

Reporting Page Configuration Guide

Introduction

The Reporting page is for administrators to review and log authentication events.

Administrators can look up specific user's access, failed authentications, and successful authentications during any desired time period.

A Reporting realm would be created to require 2-Factor Authentication to access the Reporting page outside of the appliance (Reporting page is also accessible in the **Logs** tab).

The screenshot shows the 'SecureAuth Administration' reporting configuration page. It features several input fields and checkboxes for filtering authentication events. The 'Start Date' is set to 10/1/2014 and the 'End Date' is 12/4/2014. The 'Page Size' is set to 50. The 'User Id' field is empty. The 'Group By' section includes checkboxes for User ID, Company, Realm, Event ID, Appliance, and Machine Name. The 'Event ID (or * for all)' field is also empty. The 'Successful Auth' radio button is selected, with 'Failed Auth' as an alternative. There are checkboxes for 'Bad User ID', 'Bad User Password', and 'Bad OTP/KBA/PIN'. A 'Submit' button is located at the bottom center. At the bottom left, there is a 'Restart Login' link, and at the bottom right, there is a 'Powered by SECUREAUTH' logo.

Prerequisites

1. Create a **New Realm** for the Reporting page
2. 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

Membership Connection Settings

Data Store: Active Directory (sAMAccount) ▾

Domain: @

Advanced AD User Check: True ▾

Validate User Type: Search ▾

User Group Check Type: Allow Access ▾

User Groups: admins Include Nested Groups

Groups Field: memberOf

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

Post Authentication

Authenticated User Redirect: Reporting ▾

Redirect To: Authorized/Reporting.aspx

Upload a Page:

[Download Customized Pages](#)

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

3. 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/Reporting.aspx)

4. 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

Forms Auth / SSO Token

Forms Auth/SSO Token

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

5. 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

Require SSL:

Cookieless:

Sliding Expiration:

Timeout: Minute(s)

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

Machine Key

Validation: SHA1

MD5

3DES

Decryption: AES

Validation Key:

Decryption Key:

Generate New Keys

Machine Key

Validation: SHA1



Decryption: Auto

DES

3DES

Validation Key: AES

Decryption Key:

Generate New Keys



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

Authentication Cookies

▼ Authentication Cookies

Pre-Auth Cookie:

Post-Auth Cookie:

Persistent:

Clean Up Pre-Auth Cookie:

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

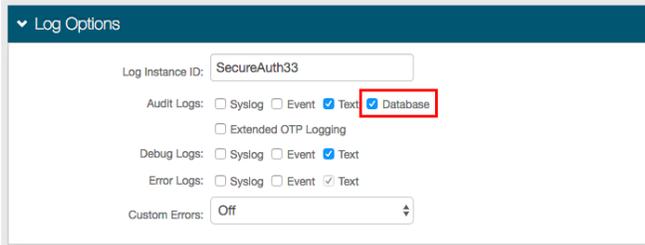
 Click **Save** once the configurations have been completed and before leaving the **Forms Auth / SSO Token** page to avoid losing changes

 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](#)

Logs

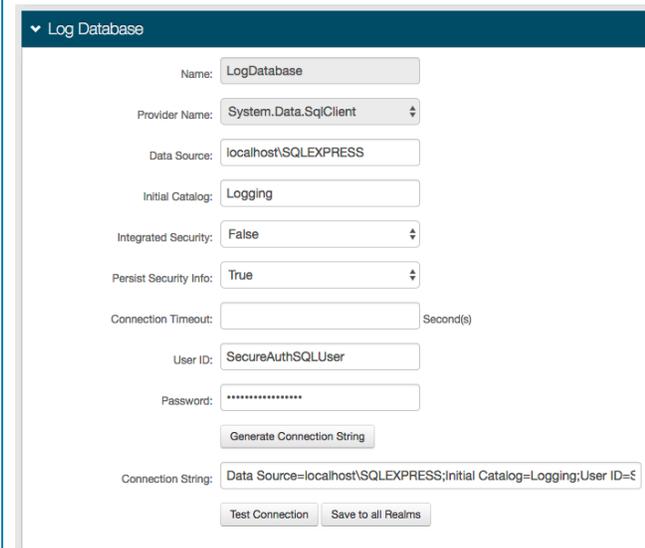
The following configuration steps are required in the Reporting page realm and all realms from which Reports pulls information



The screenshot shows the 'Log Options' configuration panel. It includes a dropdown for 'Log Instance ID' set to 'SecureAuth33'. Under 'Audit Logs', the 'Database' checkbox is checked and highlighted with a red box. Other options include 'Text', 'Event', and 'Syslog'. 'Debug Logs' and 'Error Logs' also have 'Text' checked. 'Custom Errors' is set to 'Off'.

6. In the **Log Options** section, check **Database** from the **Audit Logs** options

Log Database



The screenshot shows the 'Log Database' configuration panel. Fields include: 'Name' (LogDatabase), 'Provider Name' (System.Data.SqlClient), 'Data Source' (localhost\SQLEXPRESS), 'Initial Catalog' (Logging), 'Integrated Security' (False), 'Persist Security Info' (True), 'Connection Timeout' (empty), 'User ID' (SecureAuthSQLUser), and 'Password' (masked). A 'Generate Connection String' button is present, and the 'Connection String' field contains: 'Data Source=localhost\SQLEXPRESS;Initial Catalog=Logging;User ID=€'. 'Test Connection' and 'Save to all Realms' buttons are at the bottom.

7. Configure the **Log Database** section with a SQL-type database integration



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