

KB-101: Troubleshooting SAML Single Sign-On (SSO) Errors

Applicable Product: NexaCore Enterprise Console (v3.0+)

Target Audience: Client IT Directors / Identity Management Teams

Last Updated: 2025-11-01

Introduction

SAML Single Sign-On (SSO) is critical for enterprise user provisioning. This guide assists your Identity Management team in troubleshooting common errors encountered when configuring the NexaCore Service Provider (SP) with your Identity Provider (IdP) (e.g., Azure AD, Okta).

Section 1: Common Error Codes and Fixes

If a user receives a generic error during login, consult the corresponding error code in the NexaCore Audit Logs.

Error Code	Description	Root Cause / Recommended Fix
SAML-403	Unmatched Identity	The NameID attribute being sent by your IdP does not match a known user email or ID in NexaCore's user database. Fix: Ensure the attribute mapping in your IdP is correctly sending the user's primary email address as the NameID.
SAML-501	Expired Certificate	The signing certificate from your IdP has expired or was not updated in the NexaCore Enterprise Console before expiration.
SAML-400	Invalid Assertion	The SAML Assertion is not correctly signed or encrypted.
SAML-404	No Role Mapping	The user attempted to log

		in, but no corresponding NexaCore role could be found based on the provided group attributes.
--	--	---

Section 2: How to Access SAML Audit Logs

1. Log in to the **NexaCore Enterprise Console** as a System Administrator.
2. Navigate to **Settings Identity Management SSO Configuration**.
3. Click the "**View SAML Audit Logs**" button.
4. Filter the logs by the failed user's email address and the time of the failed login attempt.
This log provides the raw assertion data for diagnosis.

⚠ ATTENTION: If you are unable to resolve the SAML-501 error, contact your dedicated Customer Success Manager (CSM) or submit a P2 ticket with your new IdP metadata XML file attached.