JumpCloud®

Technical Data Sheet

JumpCloud is a Cloud-based Directory-as-a-Service®

The product is designed and delivered entirely in a SaaS model with no on-premise infrastructure or related networking required. The directory leverages industry-standard protocols to securely connect user identities with their systems, applications, and networks.

Authentication Protocols

JumpCloud supports the following authentication protocols to ensure connectivity with a wide array of IT resources for authentication and authorization with the directory's identities:

- LDAP
- SAML 2.0
- SSH
- RESTful HTTP
- RADIUS

SaaS Delivery Model

JumpCloud's globally hosted infrastructure is delivered to its customers via a Software-as-a-Service model, eliminating networking requirements associated with on-premise directory infrastructure.

- Highly scalable, secure, and redundant cloud-based infrastructure leveraging both Amazon Web Services and Google Cloud Platform globally
- Platform status available at http://status.jumpcloud.com/
- Zero on-premise infrastructure required for operation or backup
- Zero custom networking required between office/resource locations
- Web-based consoles for administrators and end user management
- RESTful API for automation, including auto scaling capabilities for cloud-server management

Event Logging

Learn how to use our Events API

JumpCloud captures events across the various endpoints bound to the directory enabling effective monitoring and auditing of employee access with resources.

- RESTful API
- Admin and user console changes
- System login events (Mac, Linux, Windows)
- 45-day data retention
- Event data output: JSON

JumpCloud®

Technical Data Sheet

Centralized User Management

Learn more

JumpCloud centralizes the management of your user identities through its cloud-based directory, enabling remote user management and access to assigned resources.

- Local user account binding and provisioning on Windows, Linux, and macOS
- Password complexity modeling reuse enforcement
- Group-based access for applications, systems, and networks
- Office 365 and G Suite user account provisioning
- Global administrative privilege assignment across systems
- LDAP BindDN (service account) management
- Admin add/edit/delete control over SSH keys
- Attribute management for users
  - » Immutable Base Attributes
    - FName
    - LName
    - Username
    - Email
  - » Mutable Custom Attributes
    - String Attributes

Centralized System Management

Learn more

JumpCloud's system management capabilities enable administrators to manage Windows, Mac, and Linux endpoints, at scale, regardless of location, with no need for VPN networking.

- Cross-OS support for: Windows, Mac, Linux
  - » Windows: 7, 8, 8.1, 10 (32 and 64 bit). Server: 2008 R2 (32 and 64 bit) 2012, 2016 (64 bit)
  - » Mac: 10.10, 10.11-10.11.6, 10.12
  - » Linux: Amazon® Linux, CentOS, Debian, RHEL, Ubuntu
- Port 443 outbound utilized for communication (no unique ports needed)
- Secure password hash management
- Agent size: 14-45MB on disk
- Agent CPU Consumption: 5-8MB in process
- Agent installation through configuration management solutions (e.g. Jamf, Chef, Puppet, Ansible, etc.) or API

JumpCloud®

Technical Data Sheet

LDAP-as-a-Service

Learn how to connect your applications to LDAP

Applications or other resources that require integration with a backing LDAP directory can leverage JumpCloud's cloud-based LDAP service, enabling legacy resources to connect to JumpCloud's cloud-based directory.

- RFC support - OpenLDAP-based, RFC 2307 schema
- Search Base structure:
  - » `ou=Users,o=YOUR_ORG_ID,dc=jumpcloud,dc=com`
- Binding account structure:
  - » `uid=YOUR_LDAP_BINDING_USER,ou=Users,o=YOUR_ORG_ID,dc=jumpcloud,dc=com`
- **URI:** ldap://ldap.jumpcloud.com (clear text or STARTTLS)
  - OR - ldaps://ldap.jumpcloud.com (SSL)
- **Ports:** 389 (clear text or STARTTLS) - OR - 636 (SSL)
  - » `ou=Users,o=YOUR_ORG_ID,dc=jumpcloud,dc=com`
- Globally-distributed and geo load balanced LDAP protocol servers
- Group support through **`groupOfNames`** object class including **`memberOf`** overlay on **`inetOrgPerson`** object class

RADIUS-as-a-Service

Learn how to implement RADIUS-as-a-Service

Wireless networks, switches, VPNs, and other similar resources that leverage the RADIUS protocol can be directly integrated with JumpCloud's cloud RADIUS servers for authentication and authorization.

- FreeRADIUS-based
- Geo load balanced RADIUS edge servers
- RADIUS Server IPs:
  - » 104.154.91.253
  - » 104.196.54.120
- Port 1812/UDP to our RADIUS service endpoints
- Encryption/Authentication Mode:
  - » WPA2 Enterprise
  - » WPA2 with RADIUS
- Automatic complex shared secret/password generation
- EAP-TTLS, EAP-PEAP, PAP, and MSCHAPV2 support

JumpCloud®

Technical Data Sheet

Security

See our security practices

JumpCloud has established and continually maintains a high security posture, beginning with our hiring process, to the manner we build, deploy, and monitor our software, through to our on-going security audits and process controls.

- Private and self-contained PKI infrastructure
- Encrypted two-way TLS between endpoints
- Data encryption at rest and in transit
- SSL and https communication tunnels
- Password hashing and salting, prior to storage and encryption (no clear text management)
- SOC2 audit attestations available upon request

Password Policy Management

Learn more

JumpCloud enables IT administrators to manage and improve security for your users' passwords from one location, for all resources associated to the user by modeling the password complexity and rotation.

- One password for all systems, applications, or networks the user is assigned to access
- Set password length
- Require special characters
- Limit password reuse
- Schedule or force password rotations
- Restrict use of username within password
- End user self service password reset and management

Multi-Factor Authentication (MFA)

Learn more

JumpCloud allows you to easily add a second factor of verification to provide critical additional layers of endpoint security with Multi-Factor Authentication.

- MFA Algorithm: TOTP
  - » Example generators: Google Authenticator, Duo Mobile, etc.
- MFA Endpoint Coverage:
  - » JumpCloud admin and user consoles
  - » Mac systems
  - » Linux systems

JumpCloud Technical Data Sheet

Single Sign On (SSO)

See full list of compatible apps

JumpCloud allows you to easily enable access to your commonly used apps via our user portal.

- SAML 2.0 support
- Group-based application access
- XML Metadata output for streamlined app setups
- Generic SAML 2.0 Connector for custom application integrations.
- 140+ web applications supported.

G Suite / Office 365 Integration

Video Tutorial G Suite | Office 365

JumpCloud can act as the authoritative directory for both G Suite and Office 365. Simultaneously manage the identities for both of these services with no on-premise directory components required.

- API-driven integration (no middle-tier software required)
- Enforce password complexity and rotation
- Provide core identity management services for G Suite / Office 365
- Import pre-existing accounts
- Export/Provision new accounts
- Block/suspend (deprovision) accounts
- Update accounts (password changes, attribute changes (e.g. name))
- Integration through a persisted and secure OAuth connection
- SAML SSO for users

SSH Key Management

Learn how to generate an SSH key pair

JumpCloud securely stores and controls your employee's public keys and leverages them for more secure access to Linux and Mac hosts.

- Admin add/edit/delete control over user SSH keys
- Management of multiple keys per individual user
- End user self-service SSH key management