samegoal

Alerts/Document Viewer LTI Integration

SameGoal supports Alerts and Document Viewer Integration with vendors including student information systems (SISes), learning management systems (LMSes), dashboard applications, etc. A best-in-class implementation of this integration involves:

- **Alert sync:** SIS/LMS vendor syncs program participation alerts (eg Special Education, Section 504, English Learner, etc) in its system based on data obtained from the SameGoal API (typically pulled nightly).
- **LTI launch:** When the program participation alert is clicked in the SIS/LMS vendor system, it initiates an OIDC handshake resulting in a secure LTI launch to the district's special programs vendor (SameGoal). This ultimately results in the special programs vendor displaying the complete, effective plan document for the given student and program at the end of the LTI launch workflow.

The following documentation is intended for SIS/LMS vendors to use in developing a secure, standards-based integration:

- Program participation alert sync
- Alert click LTI launch
    - Integration configuration parameters
    - 1. LTI Platform POST to LTI Tool OIDC endpoint
    - 2. LTI Tool redirect back to LTI Platform auth endpoint
    - 3. LTI Platform POST to LTI Tool launch endpoint
    - 4. LTI Tool GET to LTI Platform public keyset URL (JWKS)

Program participation alert sync

SIS/LMS vendor can create program participation alerts (eg Special Education, Section 504, etc) in its system based on data obtained from the SameGoal API **Student Program Participation** endpoint (usually obtained nightly). Each program participation record includes:

- **Student ID:** Student ID in SameGoal (usually, but not always, SIS Student ID)
- **SIS Student ID:** Local student ID (in SIS)
- **Internal SIS Student ID:** Internal identifier in SIS for this student; used in LTI launch workflow
- **Start Date:** Date student began participation in this special program
- **End Date:** Date student ended participation in this special program
- **Program:** Name of special program (eg Special Education, Section 504, etc)
- **Program Abbr:** Abbreviation for special program (eg "SE" for Special Education)

- **Notes:** Text string; typically includes key program information such as disability, LRE, etc (separated by \n line breaks)

SIS/LMS vendor can create a visual indicator (flag/alert) in its system using the fields above. **Program Abbr** is sometimes displayed within the alert, and **Notes** can be used in an additional field, tooltip and/or hover for the alert. SIS/LMS vendor should initiate an LTI 1.3 launch when a program alert is clicked.

Tip Each district/LEA must configure API access to this endpoint through data exports in the SameGoal web interface.

Alert click LTI launch

When a program alert is clicked by a user logged into the SIS/LMS vendor system, the SIS/LMS vendor system must initiate an OIDC handshake resulting in a secure LTI launch to the district/LEA special programs vendor (SameGoal).

The following standards-based approach uses the authentication portion (only) of the Learning Tools Interoperability (LTI) Core Specification (version 1.3) published by IMS Global. LTI refers to this usage as 'Messages'. In the context of this specification, the following terminology applies:

- **LTI Platform (Issuer):** SIS/LMS vendor system that authenticates the user
- **LTI Tool:** Special programs vendor (SameGoal) receiving the launch

Integration configuration parameters

LTI Platform (SIS/LMS vendor) must provide a web interface or other mechanism for districts to generate, then copy/paste, the following configuration values into the LTI Tool (SameGoal web interface). LTI Platform must also store these values to verify authentication during the LTI launch workflow:

- **Client ID**: LTI Tool (special programs vendor) identifier
- **Deployment ID:** Unique district/LEA identifier
- **OIDC Authorization Endpoint:** LTI Platform-hosted (SIS/LMS vendor) HTTPs endpoint
- **Public Keyset URL (JWKS):** LTI Platform-hosted (SIS/LMS) HTTPs endpoint

1. LTI Platform POST to LTI Tool OIDC endpoint

When a logged in user clicks a program alert in the LTI Platform, the LTI Platform must redirect the User Agent (browser) to the LTI Tool OIDC endpoint:

POST https://samegoal.com/iep/lti/oidc

Parameter	Required	Description
lti_deployment_id	Yes	Deployment ID *(config setting)*
iss	Yes	LTI Platform's issuer identifier
target_link_uri	Yes	Final launch URL; https://samegoal.com/iep/lti/launch
login_hint	Yes	Opaque string; required parameter but not used (recommend empty string)

2. LTI Tool redirect back to LTI Platform auth endpoint

LTI Tool 302 redirects back to the LTI Platform's OIDC authorization endpoint *(config setting)*, with the following parameters included in the URL:

GET https://vendor-app.com/api/lti/auth

Parameter	Value Constraint	Description
scope	"openid"	OIDC Scope
response_type	"id_token"	Indicates an implicit flow returning a JWT
client_id	[Client ID] *(config setting)*	Client ID assigned to LTI Tool
redirect_uri	"https://samegoal.com/iep/lti/launch"	LTI Tool launch URL
login_hint	[Echoed Value]	Echoed value sent in step 1
nonce	[Dynamic String]	Critical; cryptographic nonce to prevent replay attacks
prompt	"none"	Instructs LTI Platform to not display any login or consent UI
response_mode	"form_post"	Instructs LTI Platform to send the id_token via an auto-submitted HTML form (POST)

3. LTI Platform POST to LTI Tool launch endpoint

LTI Platform validates the session, constructs a signed JWT (id_token), and returns an auto-submitting HTML form.

POST https://samegoal.com/iep/lti/launch

id_token: Signed JWT, constructed as follows:

JWT Header

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "[Key ID from JWKS]"
}
```

JWT Payload (Claims)

```
{
  "iss": "https://vendor-app.com",
  "sub": "[User ID]",
  "aud": "[Client ID]",
  "exp": "[Unix Timestamp + 5 mins]",
  "iat": "[Unix Timestamp Now]",
  "nonce": "[Nonce]",

  // LTI 1.3 Standard Claims
  "https://purl.imsglobal.org/spec/lti/claim/message_type": "LtiResourceLinkRequest",
  "https://purl.imsglobal.org/spec/lti/claim/version": "1.3.0",
  "https://purl.imsglobal.org/spec/lti/claim/deployment_id": "[Deployment ID]",
  "https://purl.imsglobal.org/spec/lti/claim/target_link_uri": "https://samegoal.com/iep/lti/launch",

  // Context Claim (Program)
```

```
  "https://purl.imsglobal.org/spec/lti/claim/custom": {
    "program_id": "[Program]",
    "student_id": "[Internal SIS Student ID]"
  },

  // Role Claim
  "https://purl.imsglobal.org/spec/lti/claim/roles": [
    "http://purl.imsglobal.org/vocab/lis/v2/membership#Instructor"
  ]
}
```

4. LTI Tool GET to LTI Platform public keyset URL (JWKS)

LTI Tool retrieves LTI Platform public keyset to decrypt id_token payload:

GET https://vendor-app.com/api/lti/jwks

LTI Tool finally 302 redirects to an LTI Tool-hosted document viewer web page if id_token is successfully decrypted.