Logs Tab Configuration

Introduction

Use this guide to configure the Logs tab in the Web Admin for each SecureAuth IdP realm.

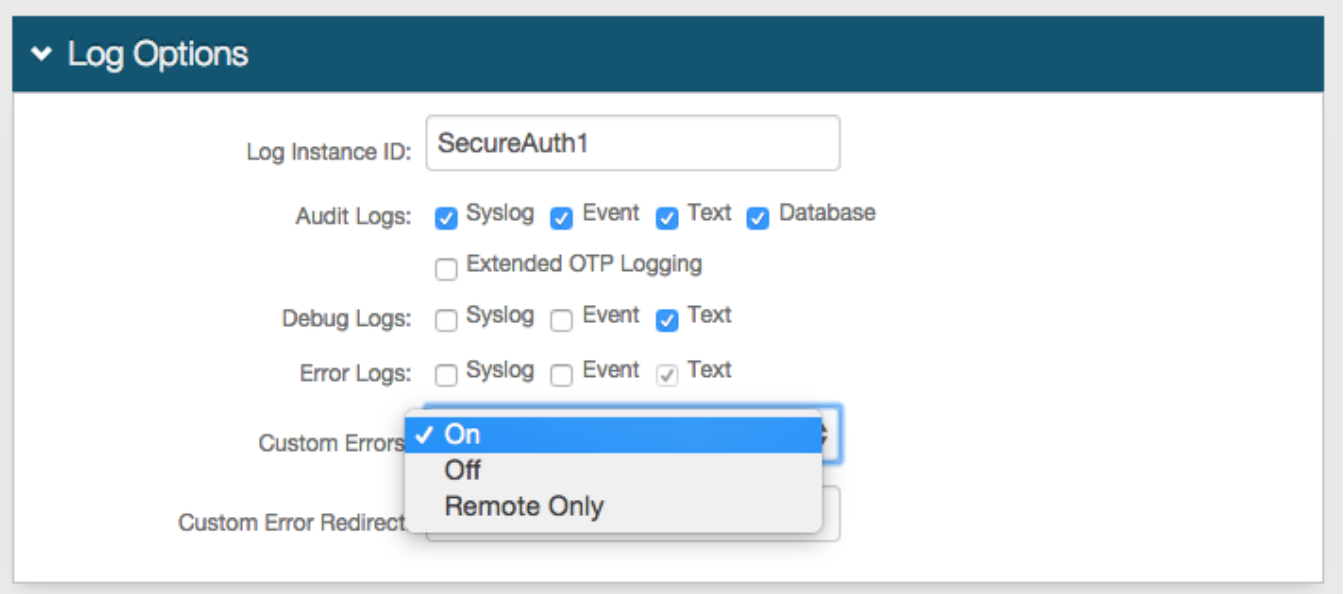
This includes enabling or disabling audit, error, and debug logs.

Prerequisites

1. Create a **New Realm** for the target resource for which the configuration settings will apply, or open an *existing realm* for which configurations have already been started

2. Configure the **Overview**, **Data**, **Workflow**, **Adaptive Authentication**, **Multi-Factor Methods**, and **Post Authentication** tabs in the Web Admin before configuring the **Logs** tab

Logs Configuration Steps



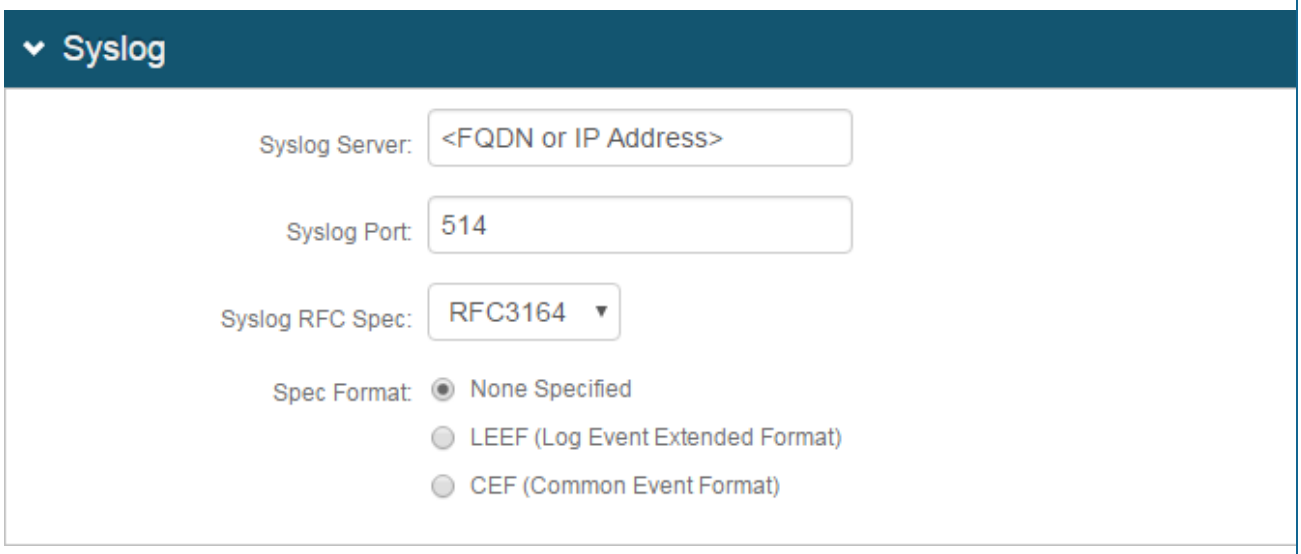
1. In the **Log Options** section, provide the **Log Instance ID**, e.g. the **Application Name** or the realm name (**SecureAuth1**)

2. Check which **Audit**, **Debug**, and **Error Logs** to enable

3. Select **On** or **Remote Only** from the **Custom Errors** dropdown to redirect end-users to a distinct page when a custom error occurs

4. Provide the URL for the **Custom Error Redirect** if **On** or **Remote Only** is selected in step 3

SysLog



1. Provide the **FQDN** or **IP Address** of the **Syslog Server**

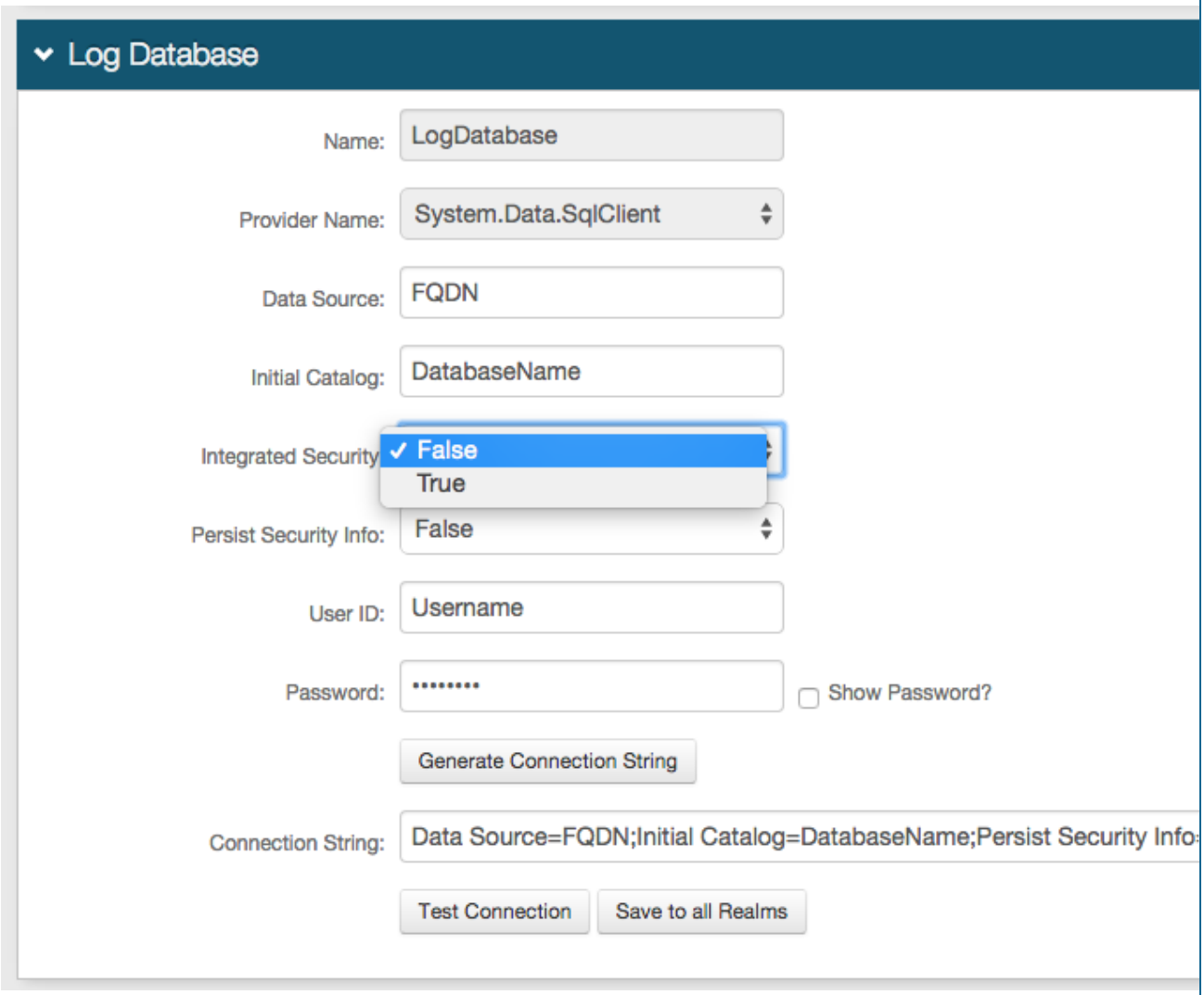
2. Provide the **SysLog Port** number

3. Select the **Syslog RFC Spec** from the dropdown as required by the Syslog

    If **RFC3164** is selected, then choose a **Spec Format**:

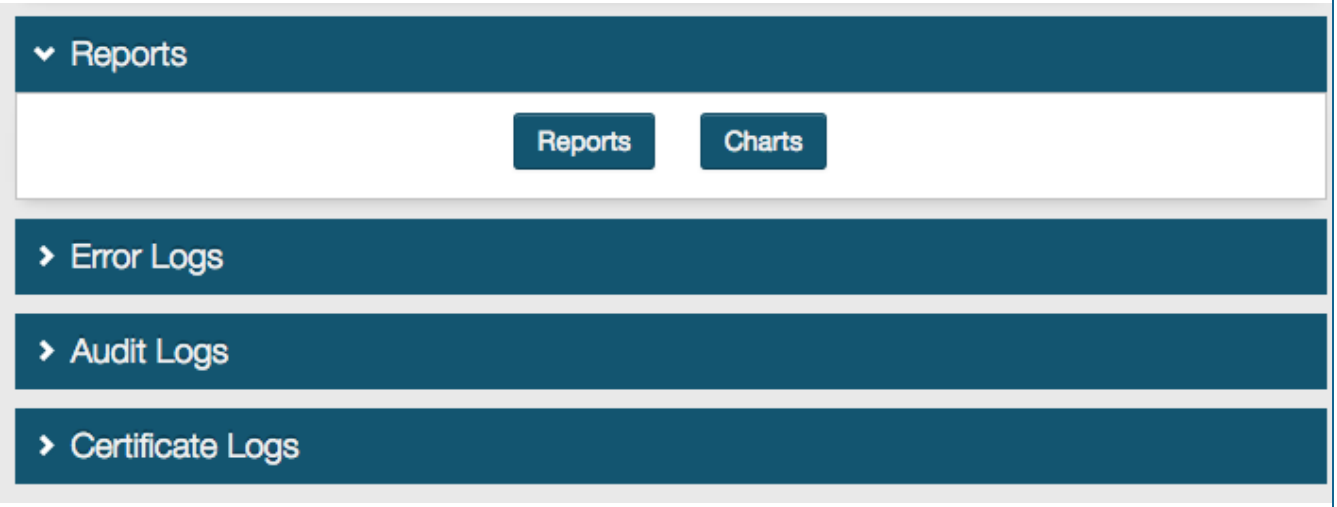
- **None Specified**: normal RFC3164 formatting, for use in most implementations
- **LEEF**: for use with IBM Security QRadar SIEM only
- **CEF**: for use with HP ArcSight SIEM only

Log Database



1. Provide the **FQDN** or the **IP Address** of the database in the **Data Source** field
2. Provide the **Database Name** in the **Initial Catalog** field
3. Select **True** from the **Integrated Security** dropdown if the webpage's ID is to be included in the **Connection String**
4. Select **True** form the **Persist Security Info** dropdown if access to username and password information is allowed
5. Provide the **User ID** of the Database
6. Provide the **Password** associated to the **User ID**
7. Click **Generate Connection String**, and the **Connection String** will auto-populate based on the previous fields
8. Click **Test Connection** to ensure that the integration is successful
9. Click **Save to all Realms** if these Database settings are to be used in each SecureAuth IdP realm

Reports



5. Review the log **Reports** and **Charts** by downloading the information

6. Review the **Error Logs**, **Audit Logs**, and / or **Certificate Logs** as enabled here in the Web Admin as needed

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

Enhanced Logging

Key-Value Pair Properties

Key-value pair properties defined in the table below are pertinent to the structured data element of a syslog entry. Several of these properties are also logged in the header or message elements of the log entry but are difficult to parse or extract. These properties are outputted in their original location as well as in the structured data element.

Property	Description	Notes
AE.IP. RiskScore	Risk score based on IP Address evaluation and threat intelligence data	Applicable only to IP reputation log entries; also logged in the message element
AllowedTokens	For some authentication methods, this property may tell which method of 2FA was used.	Text string; possible values are: • COOKIE • ZCOOKIE • BROWSERFINGERPRINT • ALL
EventID	Category of the event being logged	Also logged in the header element
ReceiveToken		Integer
RequestDuration	Displays the response time of an application request	Applicable only to log entries with event ID9004x; also logged in the message element
RequestID	Displays a unique identifier that shows the workflow for a specific request	An "Application End" log entry marks the end of a request and its corresponding RequestID
TrxResult	Displays result of an authentication attempt	Also logged in the message element
UseJava		True / False

Syslog Logging Event

Syslog generates a log entry when a user opens or saves a tab using the Web Admin tool. This tool provides information about the realm a user modified at the time the log entry was generated.

Property	Description	Notes
Loading: [realm# **]**	Describes the realm number that was opened in the Web Admin	This log entry type is generated when a user opens a realm (by clicking the sidebar in the Web Admin) or opens a tab in a realm (e.g. Workflow, Data)
Saving to: [realm#, ... **]**	Describes the realm number(s) where changes were saved in the Web Admin	The value of this key lists all realms that were saved to when the log entry was generated

Information About Transaction Logs (20990)

Events recorded in Transaction Logs (20990) provide information that can assist in troubleshooting or analyzing end-user activity on the SecureAuth IdP appliance.

The table below provides details about common fields and values identified in transaction logs, and how to interpret that data.

Field / Description	Values / Description

<table>
<tr>
<td>Configured Persistent Token</td>
<td>The persistent token corresponds to the Client Side Control configured in the Production Configuration section on the Workflow tab
<table>
<tr><th>Persistent Token</th><th>Client Side Control</th><th>Integration Method</th></tr>
<tr><td>BROWSERFINGERPRINT</td><td>Device / Browser Fingerprinting</td><td>• Certification Enrollment and Validation
• Mobile Enrollment and Validation</td></tr>
<tr><td>ALL</td><td>Java Applet, Brower Plug-ins</td><td>Certification Enrollment and Validation</td></tr>
<tr><td>ZCOOKIE</td><td>Universal Browser Credential (UBC)</td><td>• Certification Enrollment and Validation
• Mobile Enrollment and Validation</td></tr>
<tr><td>COOKIE</td><td>Browser Credential</td><td>Mobile Enrollment and Validation</td></tr>
</table>
</td>
</tr>
<tr>
<td>Configured Workflow</td>
<td>The value corresponds to the Default Workflow configured in the Workflow section on the Workflow tab

The log provides counts for any of these values that are present:
<table>
<tr><th>Value</th><th>Default Workflow</th></tr>
<tr><td>0</td><td>Username | Second Factor | Password</td></tr>
<tr><td>1</td><td>Username | Password</td></tr>
<tr><td>2</td><td>Username | Second Factor</td></tr>
<tr><td>3</td><td>Username & Password | Second Factor</td></tr>
<tr><td>4</td><td>(Valid Persistent Token) | Second Factor</td></tr>
<tr><td>5</td><td>(Valid Persistent Token) | Second Factor | Password</td></tr>
<tr><td>6</td><td>(Valid Persistent Token) | Password</td></tr>
<tr><td>7</td><td>Username & Password</td></tr>
<tr><td>9</td><td>(Validate Persistent Token) only</td></tr>
<tr><td>999</td><td>Username only</td></tr>
</table>
</td>
</tr>
<tr>
<td>Log type classification</td>
<td>Audit Logs, Debug Logs, Error Logs are configured in Log Options section on Logs tab

Warning Logs by default are found in the Error Logs folder</td>
</tr>
<tr>
<td>End-user login failure transaction event details</td>
<td>The comment includes an entry for each type of end-user failed login event, and includes the count and decimal percentage for each instance
<table>
<tr><th>Numerical Value</th><th>Definition</th></tr>
<tr><td>NULL</td><td>No error or success</td></tr>
<tr><td>1</td><td>Bad Multi-Factor Authentication attempt count (minus 1) for user with locked or disabled status</td></tr>
<tr><td>2</td><td>Message from a state machine Security Violation</td></tr>
<tr><td>3</td><td>Message from a SecurityViolation_X509 (includes -1)</td></tr>
<tr><td>4</td><td>Attempt count from a Security Limit Violation (attempts that have reached the maximum limit)</td></tr>
<tr><td>5</td><td>A Redirect URL if the user was redirected to another page</td></tr>
</table>
</td>
</tr>
</table>

NOTE: Session Aborted appears whenever a session has ended (see **TrxResult**)

Security Violation Code	Definition
SecurityViolation	Adaptive check, hard stop
SecurityViolation_ExceededMaxPasswordAttempts	Password attempt exceeds set maximum attempts
SecurityViolation_ExceededMaxUserAttempts	User ID attempt exceeds set maximum attempts
SecurityViolation_ExceededMaxUserPasswordAttempts	User ID or password attempt exceeds set maximum attempts
The current windowsIdentity is different from logon user Id	Windows identity of the logged-in user has changed since last login
SECURITYVIOLATION_EXCEEDEDMAXCHANGEPASSWORDATTEMPTS	Exceeded maximum attempts changing password
SECURITYVIOLATION_EXCEEDEDMAXKBAATTEMPTS	Exceeded maximum attempts entering KB answers
SECURITYVIOLATION_EXCEEDEDMAXPINATTEMPTS	Exceeded maximum attempts entering PIN
SECURITYVIOLATION_EXCEEDEDMAXOTPATTEMPTS	Exceeded maximum attempts entering OTP
SECURITYVIOLATION_X509	Certificate issuance error
SECURITYVIOLATION_X509_CONTINUE	Certificate error, but can click Continue button to proceed

SecurityViolation_X509 Value	Definition
-1	Default
201	No ActiveX and no fall back allowed to obtain certificate
302	Certificate expired
402	Certificate not found
403	SSL certificate not found
404	SSL certificate error
405	UserID verification of certificate failed
406	CRI verification failure
407	URL verification failure
408	Certificate reset date failed
409	Maximum certificate attempt count attained
410	Maximum mobile cookie count attained
411	Certificate chain

Reserved	Reserved

<table>
<tr>
<td>Configured Workflow Integration Method</td>
<td>The value corresponds to the Integration Method configured in the Device Recognition Method section on the Workflow tab
<table>
<tr><th>Value</th><th>Integration Method</th></tr>
<tr><td>1</td><td>Certificate Enrollment and Validation</td></tr>
<tr><td>2</td><td>Certificate Enrollment Only</td></tr>
<tr><td>3</td><td>Mobile Enrollment and Validation</td></tr>
</table>
</td>
</tr>
<tr>
<td>Field under Custom Identity Consumer configured on the Workflow tab</td>
<td>The value corresponds to the Receive Token type configured in the Custom Identity Consumer section on the Workflow tab

The log provides counts for any of these values that are present:
<table>
<tr><th>Value</th><th>Receive Token</th></tr>
<tr><td>0</td><td>None</td></tr>
<tr><td>1</td><td>Token</td></tr>
<tr><td>2</td><td>Clear Text Query String</td></tr>
<tr><td>3</td><td>XOR / Base64 Query String</td></tr>
<tr><td>4</td><td>Send Token Only</td></tr>
<tr><td>5</td><td>Send XOR / Base64 Only</td></tr>
<tr><td>6</td><td>Receive Token Only</td></tr>
</table>
</td>
</tr>
<tr><td>Authentication request identifier</td><td>Reserved</td></tr>
<tr><td>Authentication request return URL</td><td>As specified by the Service Provider</td></tr>
<tr><td>SAML authentication request relay state URL</td><td>As specified by the Service Provider</td></tr>
<tr><td>Authentication request target URL</td><td>As specified by the Service Provider</td></tr>
</table>

Transaction result	The comment includes an entry for each type of end-user login event, and includes the count and decimal percentage for each instance:

Transaction Result	Definition
Session Aborted	Session ended
Success	Successful login attempt
WS-Trust success.	Successful login via WS-Trust
WS-Trust token validation failed.	Unsuccessful login attempt due to failure to validate the WS-Trust token
SA SSO Success	Successful login attempt via SSO
Incorrect_User	Unsuccessful login attempt due to end-user invalidation
SecurityViolation	Adaptive check, hard stop
Incorrect_Browser_RegistrationMethod_PIN	Incorrect Multi-Factor Authentication PIN entered
Incorrect_UserPassword	Incorrect password entered
Incorrect_FingerPrint_Check_Password	Incorrect password entered
Incorrect_Profile_DataErr	End-user found, but no profile information returned
NULL	Successful login attempt, but no information returned
Incorrect_Standard_Check_Password	Incorrect password entered
Incorrect_Group	Incorrect group returned for end-user
Incorrect_Browser_RegistrationMethod_OTP	Incorrect Multi-Factor Authentication OTP entered
SecurityViolation_ExceededMaxPasswordAttempts	End-user exceeded maximum session attempts via an incorrect password
Denied_Browser_RegistrationMethod_AcceptDeny_LoginRequest	Push-to-Accept Multi-Factor Authentication attempt denied
SecurityViolation_ExceededMaxPINAttempts	End-user exceeded maximum session attempts via an incorrect PIN
SecurityViolation_ExceededMaxUserAttempts	End-user exceeded maximum session attempts via an incorrect username
Redirect	End-user was redirected to a different page than the one intended to be accessed