SAP Litmos | RELEASE NOTES

2019.1 Product Release

Table of contents

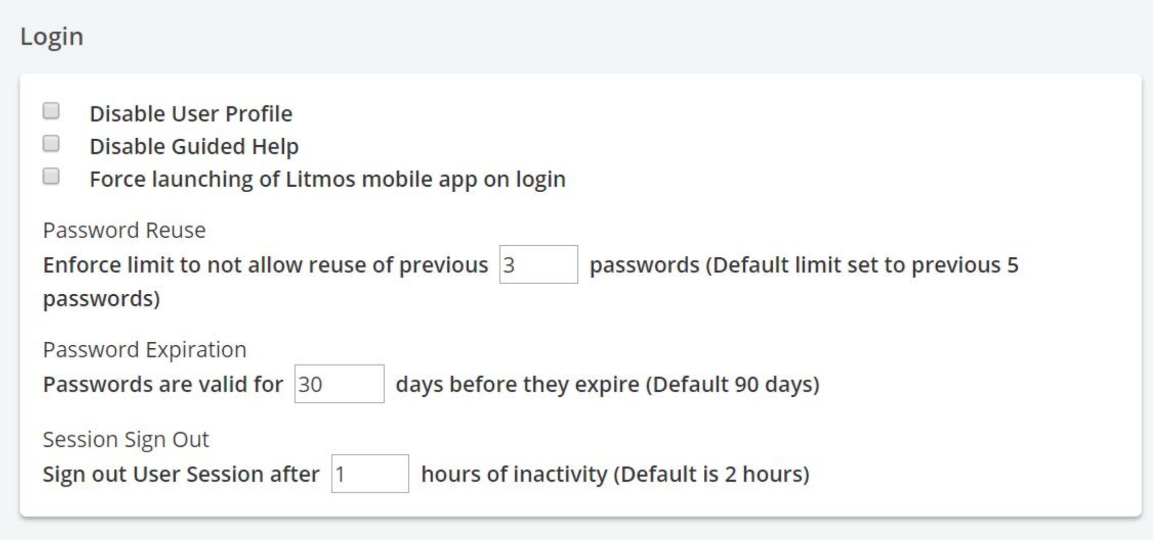
New Features

Login and Password Enhancements

Keeping security front and center, Litmos will begin to enforce new password requirements for all users. Please take note of the following changes:

- Users are now required to change passwords after a predefined interval. The default interval is 90 days as of February 15th 2019, but this interval can be configurable by the account owner. If the default interval is not configured to a specified interval (min = 30, max =180 days), then the first time any user will be required to change his/her password will be on the 91st day. This mandatory password change interval is enforced from date any user changes his/her password.
- Strong passwords are enforced for all users. If a user's password currently does not meet the minimum security standard for strong passwords (1 upper case, 1 lower case, 1 number, 1 special character, minimum 8 total characters), then that user will be required to meet these password security settings the next time the user updates his/her password.
- Users are not allowed to reuse any of their previous 5 passwords. Account Owners now have a new setting to manage password re-use, and can specify the minimum and maximum re-use limits (min = 3, max = 10).
- Users will now be given the option to show/hide passwords upon entry.
- If an Administrator sets/resets a user password, that user will be forced to change the password on the next login attempt.
- For online self sign up, users will be locked out for 2 hours if an incorrect token is entered more than 10 times from the same IP. This limit is set in the system and is not configurable.
- Account Owners will no longer have the option to “Enforce Strong Passwords” or “Disable User Ability to Change Password” in the Account Profile -> Login Settings.
- SSO users will not be subject to password expirations.
- User session timeouts after 2 hours of inactivity. The user session timeout duration is now configurable by the administrators (min = 1hr, max = 24hrs). This can be done via the Account Profile -> Login Settings.

The following configurable settings are available to the account owner in the Account Profile -> Login Settings:



Login

□ Disable User Profile
□ Disable Guided Help
□ Force launching of Litmos mobile app on login

Password Reuse

Enforce limit to not allow reuse of previous 3 passwords (Default limit set to previous 5 passwords)

Password Expiration

Passwords are valid for 30 days before they expire (Default 90 days)

Session Sign Out

Sign out User Session after 1 hours of inactivity (Default is 2 hours)

NOTE: These password changes will be in effect for all users, so please be sure to notify your learners.

For more information, please be sure to reference the following help articles:
Login/Password FAQ
User Login and Password Changes

Minor Enhancements

Email Validation for Reports

In an effort to ensure that scheduled Litmos reports are sent to valid users within the Litmos account, a new email validation will be enforced for emailed reports. Emails will only be delivered to email addresses recognized within the same Litmos account from which the report originated.

This change will be in effect for all report types (Quick Reports, Reporting Engine, Usage Reports, Quick Reports). This will impact existing scheduled reports if those are scheduled for delivery to email addresses that don't belong to users in the Litmos account.

Bug Fixes

- Account owners were unable to add new ILT locations
- Viewing users for a default brand would display users who were associated with another brand
- ILT Multi-day sessions for succeeding month were not appearing on the calendar
- Course due dates in the UI and reports were showing a day prior when the due dates were manually extended to a specific date for the learners
- Manually editing results for a course assigned to a user was reverting completion to current date instead of the date selected
- Edits made to recently created gamification items were not saving
- Team Leader/Admin - If team leader is not a leader of any team and they have the ability permission to manage courses and learning paths, the user could create a course from the dashboard but an error message will appear
- Never Logged In Usage Report : If date filter "None" was applied, the page timed out
- Disable User Profile: This feature was disabling Go To Training/Webex/Zoom authorization for Instructors. The authorizations for all three integrations (Go To Training, WebEx, and Zoom) have been removed from 'Edit my profile' page and have now been placed on the account page.
- These fields will no longer be generated onto the “Never Logged In” Quick Report: TotalCourses, TotalCompleted, PercentageCompleted, Complete, UpToDate, Marking

Important Announcements

SHA-1 SAML Authentication officially set to retire.

SHA-1 SAML authentication is no longer supported as of the start of 2019. SHA-1 is now considered a deprecated security standard and is no longer supported by SSL providers. Litmos supports SHA-2 authentication, which uses a larger bit encryption for enhanced security. If your company is still utilizing our SHA-1 endpoint (.litmos.com*/integration/samllogin*), update your SAML configuration to utilize the SHA-2 endpoint **immediately** (litmos.com*/integration/splogin).* SHA-1

If your company subscribes to a Litmos app provided by an identity and access management provider, please upgrade to the version of the Litmos app that affords SHA-2 encryption. The following identity and access management providers offer SHA-2 encryption for SAML authentication into Litmos LMS:

- Okta
- OneLogin
- Centrify

- PingIdentity
- Azure
- ADFS

Reauthorize Litmos Integrations: Webex, Salesforce, BambooHR, DocuSign and Payment Express

With this release, several Litmos integration *connections* will need to be regenerated in order to re-authorize a connection to the 3rd party application. This will require re-entry of the partner application credentials *into Litmos*, by the integration user in each organization for the following 3rd party applications: *Webex, Salesforce, BambooHR, DocuSign, and Payment Express.* Please note that Webex passwords will need to be re-entered into Litmos on a per user basis, so that Administrators and Instructors in Litmos are reach re-authorized to create Webex Meetings in the connected Webex Training Center account. Salesforce passwords only need to be re-entered for customers syncing module results.