CLOUDFLARE

Keyless SSL

Retain on-premise custody of SSL private keys with cloud-based DDoS mitigation, CDN, WAF and more

Keyless SSL lets sites use Cloudflare for SSL traffic while retaining on-premise custody of their private keys. Keyless SSL with Cloudflare includes all other benefits of Cloudflare's service—a robust, rules-based, learning web application firewall, distributed caching of objects at Cloudflare's datacenters around the world, and the industry's strongest denial-of-service mitigation technology.

With Keyless SSL, SSL private keys never leave your on-premise infrastructure, and are not shared with anyone.

Simple software-based agent running on your own hardware behind your firewall

Keyless SSL is deployed as a lightweight software agent which can run on your own hardware behind your firewall. Keyless SSL is available for a variety of operating systems, including Linux (packaged for Red Hat/CentOS, Debian and Ubuntu, and others), other UNIX operating systems (including FreeBSD), and Microsoft Windows.

Compatible with existing key management infrastructure

Keyless SSL is compatible with existing key management infrastructure, including Enterprise Key and Certificate Management (EKCM) solutions from Venafi and Hardware Security Modules (HSMs) from multiple vendors.

Extensively reviewed by cryptography experts

Keyless SSL builds upon standard SSL algorithms, just changing where they run. The Keyless SSL protocol has been extensively reviewed by both commercial (iSEC Partners/Matasano Security) and academic researchers, and is equivalent to on-premise SSL.

Highlights:

- **Keep custody of your keys on-premise:** Maintain SSL private keys on your own servers, using existing software or hardware based key management
- **Full Cloudflare performance acceleration:** SSL content can be cached in datacenters around the world, and SSL connections resumed without re-connecting to keyless server
- **Compatible with WAF and anti-DDoS filtering:** SSL traffic can be filtered through Layer 7 Web Application Firewall, and SSL servers protected from denial-of-service
- **Software-only solution:** Does not require any special hardware to be installed at your site; can run on existing Unix (Linux, FreeBSD) or Windows servers.

Key features	Benefit
Security	
Supports multiple keys	Supports multiple SSL certificates per key server
Mutually authenticated connections	Key server connects to Cloudflare’s infrastructure via mutually authenticated TLS tunnel
Standards	
Compatible with standard SSL protocol	Doesn’t require any modifications to existing web browsers or web servers.
Enterprise key management suites	Cloudflare Keyless SSL keys can be managed on-premise along with other critical enterprise keys
Supports multiple cryptographic algorithms	Supports full suite of SSL/TLS cryptographic algorithms
Flexibility	
Multiple operating systems	Key server can run on Linux, other UNIX operating systems, or Windows
Pre-packaged	Key server packaged for RPM (Red Hat, CentOS), DEB (Debian, Ubuntu)
Source available	Key server source code available for review
Software-only solution	Runs entirely as software on standard servers, does not require new hardware
Minimal network impact	Key server requires a single inbound TCP port for communication with Cloudflare
Performance	
Session Tickets	Supports RFC 5077-compliant session tickets (Chrome, Firefox) for global session resumption
Session ID	Supports session ID based session resumption on most web browsers
Persistent connections	Cloudflare to key server network connection established and maintained once per boot.
Availability	
Load balancing	Multiple key servers can run in parallel to distribute load
Automatic failover	Key server is stateless and can be configured for automatic failover
Cloud-based monitoring	Monitored within Cloudflare’s global network of edge servers
Web-based configuration	Cloudflare services managed through web-based portal