temenos

# Cookie policy

Temenos uses “cookies” and other technologies on its website to allow certain information from your web browser to be collected. Cookies are widely used on the internet.

## Cookie Settings

Other than cookies that are essential, you have a right to choose whether you want to accept or decline cookies. We will not set any cookies, other than those which are essential, unless you choose to accept them. You can amend your preferences at any time on the button below.

The full list of cookies can be found here below:

| Name | Purpose | Product | Description |
|---|---|---|---|
| **userGuid** | Session | Content | Part of Content Cloud launch mechanism for OLCO. The value of the masked student id, which is used for SSO validations |
| **sk_mf** | Persistent | Core | Used to verify if the user has gone through Multifactor authentication within the last 24 hours. If so, they will be allowed to skip MFA on subsequent logins. The cookie is only set if client setup allows for it, and value is a JWT token with no sensitive information. Lasts a maximum of 24 hours. |
| **SessionGuid** | Session | Core | Contains a unique session identifier. Protects against Session Fixation vulnerability. Does not contain any Personal Information. |
| **sco** | Session | LMS | This cookie is used for course launch functionality in the Online Course Player for Scorm 1.2/AICC . The cookie keeps track of the Sco ID if launched as the player can display multi SCOs which can be launched. Can contain the Sco relative path and user int identifier. Does not contain any Personal Information. |
| **QS_COOKIE_ENC** | Session | Core | This cookie is required for query string encryption when the user is logged out of their session so that the user's ReturnUrl link can navigate back to the same page and be successfully decoded. Contains first eight characters of the session ID. Does not contain any Personal Information. |
| **multiVPoll** | Session | LMS | This cookie is used to let the browser know whether or not to poll to check if a new version of an online course has been published after the user has launched an online course. |

| | | | |
|---|---|---|---|
| **lti_userGuid** | Session | Content | Part of Content Cloud LTI course protocol. The value of the masked student id which is evaluated against the lti_message_hint of the authentication request |
| **lti_targetLinkUri** | Session | Content | Part of Content Cloud LTI course protocol. The value of the providers target link which is evaluated against the lti_message_hint of the authentication request |
| **lti_gcid** | Session | Content | Part of Content Cloud LTI course protocol. The value of the launched course which is evaluated against the lti_message_hint of the authentication request |
| **lti_customClaims** | Session | Content | Part of Content Cloud LTI course protocol. Holds a list of LTI related custom claims which will be added to the JWT provided to course provider |
| **loginCyberU_LogoutRedirectUrl** | Session | Core | This cookie holds the redirect URL used after a user's session times out or user logs out the session. Cookie's default expiry time is set as 1 day currently but it gets deleted during the log out operation. |
| **last_view** | Session | Cornerstone | Keeps track of last blog article viewed by user in the session. Used for navigation purposes. |
| **isintermediary** | Persistent | Single Sign On / Mobile | This cookie serves as a mechanism to track and authenticate user sessions that originate from the CSOD Learn mobile app. When the user initiates the SAML SSO login flow, this cookie is set to indicate the source of the authentication request. It enables the system to verify whether the login attempt was indeed triggered by the mobile application and the user can be redirected back to the mobile application. |
| **IDPssoRequestid** | Persistent | Single Sign On | The IDPssoRequestid cookie contains a randomly generated identifier during the SAML request initiation process under the e-signature workflow. When a user initiates an e-signature workflow through a trusted identity provider (IdP), this cookie stores the unique request ID value, which is then associated with the corresponding SAML response received from the IdP. By verifying the presence and integrity of this cookie, the system can authenticate users and validate the authenticity of SAML responses, preventing tampering or replay attacks. |
| **has_js** | Session | Cornerstone | Boolean used for javascript detection. This is for feature detection only. Does not contain any personal information. |
| | | | It stores a unique session identifier that allows a user to stay authenticated across multiple Galaxy services or subdomains without needing to log in separately to each one. This ensures a seamless, unified login experience across the Cornerstone Galaxy ecosystem when Global SSO is configured. |
| **EdgeStoreAdmin** | Session | Edge Store | Used to check whether a user is authorized for access of Edge Store. Contains an encrypted token generated by AdAuth, which contains the logged-in user's username, full name, and email. |
| **EdgeAdmind** | Session | Edge Admin Web | Used to check whether a user is authorized for access of Edge Admin Web. Contains an encrypted token generated by AdAuth, which contains the logged-in user's username, full name, and email. Note: this is only for CSOD employees. |
| **DownloadToken_{resultId}** | Persistent | Analytics/Reporting | Is used to disable download button during standard report file loading and to enable it after download complete. Cookie marked as "Secure" but as we are using it in JavaScript, we cannot mark it as HttpOnly. |

| | | | |
|---|---|---|---|
| | | | For more detail, see<br><br>RSR-3891 - Update Cookie Manifest Closed |
| **CyberUErrorMessage** | Session | Core | Carries over error message from the originating page to the actual page that displays the error. Contains error message GUID. Does not contain any Personal Information. |
| **CYBERU_lastculture** | Session | Core | This cookie is used to ensure our login and maintenance pages load in the local language of origin. Contains the Region (e.g., U.S.) of the incoming machine.<br>CHR is also using this to navigate to the new Self registration UI for EXE.<br>This is used in Custom Login Pages to retrieve the last language selected by a user on the login page in turn helping returning users to see the login page in their previously chosen language. |
| **CYBERU_CorpHostAlias** | Persistent | GTS | This cookie holds the value of corp from Corp Host Mapping entry which is further used in the PFD. This cookie has expiry of 1 day. |
| **CYBERU_backUrl** | Session | Core | This cookie holds the URL to return back from the Forgot Password Page in case corp setting does not exist or user cancels the option from the page. The default expiry time for this cookie is set as 1 day but it gets deleted during the log out operation. |
| **CYBERU** | Session | Core | This cookie is used to support session timeout due to inactivity. Contains the unique session key and the URL. |
| **csodlaunch** | Session | LMS | This cookie is used during course playing and should identify if the current launch attempt belongs to an existing attempt or a new one. Contains the Corp Name and the User Id. Does not contain any Personal Information. |
| **CSODApiconnectorAdUser** | Session | API Connector Web GPS Admin Tools | Used to check whether a user is authorized for access of GPS admin tools in API Connector Web. Contains an encrypted token generated by AdAuth, which contains the logged-in user's username, full name, and email. Note: this is only for CSOD employees. |
| **CSODApiconnectorAdmin** | Session | API Connector Web Admin Tools | Used to check whether a user is authorized for access of the admin tools in API Connector Web. Contains an encrypted token generated by API Connector Web, which contains the logged-in user's username and password. Note: this is only for CSOD employees. |
| **cscx** | Session | Core, Recruiting | Provides our 24x7 global performance monitoring system with regional statistics to ensure our pages (react and legacy pages) load quickly and consistently. Contains the name of the portal logged into and the numeric system identifier of the logged in user. Does not contain any Personal Information.<br><br>***c-c-n*** cookie has been retired and replaced with ***cscx*** |
| **ContentSettings** | Session | LMS | This cookie is used for IE browser to indicate compatibility that the browser engine will use. This will determine the respective meta header in the online course player. Does not contain any Personal Information. |

| | | | |
|---|---|---|---|
| **CodeChallenge** | Persistent | Single Sign On | CodeChallenge cookie contains a cryptographically secure code challenge value generated on the client-side when Proof Key for Code Exchange (PKCE) is enabled. When a user initiates an OAuth authorization flow, this cookie stores the expected code challenge value sent by the authorization server. By verifying the presence and integrity of this cookie, the Cornerstone system can authenticate users through OAuth with enhanced security and protection against intercepting attacks. |
| **CloudFront-Signature** | Session | LMS | Part of a set of cookies for authenticating requests going to access CCA course data in a shared location |
| **CloudFront-Signature** | Session | Content | Part of Content Cloud SCORM 1.2 course protocol. It is meant for signed cookies usage in Amazon CloudFront. |
| **CloudFront-Policy** | Session | LMS | Part of a set of cookies for authenticating requests going to access CCA course data in a shared location |
| **CloudFront-Policy** | Session | Content | Part of Content Cloud SCORM 1.2 course protocol. It is meant for signed cookies usage in Amazon CloudFront. |
| **CloudFront-Key-Pair-Id** | Session | LMS | Part of a set of cookies for authenticating requests going to access CCA course data in a shared location |
| **CloudFront-Key-Pair-Id** | Session | Content | Part of Content Cloud SCORM 1.2 course protocol. It is meant for signed cookies usage in Amazon CloudFront. |
| **c-s** | Session | Core | This cookie is required to support content file encryption and Java applets. Contains the name of the portal logged into. Not httpOnly as it is used for Flash requests. |
| **c-n-s** | Session | LMS | This cookie is required to support content file encryption and Java applets when client launches http content. Contains the name of the portal logged into. |
| **ASP.NET_SessionId** | Session | Core, Recruiting | This is a default cookie that is required for ASP based pages to load. Without this cookie, our website will not function. Contains the unique session identifier. Does not contain any Personal Information. |
| **AntiForgeryToken** | Persistent | Single Sign On | The AntiForgery token is a cryptographically secure value generated and stored on the client-side. During the OAuth SSO flow, this token is included in all requests to prevent unauthorized access attempts that may exploit vulnerabilities in the system. By verifying the presence of this token, the server can confidently authenticate users through OAuth, ensuring a secure and trustworthy experience. |
| **anon_user_cart_cookie** | Session | LMS | This cookie is used to temporarily hold items placed in the shopping cart by an anonymous user. The items are transferred to the user's shopping cart once they log in with their individual account. Selected items would be lost without this cookie. Contains Learning Object GUID. Does not contain any Personal Information. |
| **_accss** | Session | LMS | This cookie is used for automated course launch functionality in the Curriculum Player. The cookie keeps track of the Curriculum ID if launched in the Curriculum Player and the next Learning Object to be launched. Contains Curriculum and Learning Object GUIDs. Does not contain any Personal Information. |

| | | | |
|---|---|---|---|
| **.CSODApiconnector** | Session | API Connector Web | Used to check whether a user is authorized for access of certain pages within API Connector Web. Contains an encrypted FormsAuthenticationTicket generated by API Connector Web, which contains the SSO user's corp, email, first name, last name, user ID, username, whether they are an admin, whether they are a guest, permissions, and culture ID. |