Account Management (Help Desk) Page Configuration Guide

Introduction

Use this guide to configure the Account Management (Help Desk) Page, which enables administrators and help desk teams to modify and update user profiles.

The Account Management page is equipped with various features to easily allow help desks to manage user accounts, including username search to retrieve accounts, password reset, account status options (lock / unlock / disable / enable), and user profile fields.

Once an account is displayed on the page, the help desk 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 Account Management page are written to and updated in the corporate data store. This significantly reduces directory management time and costs.

Prerequisites

1. Create a **New Realm** for the Account Management Page

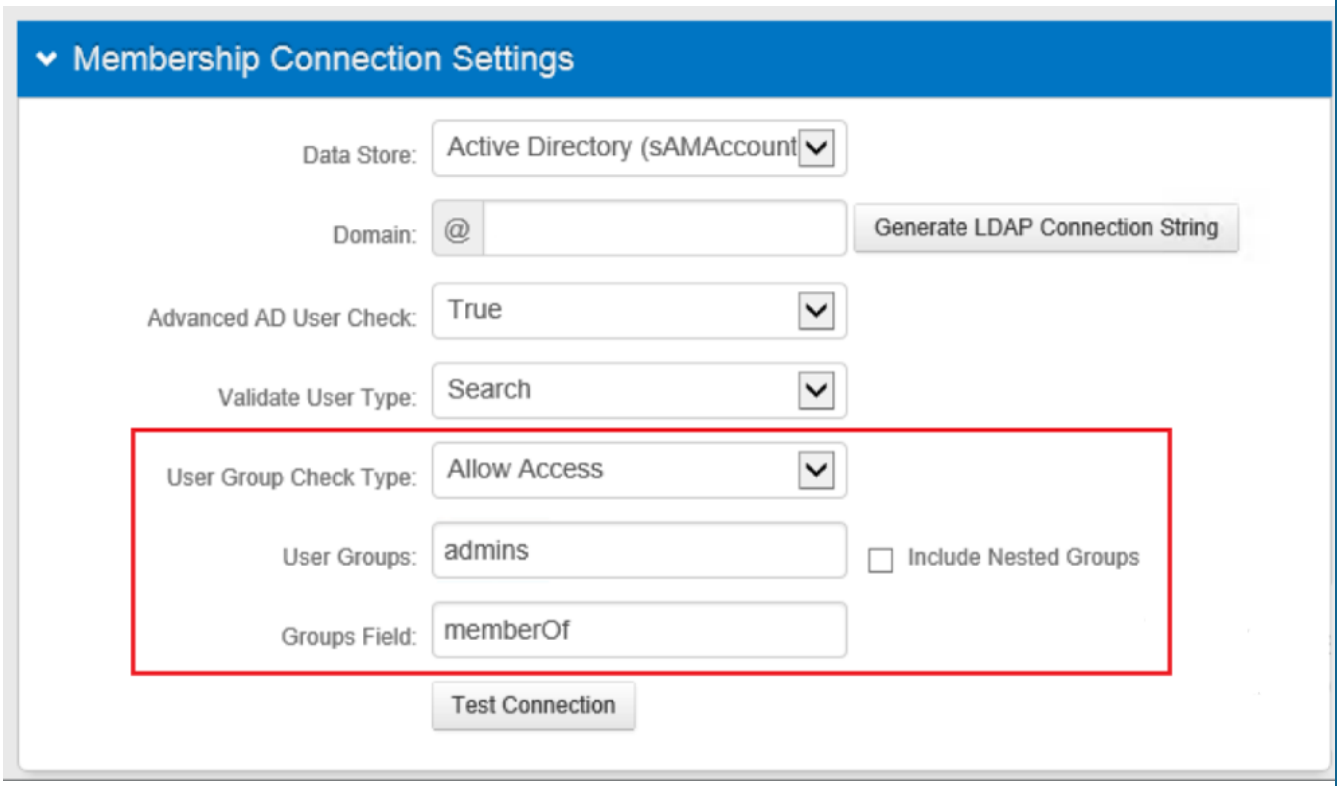
2. The SecureAuth IdP directory Service Account must have the write privileges in order to change/add user information

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

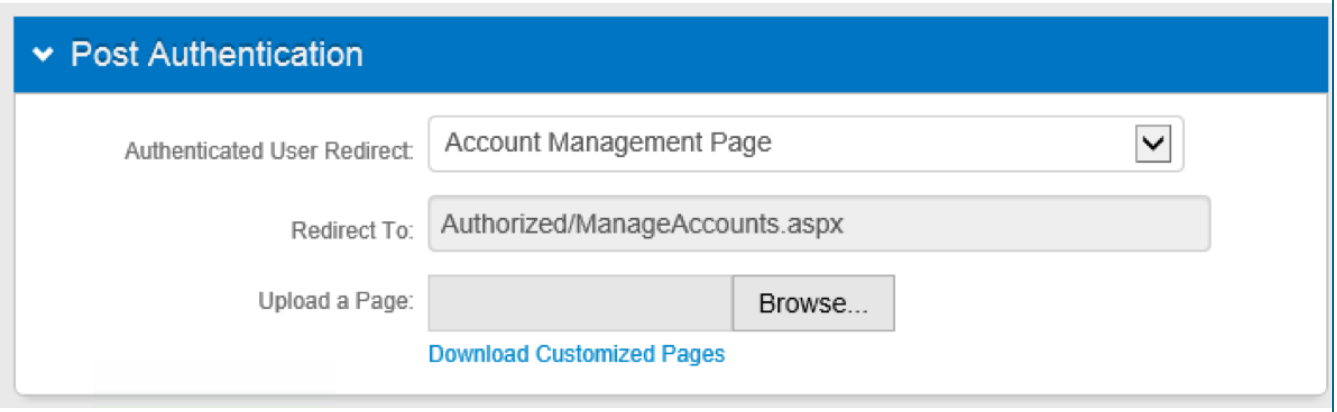
Data



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

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

Post Authentication

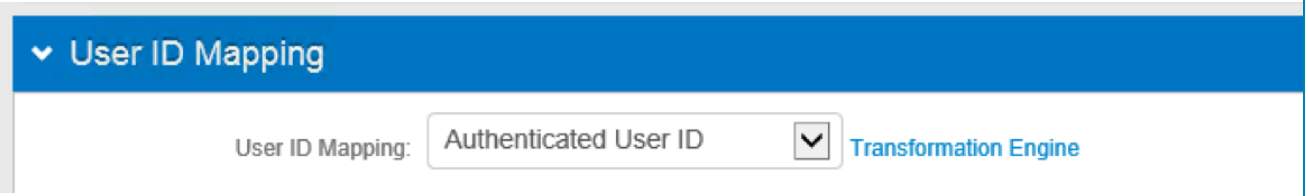


2. Select **Account Management Page** from the **Authenticated User Redirect** dropdown in the **Post Authentication** tab in the Web Admin

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/ManageAccounts.aspx)

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

User ID Mapping



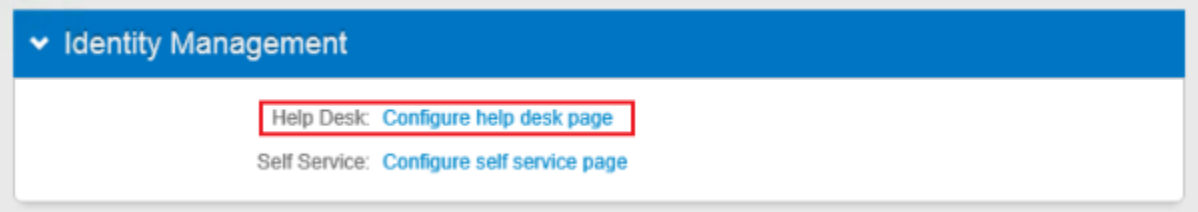
5. Select the type of User ID that will be asserted to the Account Management Page from the **User ID Mapping** dropdown

   This is typically the **Authenticated User ID**

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

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

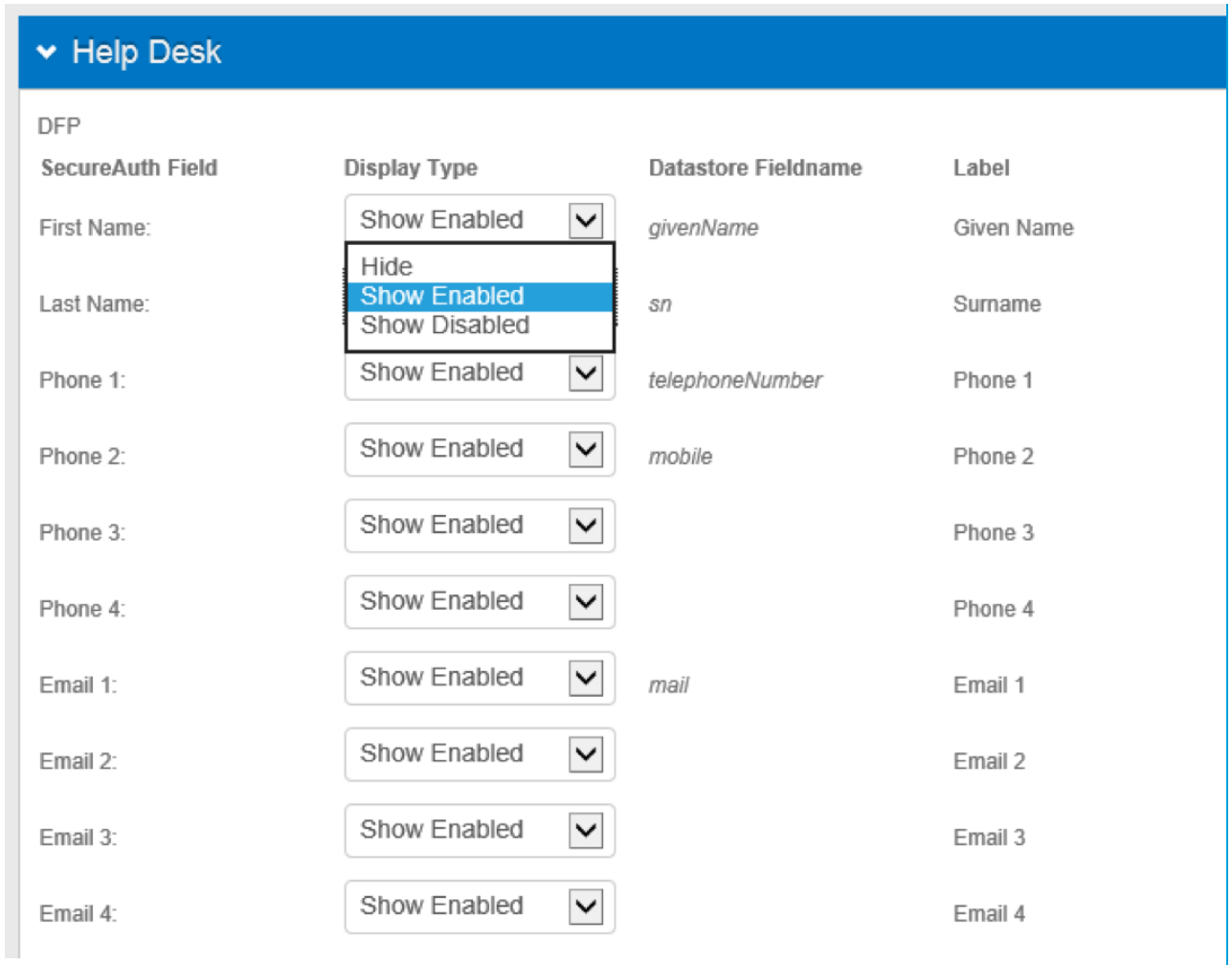
Identity Management



6. Click **Configure help desk page** in the **Identity Management** section

> No configuration is required for the **Self Service** page

Help Desk


Help Desk
DFP
SecureAuth Field
Display Type
Datastore Fieldname
Label
First Name:
Show Enabled
givenName
Given Name
Last Name:
Hide
Show Enabled
Show Disabled
sn
Surname
Phone 1:
Show Enabled
telephoneNumber
Phone 1
Phone 2:
Show Enabled
mobile
Phone 2
Phone 3:
Show Enabled
Phone 3
Phone 4:
Show Enabled
Phone 4
Email 1:
Show Enabled
mail
Email 1
Email 2:
Show Enabled
Email 2
Email 3:
Show Enabled
Email 3
Email 4:
Show Enabled
Email 4

Clear KBQ-KBA CheckBox:	Show	*houseIdentifier - info*	Clear the user's Knowledge Based Answers
Challenge Question:	Show		Challenge Question:
Cert Count Field:	Show Enabled		
Cert Rev Field:	Show Enabled		
Cert Rev Button:	Show		
Mobile Rev:	Hide		
PIN:	Hidden	*extensionAttribute1*	PIN
AuxID1:	Hide		AuxID1
AuxID2:	Hide		AuxID2
AuxID3:	Hide		AuxID3
AuxID4:	Hide		AuxID4
AuxID5:	Hide		AuxID5
AuxID6:	Hide		AuxID6
AuxID7:	Hide		AuxID7
AuxID8:	Hide		AuxID8
AuxID9:	Hide		AuxID9
AuxID10:	Hide		AuxID10
Digital Fingerprints:	Hide		Digital Fingerprints (uncheck to revoke)
Push Notifcation Devices:	Hide		Push notification devices (uncheck to remove)

7. Select **Hide**, **Show Enabled**, or **Show Disabled** 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 Account Management Page

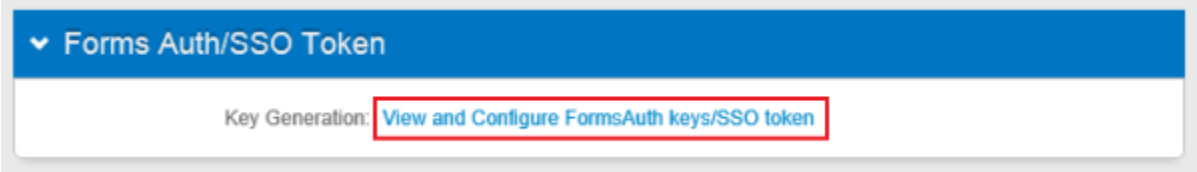
Hide will not show the **SecureAuth Field** on the page

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

Show Disabled will show the **SecureAuth Field** on the page, but the administrator *cannot* edit the information

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

Forms Auth / SSO Token



8. 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

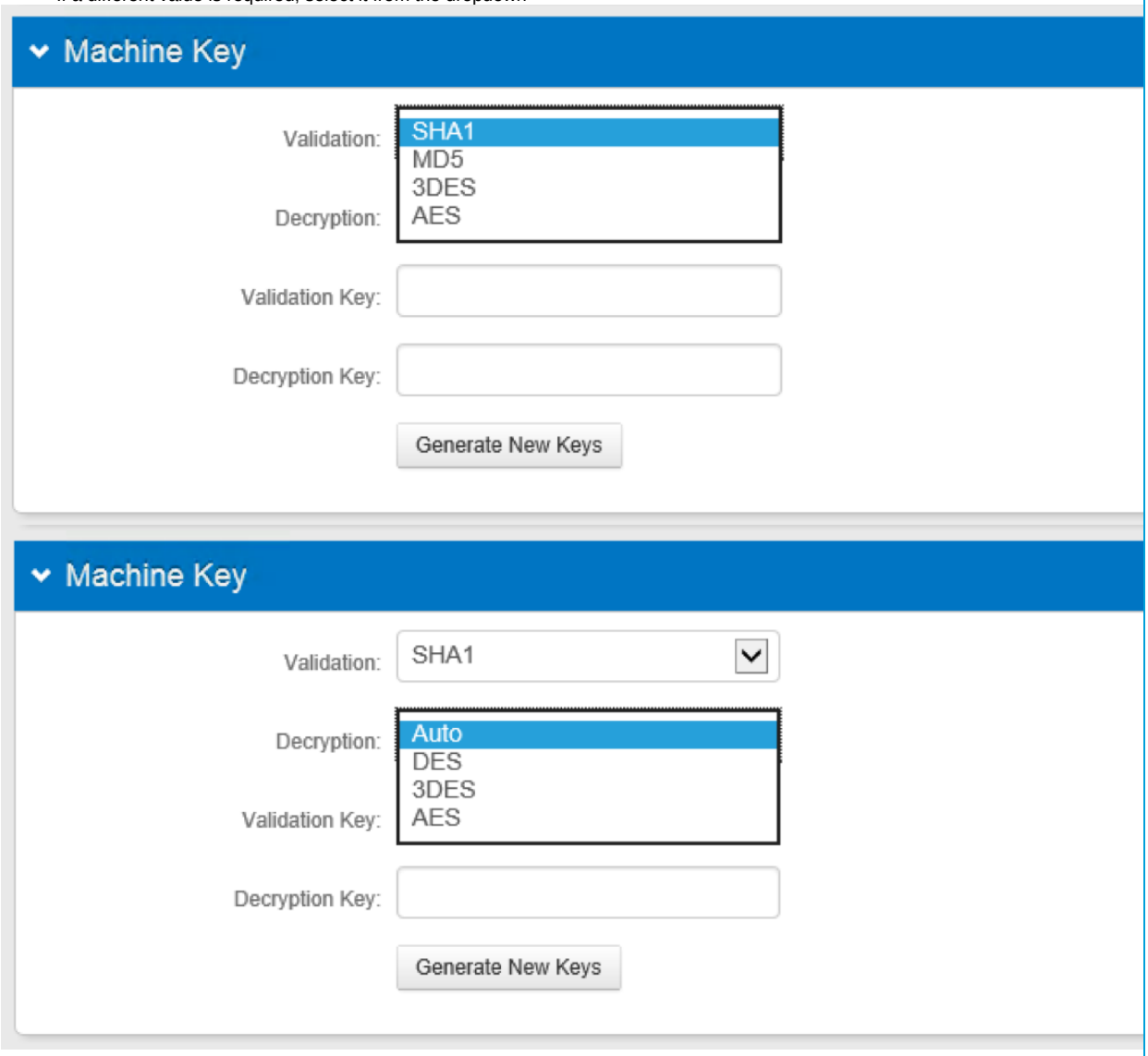
Machine Key

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

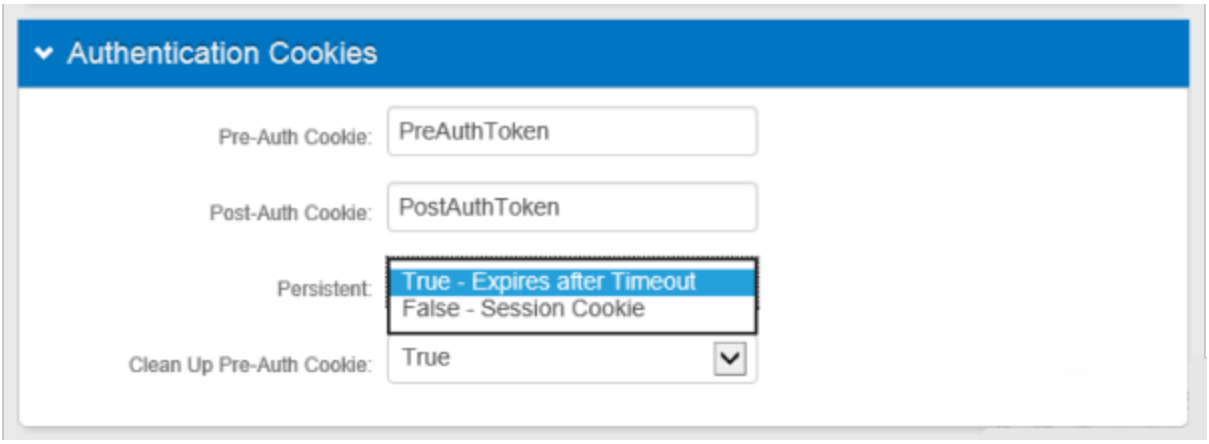
6. No changes are required in the **Decryption** field, unless the default value does not match the company's requirement

    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**