

Secure Portal Configuration Guide

Introduction

Use this guide to configure the Secure Portal for end-user Single Sign-on (SSO).

The Secure Portal provides a centralized page for end-users to access applications and resources that are available for them to access. This includes SecureAuth's built-in Identity Management (IdM) features as well as cloud and internal web applications and VPNs. Multiple realms can be associated with the Secure Portal page, enabling users to easily navigate between them via SSO. In addition, icons can be uploaded to customize the page's appearance.

Prerequisites

1. Create a **New Realm** for the Secure Portal page
2. Configure the realms to which the Secure Portal page connects for access
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

Post Authentication

▼ Post Authentication

Authenticated User Redirect: Secure Portal

Redirect To: SecurePortal.aspx

Upload a Page: Browse...

[Download Customized Pages](#)

1. Select **Secure Portal** from the **Authenticated User Redirect** dropdown in the **Post Authentication** tab in the Web Admin
2. An unalterable URL is auto-populated in the **Redirect To** field, which appends to the domain name and realm number in the address bar (Authorized/SecurePortal.aspx)
3. A customized post authentication page can be uploaded, but it is not required



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

Portal Page

▼ Portal Page

Portal Page: [View and Configure the portal page](#)

4. Click **View and Configure the portal page** to dictate which realms are displayed on the Secure Portal

Portal Page Builder

▼ Portal Page Builder

Portal Page Authorization:

Links shown on portal page:

Not Available
Token Required
NO Token
GAE

SecureAuth1
 SecureAuth2
 SecureAuth3
 SecureAuth4
 SecureAuth5
 SecureAuth6
 SecureAuth7

5. Select **Token Required** from the **Portal Page Authorization** dropdown to require 2-Factor Authentication into the Secure Portal

Selecting **Not Available** disables the use of the Secure Portal

Selecting **NO Token** enables access to the Secure Portal without 2-Factor Authentication, but the realms associated with the Secure Portal require 2-Factor Authentication if the **Workflow** dictates it

Selecting **GAE** enables access with a token from a Google Apps Engine (GAE) SecureAuth instance

6. Check the SecureAuth IdP realms to which the Secure Portal enables SSO access in the **Links shown on portal page** section

Add images and titles in each of the realms that appear on the Secure Portal in the [Overview](#) instructions below; and restrict access by **Groups** in the [Data](#) instructions below



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

Forms Auth / SSO Token

Forms Auth/SSO Token

Key Generation: [View and Configure FormsAuth keys/SSO token](#)

7. Click **View and Configure FormsAuth keys / SSO token**

Forms Authentication

8. The Forms Based Authentication (FBA) token **Name** must be set and match in each realm for which SSO is enabled

By default, the **Name** is set to **.ASPXFORMSAUTH[realm#]**, but it can be changed to any name

If a realm has already been set up for SSO, then the **Name** from that realm is used here

9. The common **Domain** of the realms must be set and match in each realm for which SSO is enabled

By default, this field is left empty and SecureAuth IdP utilizes the appliance's domain

If a realm has already been set up for SSO, then the **Domain** from that realm is used here

Forms Authentication

Name:

Login Url:

Domain:

Forms Authentication

Name:

Login Url:

Domain:

The FBA Token **Require SSL**, **Cookieless**, and **Sliding Expiration** settings must match across the SSO realms; the **Timeout** values can be distinct

Machine Key

10. Set the **Validation Key** and the **Encryption Key** by clicking **Generate New Keys**

These fields *must match* in each realm for which SSO is enabled

If a realm has already been set up for SSO, then *do not* click **Generate New Keys**; the **Validation Key** and **Encryption Key** from that realm are used here

The image displays two screenshots of the 'Machine Key' configuration interface. Both screenshots show a blue header with a dropdown arrow and the text 'Machine Key'. Below the header, there are four fields: 'Validation:' with a dropdown menu set to 'SHA1', 'Decryption:' with a dropdown menu set to 'Auto', 'Validation Key:' with an empty text input field, and 'Decryption Key:' with an empty text input field. A 'Generate New Keys' button is located below the key input fields. In the top screenshot, a red rectangular box highlights the 'Validation Key' and 'Decryption Key' input fields. In the bottom screenshot, a red rectangular box highlights the 'Generate New Keys' button.

The **Validation** and **Decryption** settings must match across the SSO realms

Authentication Cookies

▼ Authentication Cookies

Pre-Auth Cookie:

Post-Auth Cookie:

11. The **Pre-Auth Cookie** and the **Post-Auth Cookie** must be set and match in each realm for which SSO is enabled

If a realm has already been set up for SSO, then the **Pre-Auth Cookie** and the **Post-Auth Cookie** from that realm are used here

The **Persistent** and **Clean Up Pre-Auth Cookie** settings must match across the SSO realms



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

Best Practices

These Best Practice configurations are completed in realms that are connected to the Secure Portal (selected in step 6), **not** in the Secure Portal realm

Application Logo Displayed on Secure Portal Page

Follow these configuration steps to modify the realm's information on the Secure Portal page, which includes application logo (image) and application title for immediate recognition

These optional steps are completed in the realms associated to the Secure Portal realm, NOT in the Secure Portal realm itself

Overview

Details

Realm Name

SecureAuth1

Realm Description

Company Logo

Browse...

Application Logo

Browse...

Look and Feel

Document Title

Application Title

Displayed in the browser's window title/tab.

Page Header

Application Title

Displayed at the top of the page.

1. In the **Details** section, upload the **Application Logo** in the **Details** section, which appears on the Secure Portal page
2. In the **Look and Feel** section, write in the **Application Title** in the **Document Title** and the **Page Header** fields (typically the same) in the **Look and Feel** section, which appear on the Secure Portal with the **Application Logo**



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

Group Restrictions

Follow these configuration steps to restrict the realm to specific groups, which then manages which resources are displayed to each user on the Secure Portal page

These optional steps are completed in the realms associated to the Secure Portal realm, NOT in the Secure Portal realm itself

Data

▼ Profile Connection Settings

Data Store:	Directory Server	▼
Directory Server:	Active Directory (sAMAccountName)	▼
Connection String:	<input type="text"/>	
Service Account:	<input type="text"/>	
Password:	●●●●●●●●	<input checked="" type="checkbox"/> Hidden
Connection Mode:	Secure	▼
Search Attribute:	samAccountName	<input type="button" value="Generate Search Filter"/>
Search Filter:	(&(samAccountName=%v)(objectclass=*))	
Allowed User Groups:	usergroup_1, usergroup_2	<input type="checkbox"/> Include Nested Groups
<input type="button" value="Test Connection"/>		

1. In the **Profile Connection Settings** section, set the **Allowed User Groups** to the group(s) that can access this application, comma separated

The example shown is for a Directory Server, but the step is the same for SQL-type data stores

Profile Fields

▼ Profile Fields				
Property	Source	Field	Data Format	Writable
Groups	Default Provider	memberOf		<input type="checkbox"/>
First Name	Default Provider	givenName		<input type="checkbox"/>
Last Name	Default Provider	sn		<input type="checkbox"/>

2. Map the **Groups** Property to the directory attribute that contains the user's group information, e.g. **memberOf**

This step is required for LDAP directories *only*

For SQL-type data stores, the information must be provided in the Tables and Stored Procedures



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