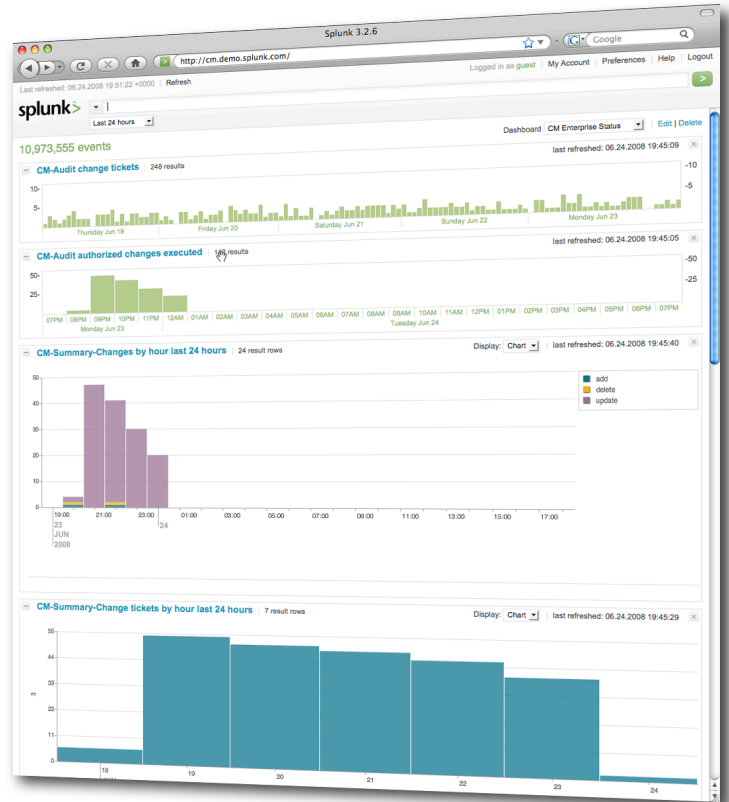
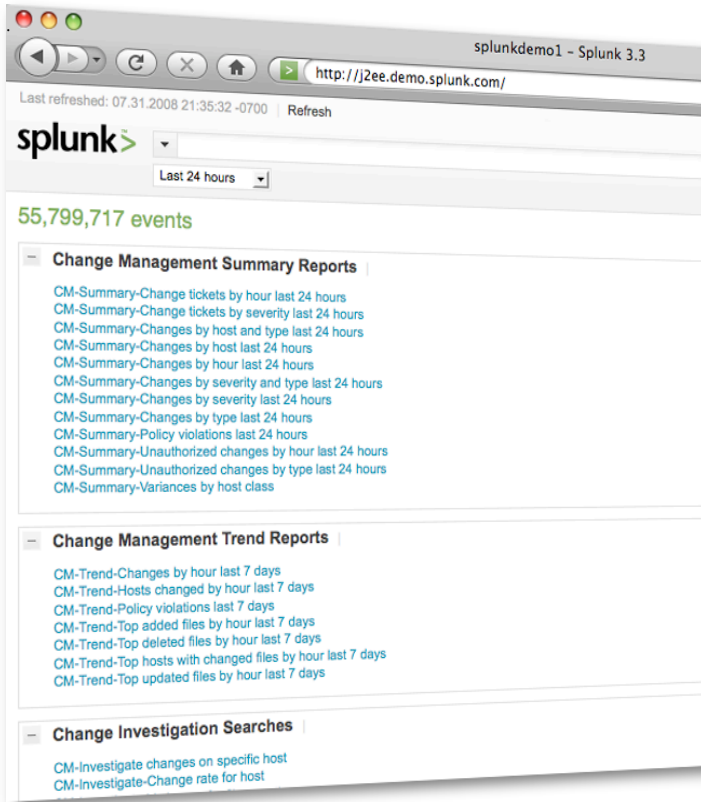




# Splunk for Change Management

Detect and react to unauthorized changes and resolve change related incidents faster.



## Comprehensive change management

Splunk for Change Management, an application built on the Splunk IT Search platform, lets you navigate from changes to system behavior with everything you need all in one place.

- Pre-built searches, alerts and reports for change lifecycle
- Change Auditing - make it an effortless daily routine
- Change Detection - adaptive detection and remediation
- Change Reporting - see change across all your IT infrastructure components
- Change Validation - close the loop on change
- Incident Response - link change to system behavior

Now you can drive efficiency through all change management processes: audit, detection, reporting and validation. Bring all your change and IT data together in one place and break down change control and change audit silos.

Operations will benefit with improved mean time to recovery (MTTR) by quickly pinpointing service-impacting changes during incident response. You'll avoid downtime by detecting changes prior to negative system impact.

## The old way

### Unauthorized change causes downtime.

Frequently the root cause of critical service problems is change. Unauthorized change is the worst kind. Until now, IT management has tried to combat unauthorized change through a combination of change control through CMDB and configuration management, and change auditing through server and network change detection. The change control approaches have been incompletely applied, while the change auditing approaches have resulted in expensive new information silos that are divorced from incident and problem response processes. Unauthorized changes still go undetected, and it's exceedingly difficult to track down the changes behind new problems.

## The new way

### Splunk links change to system behavior.

Bring powerful indexing, search, alerting and reporting to the challenges of change management. Splunk captures and indexes file system changes, database audit logs, and actual configuration files and database records alongside configuration policy, change tickets, error events and other IT data for a contextualized view of change. Its powerful search capabilities let you correlate data from different servers, compare actual configuration to policy, and alert and report on anomalies and unauthorized changes. Better yet, Splunk lets you navigate from errors to changes and configurations within a single search interface to speed root cause identifications and resolve problems fast.

# Using Splunk for Change Management

## Change Auditing

Splunk makes the change audit process an effortless daily routine. Use Splunk's pre-defined change auditing searches to find and review all configuration file changes, deletions and additions. Pre-defined searches leverage Splunk's sophisticated transaction correlation capabilities to retrieve scheduled authorized changes, those made outside the authorized time window, and those that lack corresponding change tickets. Splunk's easy-to-navigate results make quick work of reviewing these changes. And an audit trail lets you prove that you're complying with review requirements.

## Change Detection

No matter what controls are in place, real-world systems continually drift from their target configurations. Splunk detects when files on some hosts differ from others, and when files on production hosts differ from master configurations in CMDB or change control systems—before they cause downtime or performance problems. Splunk alerts you to these variances via email or RSS. Splunk can even automatically remediate change variances by triggering scripts.

## Change Reporting

Keeping tabs on changes throughout the day is the best way to be sure you know what's happening in your environment. Splunk provides dashboards and reports to look at the volume of changes in a variety of different dimensions at-a-glance. Keep tabs on changes by host, by host group, by file and trended over time. Monitor the volume of authorized and unauthorized changes. And if something stands out, quickly drill down to individual change events, specific configurations, and other activity impacted by the change.

## Change Validation

Authorized changes that don't take place, or don't have their intended impact, must be tracked as well. Splunk makes it easy to close the loop on every authorized change by configuring searches that routinely validate changes and intended impact. This search can be linked from each change ticket, and built into the standard change management workflow. For example, for a change intended to cure an intermittent error on an application server, a search for the error message can validate whether the change was effective.

## Incident Response

Best of all, Splunk lets you link change to its impact on system behavior and performance. When an error occurs, Splunk quickly locates the symptom in error logs, and then correlates on time with underlying changes, configurations and administrative events—all from a single web interface. Instantly identify the latest configuration of every component involved in a failed transaction. Find out what changed last and who changed it. Find the reference configuration and quickly highlight the specific variances. There's no need to switch contexts to a dedicated change management console.

## Features

### Index

- File system change monitoring detects and records change events across all commonly deployed operating systems including Linux, Solaris, Windows, AIX and Mac OSX  
Windows registry monitoring captures all Windows configuration changes
- Captures network configurations and changes remotely
- Indexes other sources of change monitoring data including Solaris BSM and Linux auditd
- Captures master configurations from CMDBs and change control systems
- Captures tickets from service desk tools to correlate authorizations with actual changes
- Indexes actual configuration files and scripts with changes, log events and other IT data

### Search

- Instant freeform search across all IT data for rapid identification of service-impacting changes during incident response
- Predefined searches support routine auditing of authorized and unauthorized changes
- Workflow integration with ticketing systems facilitates validation of change impact

### Alert

- Predefined alerts notify administrators of unauthorized changes and configuration variances via email, RSS or scripts

### Report

- Predefined reports and dashboards provide management visibility into the volume and profile of system changes

## Get Started Today !

- Download your own free copy of Splunk today at [www.splunk.com/download](http://www.splunk.com/download).
- Download a 30-day free trial of the Splunk for Change Management application at [www.splunk.com/goto/apps/change](http://www.splunk.com/goto/apps/change)
- Visit [www.splunk.com/apps/](http://www.splunk.com/apps/) for tips, tricks and applications to help get off the ground with Splunk for Change Management.