LightspeedEVO

Third Party Access - Password Rotation Policy

Purpose

This addendum establishes password rotation requirements specific to the LightspeedEVO Third Party Access (3PA) Dealer-Direct Partner Program. It supplements the Lightspeed DMS Password Security Policy and should be read in conjunction with that document. The intent is to ensure continuous security of dealership data shared with authorized third-party vendors through standardized, enforced password lifecycle management.

Scope

This addendum applies to all dealership administrators, authorized personnel, and third-party vendors operating under the 3PA Dealer-Direct Partner Program. It governs the 3PA access credentials managed within LightspeedEVO at the store level under **System – Lists – Stores – Third Party Access**. This policy comes into effect April 6, 2026.

Authentication Principles

Consistent with the Lightspeed DMS Password Security Policy, the 3PA access password is one component of access control and must not be treated as the sole security measure governing third-party data access. Dealers retain full control over third-party access and are responsible for ensuring that only currently authorized vendors hold valid credentials at all times.

Password Generation

3PA access passwords are generated internally by the system and are not user-defined. A new password may be generated manually at any time by clicking the Generate New Password button located in the Third Party Access (3PA) tab of the Store detail view. Both automatic and manual password generation produce internally created credentials.

Prohibited Password Practices

As the 3PA password is system-generated, it is inherently compliant with Lightspeed DMS password construction standards. Dealers and administrators must not attempt to manually define, replicate, or share 3PA passwords outside of the secure credential distribution process outlined in Section “Password Distribution and Vendor Responsibilities” of this addendum.

Password Rotation and Expiration

In alignment with Section 6 of the Lightspeed DMS Password Security Policy, which requires service accounts and API keys to rotate every 90 to 180 days, 3PA access passwords are subject to the following rotation requirements:

The system will automatically renew the 3PA access password every 90 days. The rotation cycle is calculated from the date of the previous password reset, regardless of whether that reset was performed automatically by the system or manually by an authorized administrator. Manual password generation resets the 90-day clock from the date the new password is created.

This policy is effective April 6, 2026. For stores already active in the 3PA program, the 90-day rotation window is calculated from the most recent password reset date prior to or on the effective date.

Accessing the Password

To retrieve the current active 3PA password, an authorized administrator must navigate to **System – Lists – Stores**, open the Store detail record, and click on the **Third Party Access (3PA)** tab. Click the **Show Password** button and copy the password shown. Access to this tab requires security enabled for **System – Lists – Stores – Third Party Access** and is restricted to authorized personnel only.

Password Distribution and Vendor Responsibilities

Following each password rotation — whether automatic or manual — the authorized administrator is responsible for distributing the updated password to all currently authorized 3PA vendors in a timely manner to prevent disruption of service. Password distribution must follow the vendor's designated credential intake instructions. Only vendors with a current and active authorization are to receive updated credentials. Vendors not provided the updated password will lose data access immediately upon rotation.

If unauthorized access is suspected, a new password must be generated immediately using the **Generate New Password** button. The updated password should then be provided only to vendors authorized to maintain continued access.

Monitoring and Logging

In alignment with Section 12 of the Lightspeed DMS Password Security Policy, all password reset events within the 3PA program — whether system-initiated or manually triggered — must be treated as security-relevant events. Administrators should note the date of each reset to ensure compliance with the 90-day rotation window and to support audit requirements.

Enforcement

Violations of this policy, including failure to rotate passwords within the required 90-day cycle or unauthorized distribution of 3PA credentials, are subject to the enforcement provisions outlined in Section 14 of the Lightspeed DMS Password Security Policy, up to and including revocation of access, disciplinary action, or termination.