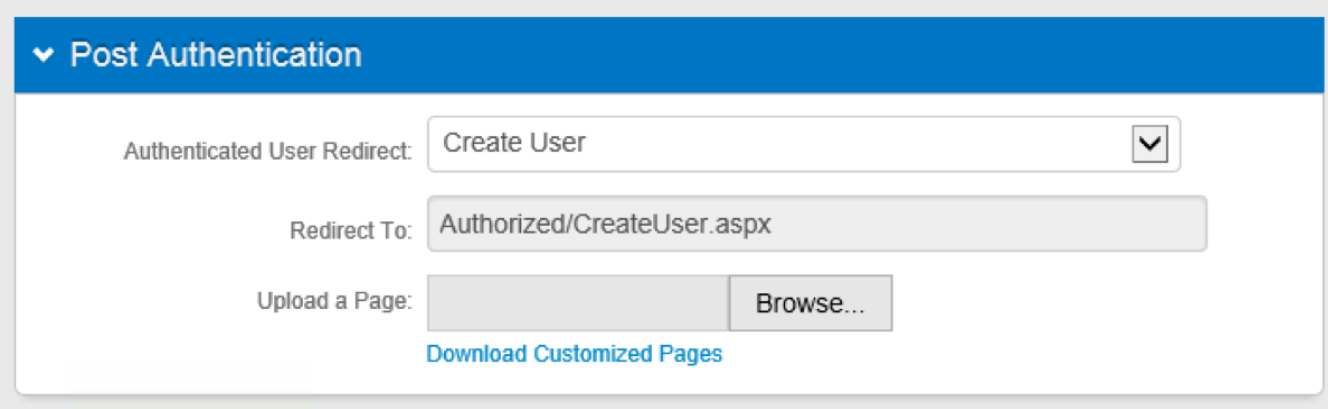


1. Restrict the realm to only admins in the **Membership Connection Settings** section by selecting **Allow Access** from the **User Group Check Type** dropdown, provide the **User Groups** name(s) (e.g. "admins"), and the **Groups Field** in the enterprise directory that contains group information of each user

    This is not required, as a company may wish to have users create their own accounts

Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

Post Authentication

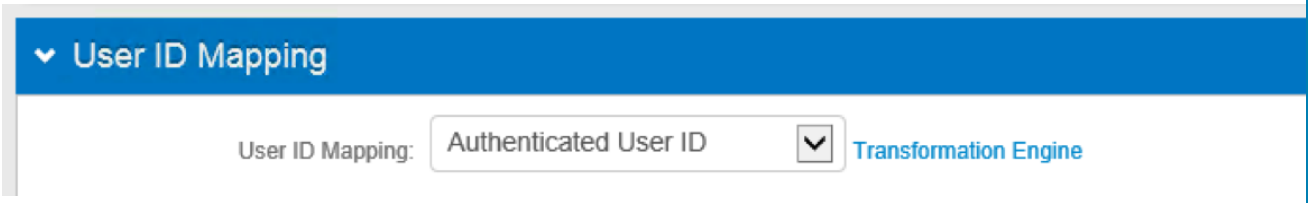


2. Select **Create User** from the **Authenticated User Redirect** dropdown in the **Post Authentication** tab in the Web Admin

3. An unalterable URL will be auto-populated in the **Redirect To** field, which will append to the domain name and realm number in the address bar (Authorized/CreateUser.aspx)

4. A customized post authentication page can be uploaded, but it is not required

User ID Mapping

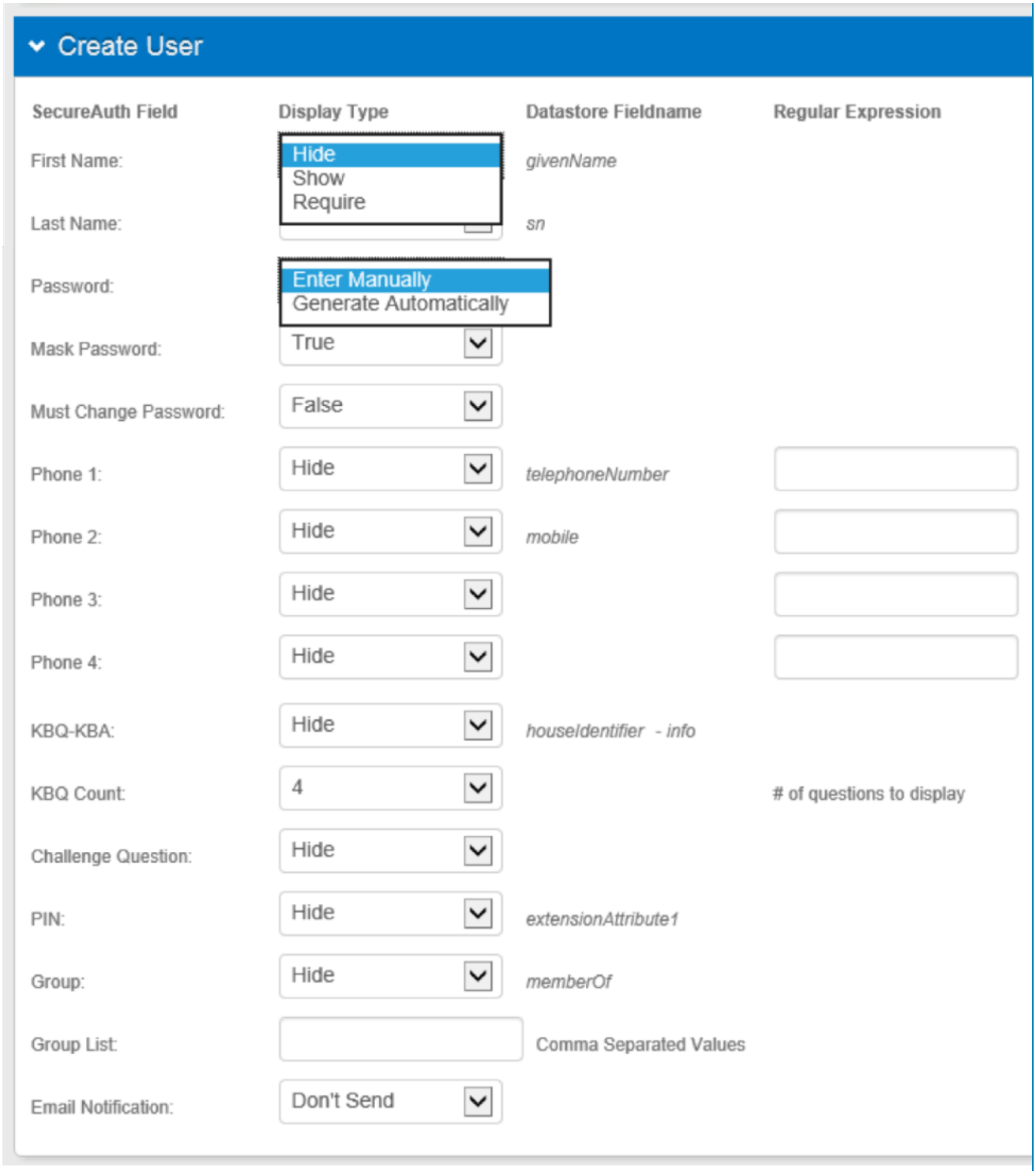


5. Select the type of User ID that will be asserted to the Create User function from the **User ID Mapping** dropdown

   This is typically the **Authenticated User ID**

> No configuration is required for the **Name ID Format** and **Encode to Base64** fields

Create User


Create User
SecureAuth Field
Display Type
Datastore Fieldname
Regular Expression
First Name:
Hide
Show
Require
givenName
Last Name:
sn
Password:
Enter Manually
Generate Automatically
Mask Password:
True
Must Change Password:
False
Phone 1:
Hide
telephoneNumber
Phone 2:
Hide
mobile
Phone 3:
Hide
Phone 4:
Hide
KBQ-KBA:
Hide
houseIdentifier - info
KBQ Count:
4
# of questions to display
Challenge Question:
Hide
PIN:
Hide
extensionAttribute1
Group:
Hide
memberOf
Group List:
Comma Separated Values
Email Notification:
Don't Send

6. Select **Hide**, **Show**, or **Required** for each **SecureAuth Field** (corresponding to the **Profile Properties** in the **Data** tab) to elect what will appear and what can be modified on the Create User page

Hide will not show the **SecureAuth Field** on the page

Show will show the **SecureAuth Field** on the page, and the administrator can edit the information

Required will show the **SecureAuth Field** on the page, and the administrator *must* edit the information

7. Select **Enter Manually** to create a specific password or **Generate Automatically** to create a random password from the **Password** field

8. Choose whether to **Mask Password** and whether the user **Must Change Password** after the account is created

9. Select the **KBQ Count**

10. Provide the **Group List** to assign the new user into the appropriate groups, separated by commas

11. Choose whether to send an **Email Notification** to the user when the account is created

Click **Save** once the configurations have been completed and before leaving the **Post Authentication** page to avoid losing changes

Forms Auth / SSO Token

12. Click **View and Configure FormsAuth keys / SSO token** to configure the token/cookie settings and to configure this realm for Single Sign-on (SSO)

These are *optional* configurations

Forms Authentication

1. If SSL is required to view the token, select **True** from the **Require SSL** dropdown

2. Choose whether SecureAuth IdP will deliver the token in a cookie to the user's browser or device:

   - **UseCookies** enables SecureAuth IdP to always deliver a cookie
   - **UseUri** disables SecureAuth IdP to deliver a cookie, and instead deliver the token in a query string
   - **AutoDetect** enables SecureAuth IdP to deliver a cookie if the user's settings allow it
   - **UseDeviceProfile** enables SecureAuth IdP to deliver a cookie if the browser's settings allow it, no matter the user's settings

3. Set the **Sliding Expiration** to **True** if the cookie remains valid as long as the user is interacting with the page

4. Set the **Timeout** length to determine for how many minutes a cookie is valid

> No configuration is required for the **Name**, **Login URL**, or **Domain** fields

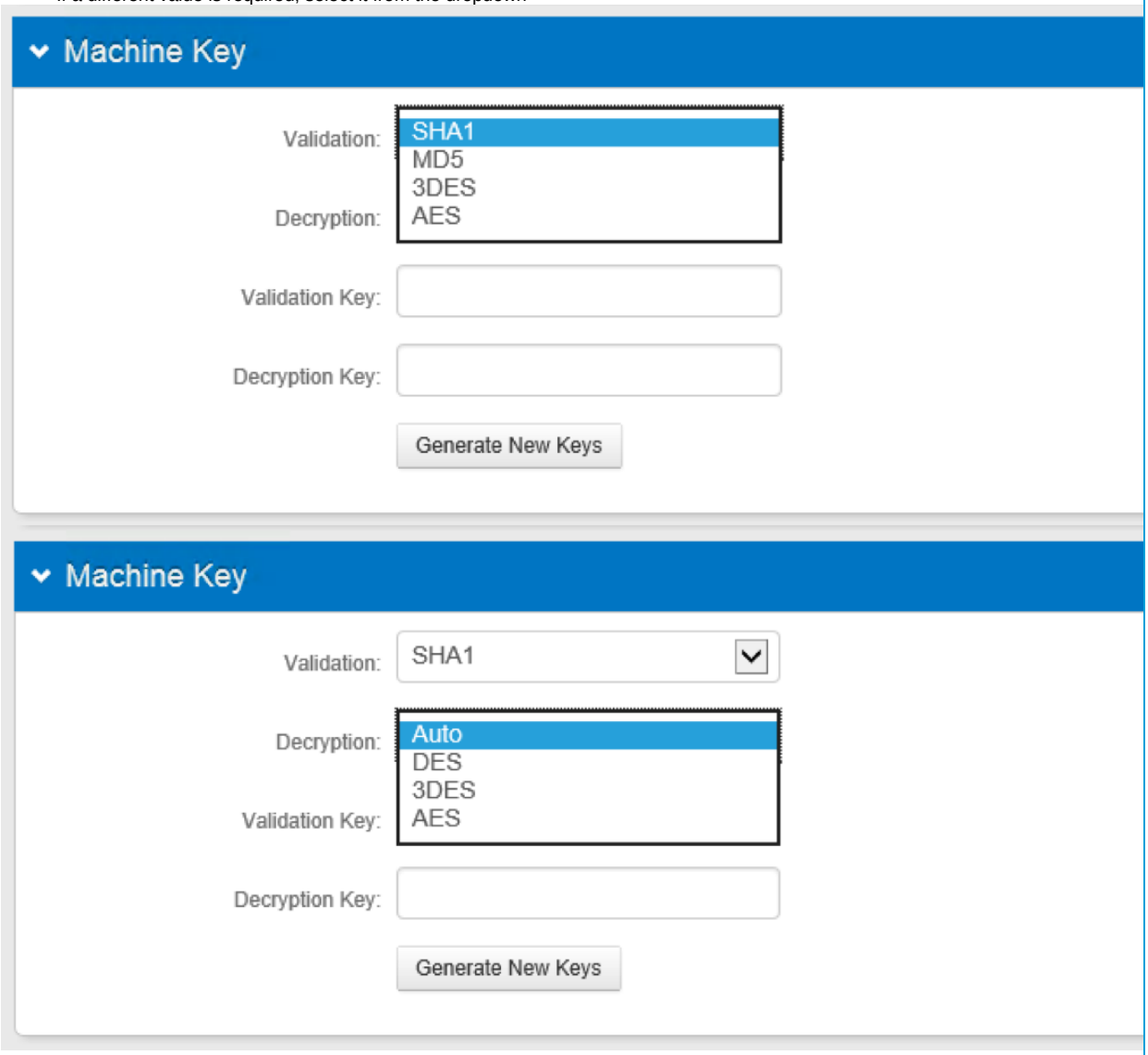
Machine Key

5. No changes are required in the **Validation** field, unless the default value does not match the company's requirement

    If a different value is required, select it from the dropdown

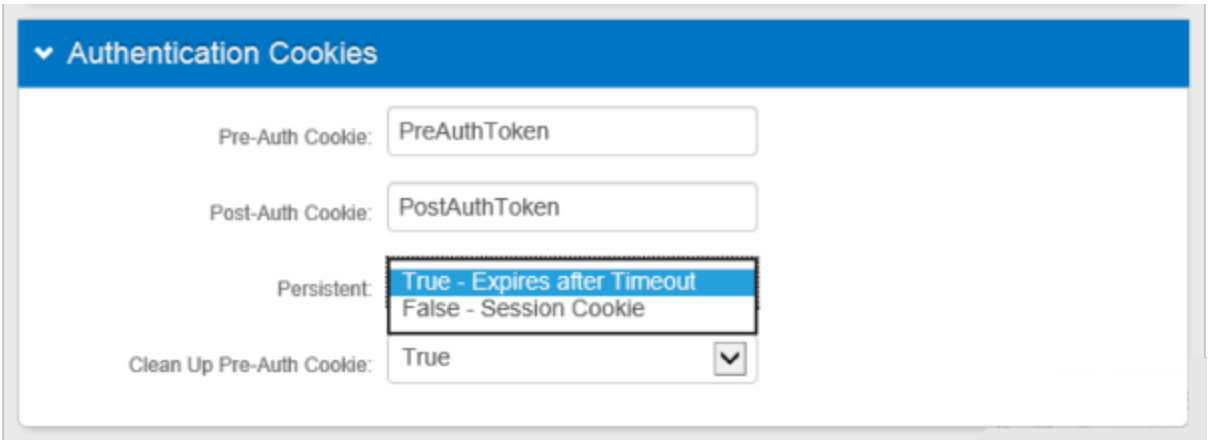
6. No changes are required in the **Decryption** field, unless the default value does not match the company's requirement

    If a different value is required, select it from the dropdown



No configuration is required for the **Validation Key** or **Decryption Key** fields

Authentication Cookies



7. Enable the cookie to be **Persistent** by selecting **True - Expires after Timeout** from the dropdown

   Selecting **False - Session Cookie** enables the cookie to be valid as long as the session is open, and will expire once the browser is closed or the session expires

> No configuration is required for the **Pre-Auth Cookie**, **Post-Auth Cookie**, or the **Clean Up Pre-Auth Cookie** fields

> Click **Save** once the configurations have been completed and before leaving the **Forms Auth / SSO Token** page to avoid losing changes

> To configure this realm for SSO, refer to **SecureAuth IdP Single Sign-on Configuration**

> To configure this realm for *Windows Desktop SSO*, refer to **Windows Desktop SSO Configuration Guide**