meridian
KNOWLEDGE SOLUTIONS

SSO & SAML Setup: Your Step-by-Step LMS Integration Audit

Use this audit to validate your LMS's SSO/SAML configuration end-to-end. Walk through each step before go-live to ensure seamless, secure access for your learners.

1. **Confirm Identity Provider (IdP) Details**
    a. Record IdP name, version, and endpoint URLs (SSO URL, SLO URL).
    b. Verify IdP metadata file (XML) is current.
2. **Obtain Service Provider (SP) Metadata**
    a. Export your LMS's SAML metadata (entityID, ACS URL, certificate).
    b. Ensure metadata file includes correct Assertion Consumer Service endpoints.
3. **Validate Certificate & Encryption Settings**
    a. Check SAML certificates for expiration dates.
    b. Confirm signing and encryption certificates match between IdP and LMS.
4. **Configure Single Sign-On (SSO) URL & Binding**
    a. Ensure SAML HTTP-POST (or Redirect) binding is correctly specified.
    b. Confirm SSO endpoint in LMS matches IdP configuration exactly.
5. **Map SAML Attributes & Claims**
    a. List required attributes (e.g., NameID, email, firstName, lastName, groups).
    b. Verify attribute names/formats match IdP claims and LMS field expectations.
6. **Set Up Single Logout (SLO) (Optional but Recommended)**
    a. Configure SLO endpoint and binding in both IdP and LMS.
    b. Test that logging out of one system terminates the session everywhere.
7. **Define Session & Assertion Timeouts**
    a. Confirm NotBefore and NotOnOrAfter validity windows in the SAML assertion.
    b. Align session timeout settings between IdP and LMS to avoid premature logouts.
8. **Test User Provisioning via SAML (Just-in-Time)**
    a. If you use JIT provisioning, attempt to log in with a new user.
    b. Verify that accounts are created with correct roles/groups based on SAML data.
9. **Conduct Positive & Negative Login Tests**
    a. Positive: Log in as a valid user, confirm redirection to LMS dashboard.
    b. Negative: Attempt login with invalid credentials or revoked account to ensure access is denied.
10. **Audit Security & Compliance Logs**
    a. Review SAML request/response logs for errors or warnings.
    b. Confirm that assertions are signed and, if required, encrypted.
    c. Archive logs per your organization's compliance policy.

Audit Completion: ✓ Tick off each item as you validate it. Any failed checks should be remediated before granting broad access to avoid user lockouts or security gaps.