KerioConnect

Enterprise-Class Email, Calendars and Instant Messaging at a Fraction of the Cost and Complexity of Other Solutions

The award-winning, low-overhead Microsoft Exchange alternative, Kerio Connect meets the needs of small and mid-sized businesses while offering a robust feature lineup. Business users enjoy support for their favorite email client and easy webmail access. Kerio Connect is highly stable—so you can focus on business rather than unexpected downtime and recovery.

- ✓ **Cross-platform** support for a variety of email clients for the flexibility business users demand

- ✓ **Protection** for email users and the network with security features such as SSL encryption, S/MIME and powerful antivirus and anti-spam tools

- ✓ **Intuitive** anytime, anywhere administration through the Kerio Connect web-based administration console

- ✓ **Rapid deployment** in any IT environment whether cloud, on-premises or virtualized

- ✓ **Secure mobile** support for a wide range of devices—from iPhones and Android phones to tablets.

Deliver the Cross-Platform Support that End Users Demand

- Provide the flexibility business users want through support for Outlook on Windows and Mac as well as Apple Mail, Calendar and Contacts apps.

- Offer access to full-featured webmail via the Kerio Connect client.

- Support any email solution that supports IMAP/CalDAV/CardDAV open standards.

- Allow user self-setup with Kerio Connect's auto-configuration tools.

Protect Email Users—and Your Network —with Integrated Security Features

- Get powerful protection with SSL encryption, S/MIME, anti-spam tools—such as SpamAssassin filtering technology and algorithms—auto-blocking of unknown spam servers and custom whitelists of trusted servers.

- Protect your network from viruses, Trojans, worms, spyware and adware while minimizing impact on memory and system performance with the Sophos Antivirus engine.

- Block IP addresses suspected of account and password-guessing attacks, block accounts that have been targeted by password-guessing and even elect not to block guessing by local clients.

- Leverage the Kerberos protocol to authenticate log-in attempts between a client and server or between servers.

- Repel hacking and malicious behind-the-firewall activity by automatically filtering and disallowing suspicious attachments.

Administer Email, Calendaring and Other Critical Functionality Easily and Efficiently

▪ Configure and manage your system anytime, anywhere—even from a tablet—through the clean and simple Kerio Connect web-based administration console.

▪ Perform full or differential on-demand or scheduled backups of both data and server configurations without downtime.

▪ Exercise fine-grained administrative access and control on servers, public folders and archive folders.

▪ Enjoy easy access to detailed logs, reports and usage statistics.

▪ Integrate with popular directory services like Apple Open Directory and Microsoft Active Directory.
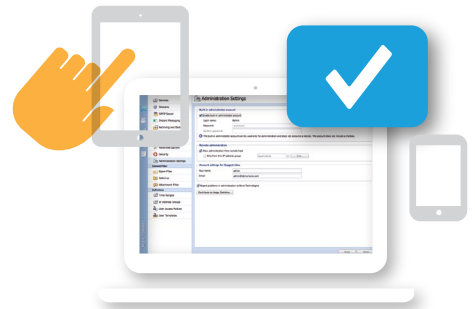
Deploy Rapidly in Any IT Environment

▪ Deploy side-by-side on the same hardware as other business applications and on popular hypervisor platforms, such as VMware and Hyper-V.

▪ Install Kerio Connect software on existing hardware through support for most versions of Windows Server, Linux and Mac OS X—including many legacy and desktop (non-server) versions.

▪ Choose Kerio Connect as a pay-as-you-go hosted service delivered by an authorized Kerio Connect Hosting Provider.

▪ Integrate Kerio Connect into existing IT processes for a great user experience at the desktop or on the road.

▪ Leverage free migration tools to move quickly and easily from Exchange, IMAP and any other environment.

Offer Smooth and Seamless BYOD Support

▪ Provide support for a wide range of mobile devices—from iPhones and Android phones to tablets of all kinds – using Exchange ActiveSync or IMAP/CalDAV/CardDAV protocols.

▪ Secure communications with the SSL and S/MIME protocols to protect users on the go.

▪ Enable end users to configure their own mobile devices without requiring assistance from IT.

▪ Remotely delete suspicious files and other data from mobile devices to protect users from hacking or malicious activity.