08-12-2026

Update data

Update data refers to the information, files, or instructions that are transmitted and applied to modify, enhance, or fix existing software systems. This data typically contains changes such as bug fixes, security patches, performance improvements, feature enhancements, or version upgrades. Update data ensures that software remains functional, secure, and relevant to user needs or compliance standards. Updates ensure protection against vulnerabilities and emerging threats and enhance software efficiency and responsiveness. Updates also help meet regulatory or industry standards.

Update data is often delivered through mechanisms such as over-the-air (OTA) updates, patch files, or versioned releases and might target an application, operating system, firmware, or other software components. They generally follow a regular release cycle (for example, weekly, monthly, or quarterly) or be delivered as major version upgrades, but patches are usually released on an as-needed basis (for example, to address security vulnerabilities or urgent bugs).

Update data typically includes:

- **Feature enhancements**: Updates that introduce new features or improve existing ones
- **Version upgrades**: Comprehensive updates that include significant changes to the software, often denoted by a major version number change
- **Database schema updates**: Changes to the structure of a database, such as adding new tables or modifying columns
- **Configuration file updates**: Modifications to configuration files to update settings or parameters for the software
- **Firmware updates**: Updates to the embedded software controlling hardware devices
- **Dependency updates**: Updates to third-party libraries, frameworks, or modules used by the software
- **Operating system (OS) updates**: Updates to the underlying OS that software depends on
- **Application metadata updates**: Changes to metadata such as descriptions, icons, or permissions in app stores
- **Localization updates**: Updates that add or improve language translations and regional settings
- **UI/UX updates**: Updates focused on improving the user interface (UI) or user experience (UX)
- **Performance optimization updates**: Changes aimed at improving software speed, efficiency, or resource usage
- **Analytics and telemetry updates**: Updates that improve or change how software collects usage data for analytics purposes

The Splunk Common Information Model (CIM) add-on contains an Updates data model with fields that focus specifically

on patch management events from individual systems or central management tools. Patch management data is a subset of update data.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for Splunk Enterprise, Splunk Cloud Platform or Splunk Observability Cloud.

Add-ons and apps

- Linux/Unix
  - Splunk Add-on for Unix and Linux
  - Splunk Add-on for Linux
  - Monitoring Linux - Metrics and Logs Forwarding
  - Linux Splunk App
- Microsoft
  - Splunk Add-on for Microsoft Windows
  - Splunk Add-on for Microsoft Hyper-V
  - Splunk Add-on for Microsoft Cloud Services
  - Monitoring Windows Containers - Metrics and Log Forwarding
- Oracle
  - Splunk Cloud Addon for OCI (Oracle Cloud Infrastructure)
  - Splunk App for Oracle Cloud Infrastructure (OCI)
  - Splunk Add-On for Oracle Cloud Infrastructure (OCI)
- Splunk Add-on for Sysmon
- Splunk Add-on for Google Cloud Platform
- Qualys Technology Add-on (TA) for Splunk
- Docker
  - Docker Connector
  - Docker App for Splunk
  - Splunk Connect for Docker
  - Docker Monitoring Add-on for Splunk
- Kubernetes Connector

Splunk Lantern articles for the Splunk platform

- Automating Splunk platform administration with a Continuous Configuration Automation framework
- Maintaining *nix systems with the Splunk platform
- Sizing your Splunk architecture
- Maintaining Microsoft Windows systems with the Splunk platform

Splunk Lantern articles for Splunk observability products

- Collecting Mac OS log files
- Monitoring Kubernetes pods