07-12-2026

Authentication data

Authentication data refers to the information used to verify the identity of a user, system, application, or device attempting to access a resource or service. Authentication verifies identity, while authorization determines what the authenticated user is allowed to do.

Authentication data is a critical component of security mechanisms, ensuring that only authorized entities can access protected resources. It can include credentials such as passwords, tokens, biometrics, or certificates. It should should never be stored in plaintext. Instead, it should be hashed or encrypted, and transmitted using secure protocols to prevent unauthorized access or interception. Handling authentication data often falls under privacy regulations like GDPR, CCPA, or HIPAA, depending on the context.

Authentication data typically includes:

- **Knowledge-based authentication (something you know)**
  - Personal identification number
  - Security questions and answers
  - Username and password
- **Possession-based authentication (something you have)**
  - Digital certificates
  - One-time passwords
  - Physical security tokens
  - Smart cards
- **Biometric authentication (something you are)**
  - Facial recognition data
  - Fingerprint data
  - Iris or retina scans
  - Voice recognition data
- **Behavioral authentication (something you do)**
  - Keystroke patterns
  - Mouse movement or gesture patterns
- **Token-based or cryptographic authentication**

    - API keys
    - OAuth access tokens
    - Session tokens
    - SSH keys
- **Multi-factor authentication (MFA)**
    - Password + biometric
    - Password + OTP
    - Smart Card + PIN

The Splunk Common Information Model (CIM) add-on contains an Authentication data model with fields that describe login activities from any data source.

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

- Aruba ClearPass App for Splunk
- AWS IAM Connector
- Azure AD User Registration Details
- CrowdStrike OAuth API
- Entrust Identity as a Service Add-on for Splunk
- Okta Connector
- PingFederate App for Splunk
- RSA SecureID Authentication Manager
- Splunk Add-on for Cisco ESA
- Splunk Add-on for Cisco Identity Service
- Splunk Add-on for Cisco WSA
- Splunk Add-on for Jira Cloud
- Splunk Add-on for Jira Data Center
- Splunk Add-on for Okta Identity Cloud
- Splunk Add-on for RSA SecurID
- Splunk Add-on for RSA SecurID CAS
- Splunk Supporting Add-on for Active Directory

Splunk Lantern articles for the Splunk platform

- Accelerating security forensics with Federated Search for Amazon S3
- Complying with General Data Protection Regulation

- Configuring SAML authentication for the Splunk platform
- Detecting anomalous customer record lookups with statistical baselines
- Detecting brute force access behavior
- Enabling Okta single sign-on in the Splunk platform
- Finding interactive logins from service accounts
- Getting Okta data into the Splunk platform
- Implementing business, data, and security compliance
- Managing Azure cloud infrastructure
- Monitoring NIST SP 800-53 rev5 control families
- Monitoring Windows account access
- Performing data exploration and statistical analysis with Federated Search for Amazon S3
- Running common General Data Protection Regulation compliance searches
- Securing a work-from-home organization
- Securing a work-from-home organization
- Securing the Splunk Cloud Platform
- Securing the Splunk platform with TLS
- Simplifying compliance trails and audits with Federated Search for Amazon S3
- Streamlining threat reporting, dashboarding, and alerting with Federated Search for Amazon S3
- Troubleshooting SAML authentication for the Splunk platform

Splunk Lantern articles for Splunk security products

- Configuring Windows event logs for Enterprise Security use
- Configuring Windows security audit policies for Enterprise Security visibility
- Detecting cloud federated credential abuse in AWS
- Detecting cloud federated credential abuse in Windows
- Detecting non-privileged user accounts conducting privileged actions
- Detecting Office 365 attacks
- Detecting password spraying attacks within Active Directory environments
- Disabling a user account with Azure AD Graph connector
- Enabling an audit trail from Active Directory
- Managing identity risk with Enterprise Security and Cisco Identity Intelligence
- Monitoring for signs of a Windows privilege escalation attack
- Monitoring medical record numbers for anomalous access
- Tuning Enterprise Security assets and identities
- Using the Splunk Enterprise Security assets and identities framework

Splunk Lantern articles for Splunk Observability Cloud

- Building a self-serve and scalable observability practice
- Monitoring for signs of Windows privilege escalation attacks