



Automated Kernel **SECURITY UPDATES** Without Reboots

Safe Kernel. Safer Linux.



KernelCare

We are  CloudLinux

Rebootless Kernel Security Updates

KernelCare keeps kernels secure and ends reboots forever with a single command. It ensures you never miss security patches, and your kernels are always up to date.

For Admins, it provides huge convenience, security, and time savings. For business users, it eliminates downtime to their business-critical applications.

50K+ servers running



KernelCare Protects Servers

1

Eliminate
downtime

Installs patches to live (or staging) servers without performance impact or downtime

2

Never miss a
critical patch

Super-fast, latest security patch release – the agent checks for new patches every 4 hours

3

Single-line rebootless
installation

A few minutes to install, nanoseconds to update, with roll-back capability, all without reboots



“The downtime that reboots cause is a disruption for customers, and nuisance for admins, that can be easily avoided with KernelCare. We’re moving closer to a time in which this type of “disruption is no longer excusable.”

JOE OESTERLING, Chief Technology Officer at Liquid Web

KernelCare Streamlines Costs

1

Avoid security issues

No more vulnerabilities as kernels are always up to date on all security updates.

We monitor security lists so your Admins don't have to.

2

Lower operating cost for server management

Automated patching frees up your IT team. No more middle-of-the-night & weekend maintenance windows.

3

No more application downtime for business users

Avoid application downtime due to kernel updates, eliminate the need to coordinate between various locations, users and Admins.

Cost Considerations

Traditional kernel updates

OPERATIONAL COSTS:

Kernel Updates: *Due to maintenance windows and admin costs, timely updates and server reboots are difficult. Factors to consider:*

1. Number of servers that need to be updated;
2. % of servers that will have restart issues during a reboot;
3. Damage control from issues arising within the timeframe of discovered vulnerability and a fix;
4. Being non-compliance due to running unpatched software prior to next maintenance window;
5. Number of Admins needed to perform updates;
6. Days/hours Admins spent performing mundane maintenance planning and updates, as opposed to other important IT initiatives.

BUSINESS COSTS:

Business Interruption: *Various business units are affected by the downtime during the update. Factors to consider:*

1. Business and opportunity cost of application downtime
2. Stakeholders involved in downtime planning
3. Risk factors related to security issues if they arise

Using KernelCare

Admin costs related to:

One-time:

...KernelCare rebootless installation on each server.

In rare cases... testing of patches on the staging environment

KernelCare is Affordable

\$2.25

per server per month for accounts with 500+ licenses

No interruption to running applications, no vulnerable kernels, and no Admin hassle.

How KernelCare Works

1

Our security experts with deep knowledge of kernel development monitor all Linux security lists 24x7x365;

2

Once they notice a vulnerability that affects our supported kernels, they promptly prepares a security patch;

3

Patch is compiled in a binary format and is deployed to KernelCare distribution servers;

4

KernelCare agent checks for new patches every 4 hours and if any, it downloads it and updates kernels without the reboot.

**ENTERPRISE-
READY:**

*Full support for
servers behind the
firewall*

Our team combines **450+** man-years of in-depth technical knowledge of **Linux and kernel development.**

Built for the Enterprise

Supports automatic updates or managed updates in a live environment or in your desired staging environment. Works on typical servers as well as virtual environments.

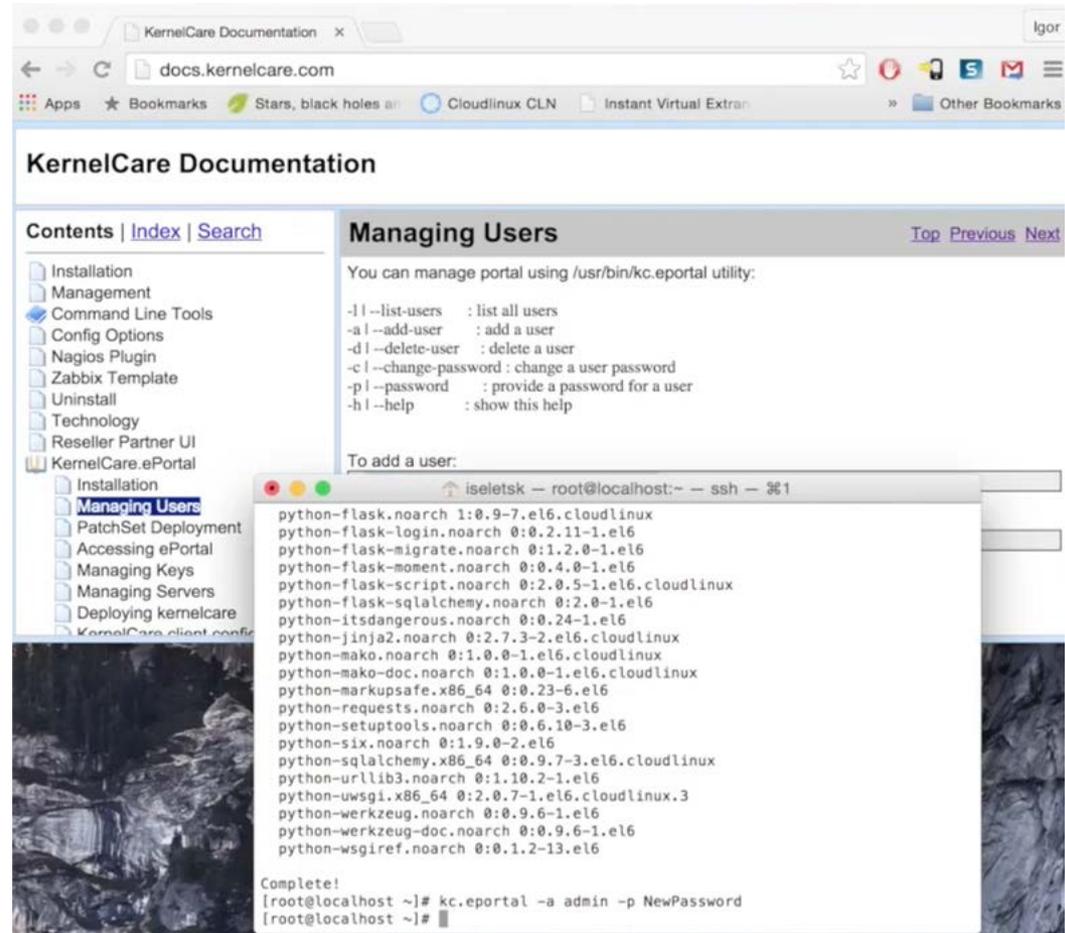
SUPPORTS MOST POPULAR LINUX DISTRIBUTIONS:

CentOS/RHEL 5, 6, 7; CentOS 7 Plus; Xen4CentoS 6, 7; CloudLinux 5, 6, 7; Proxmox VE 2.6, 3.10, 4.4; Ubuntu LTS 14.04, 16.04; Virtuozzo/OpenVZ 2.6.32 and Debian 6, 7, 8.



Built for the Enterprise

KernelCare.ePortal, an enterprise tool for security, control, and flexibility, allows Admins to manage patches for servers located behind the firewall.



The image shows a screenshot of the KernelCare Documentation website and a terminal window. The website, accessed at docs.kernelcare.com, displays the 'Managing Users' section. The terminal window shows the output of the 'kc.eportal' utility, listing various Python-based packages and their versions for different architectures.

KernelCare Documentation

Contents | Index | Search

- Installation
- Management
- Command Line Tools
- Config Options
- Nagios Plugin
- Zabbix Template
- Uninstall
- Technology
- Reseller Partner UI
- KernelCare.ePortal
 - Installation
 - Managing Users**
 - PatchSet Deployment
 - Accessing ePortal
 - Managing Keys
 - Managing Servers
 - Deploying kernelcare
 - KernelCare.client.config

Managing Users [Top](#) [Previous](#) [Next](#)

You can manage portal using /usr/bin/kc.eportal utility:

```
-l --list-users : list all users
-a --add-user : add a user
-d --delete-user : delete a user
-c --change-password : change a user password
-p --password : provide a password for a user
-h --help : show this help
```

To add a user:

```
python-flask.noarch 1:0.9-7.el6.cloudlinux
python-flask-login.noarch 0:0.2.11-1.el6
python-flask-migrate.noarch 0:1.2.0-1.el6
python-flask-moment.noarch 0:0.4.0-1.el6
python-flask-script.noarch 0:2.0.5-1.el6.cloudlinux
python-flask-sqlalchemy.noarch 0:2.0-1.el6
python-itsdangerous.noarch 0:0.24-1.el6
python-jinja2.noarch 0:2.7.3-2.el6.cloudlinux
python-mako.noarch 0:1.0.0-1.el6.cloudlinux
python-mako-doc.noarch 0:1.0.0-1.el6.cloudlinux
python-markupsafe.x86_64 0:0.23-6.el6
python-requests.noarch 0:2.6.0-3.el6
python-setuptools.noarch 0:0.6.10-3.el6
python-six.noarch 0:1.9.0-2.el6
python-sqlalchemy.x86_64 0:0.9.7-3.el6.cloudlinux
python-urllib3.noarch 0:1.10.2-1.el6
python-uwsgi.x86_64 0:2.0.7-1.el6.cloudlinux.3
python-werkzeug.noarch 0:0.9.6-1.el6
python-werkzeug-doc.noarch 0:0.9.6-1.el6
python-wsref.noarch 0:0.1.2-13.el6
```

Complete!
[root@localhost ~]# kc.eportal -a admin -p NewPassword
[root@localhost ~]#

More information on KernelCare.ePortal can be found at cloudlinux.com/kernelcare-eportal

1,000+ companies, including Dell & IBM, keep their Linux servers on and secure with KernelCare

We are  CloudLinux

KernelCare is a product of CloudLinux, the company that is making Linux secure, stable and profitable since 2009. Its flagship **CloudLinux OS powers over 20 million websites.**

50K+
servers running
securely without
reboots with
KernelCare

To learn more about **KernelCare for the Enterprise**, visit <https://www.cloudlinux.com/kernelcare-enterprise>

Questions? Contact Alex Yevelev, VP of Business Development
+1 (201) 720-2340 | ayevelev@cloudlinux.com