Splunk Configuration Files - Detailed Overview

# 📁 Overview of Splunk Configuration Files

Splunk uses plain-text configuration files (.conf files) to define its behavior. These files are stored in specific directories and follow a layered precedence model (default, app-level, user-defined).

# 🔑 Key Configuration Files

* inputs.conf: Defines data inputs (files, ports, scripts, etc.)
* props.conf: Controls parsing rules (line-breaking, field extractions, timestamps)
* transforms.conf: Works with props.conf to apply regex-based transformations (routing, masking, etc.)
* outputs.conf: Defines data forwarding settings (used by forwarders)
* server.conf: Core server settings (e.g., GUID, roles, clustering)
* indexes.conf: Configuration for index creation and data retention
* authentication.conf: External authentication (LDAP, SAML, etc.)
* authorize.conf: Role-based access control (RBAC) settings
* deploymentclient.conf: Used by deployment clients to connect to deployment server
* deploymentserver.conf: Used by deployment server to manage apps on clients
* web.conf: Web interface settings (ports, HTTPS, etc.)
* limits.conf: Controls resource usage limits and search constraints
* alert\_actions.conf: Defines custom alert actions (e.g., send to webhook, email, script)
* savedsearches.conf: Stores saved searches, alerts, and reports
* commands.conf: Configuration for custom search commands

# 🗂️ Configuration File Locations

* $SPLUNK\_HOME/etc/system/default/ - Splunk default settings — do not edit!
* $SPLUNK\_HOME/etc/system/local/ - System-wide custom settings — override default
* $SPLUNK\_HOME/etc/apps/<app\_name>/local/ - App-specific configs — most commonly modified
* $SPLUNK\_HOME/etc/users/ - User-specific settings

# 📋 Example Snippets

1. 1. inputs.conf (monitoring a log file)

[monitor:///var/log/syslog]  
disabled = false  
index = os\_logs  
sourcetype = syslog

1. 2. props.conf (custom timestamp and line breaking)

[source::...access.log]  
TIME\_FORMAT = %d/%b/%Y:%H:%M:%S  
MAX\_EVENTS = 1000  
SHOULD\_LINEMERGE = false

1. 3. transforms.conf (masking sensitive data)

[mask\_ssn]  
REGEX = \d{3}-\d{2}-\d{4}  
FORMAT = XXX-XX-XXXX  
DEST\_KEY = \_raw

1. 4. outputs.conf (forwarding data)

[tcpout:central\_indexer]  
server = indexer1.company.com:9997

# 🧠 Best Practices

* Never modify default/ files – always override in local/.
* Use version control (e.g., Git) for managing app configs.
* Backup configuration files regularly.
* Use btool to troubleshoot configuration merging:  
   splunk btool inputs list --debug