

Extensis Connect service disruption

July 2, 2026

Summary

On July 2, 2026 at 08:30 UTC, Extensis Connect experienced a service disruption that prevented users from logging in and accessing authenticated features. Because login is required to use the platform, affected users were unable to access key workflows during the incident window.

Service was fully restored at 11:26 UTC. The incident lasted 176 minutes (2 hours 56 minutes). The disruption was caused by a recent update to a core user-related service that introduced inefficient database queries, creating unexpectedly high load on supporting infrastructure and resulting in service unavailability. No data loss or data corruption occurred during the incident.

Event Timeline (UTC)

8:30 AM - Increased errors were detected affecting login to Extensis Connect. Investigation started.

9:19 AM - The issue was identified, and mitigation work began.

10:25 AM - Mitigation steps were applied, and services began recovering. Platform stability continued to be monitored.

11:26 AM - Service was fully restored and confirmed operational.

Root Cause Analysis

The incident was caused by a recent update to a core service used in the Extensis Connect authentication and user access flow. The update introduced inefficient database queries that, under production traffic, generated significantly higher load than expected on supporting database infrastructure. The resulting resource exhaustion prevented new application connections and caused login-dependent operations to become unavailable.

Because this service is in the critical path for authenticated access, the failure affected login and other application features that require an active user session. Once the issue was identified, supporting infrastructure capacity was increased, affected application services were restarted, and recovery was validated through monitoring before normal service was confirmed.

Key Observations

- The disruption affected authenticated access to Extensis Connect, including login and other application features that require an active user session.
- Because authentication is required for normal platform use, the incident resulted in a broad user-facing outage.
- The issue originated from service behavior under production load that placed excessive demand on supporting database infrastructure.
- No data loss or data corruption occurred during the incident.

Corrective and Preventative Actions

Immediate Corrective Actions

- Increased supporting database capacity to stabilize the affected service under production load.
- Restarted affected application services and validated recovery across critical user journeys.
- Monitored platform health and synthetic user journeys to confirm stable restoration of service.

Preventative Actions Implemented

- Reviewing and optimizing the service queries responsible for excessive database load.
- Strengthening production release coordination and notification for critical services.
- Adding performance and database load validation for changes that can materially affect supporting infrastructure.
- Improving monitoring, alerting, and operational readiness to identify similar degradation earlier and reduce recovery time.

These measures ensure improved stability, resilience, and long-term scalability of Extensis Connect services.