



SaaS

(Software as a Service)

2012 Product Guide





Page 1	Cover Page
Page 2	Directory of Services
Page 3	About Excel Micro, Inc.
Page 4	Google Message Security
Page 5	Google Message Discovery
Page 6	Google Message Encryption
Page 7	Google Apps for Business
Page 9	ZixCorp Email Encryption
Page 10	IronPort Email Encryption
Page 11	EXM Email Continuity
Page 12	Webroot Web Security
Page 13	Contact Information

Thank You for your interest in Excel Micro!
We currently are the Largest Authorized Distributor of the complete suite of Google Message Security & Compliance Solutions formally known as Postini. We manage over 3,500 resellers worldwide and close to 1 million SaaS licenses sold.

Call Us at (877) 4NO-SPAM (466-7726)
Or
Visit <http://www.excelmicro.com>

Excel Micro, Inc.

ABOUT US

Founded in 1991 in the Philadelphia-area's technology corridor, the company's mission is to consistently be: The most reputable distributor of SaaS "Software as a Service" solutions.

Excel Micro is the largest Authorized Distributor of the complete suite of Google Message Security & Compliance Solutions and are responsible for the worldwide reseller channel, managing over 3,500 resellers and close to a million SaaS Licenses sold. In addition, Excel Micro is an industry leader in the SaaS marketplace.

You will have the ability to purchase the market leading SaaS solutions, for Spam/Virus Filtering, Email Encryption, Email Archiving, Office Collaboration, and Web Security.

Our product brands include Google, Postini, ZixCorp, Cisco IronPort, Webroot, and other industry leaders. As an Excel Micro reseller you will have access to marketing and training materials, webinars, presentations, fully-functional trials, as well as, Excel Micro's Product Support Specialists. We invite you to join the thousands of companies moving toward SaaS solutions everyday.

Product / Service Overview

This product guide will give you insight to the services that we can offer

Built on industry standards, Excel Micro's suite of products and services brings your business:

- Cost Savings
- Improved Network and Desktop Security
- Administrative Ease

Industry professionals and editors are raving about the Excel Micro solution as:

- Comprehensive
- Cost Effective
- Easy to Install and Maintain

The SaaS model is on track to become the standard that will replace everything you're currently using. It's more effective and less expensive protection.

PRODUCTS

EMAIL SECURITY

- Google Message Security, powered by Postini

EMAIL ARCHIVING

- Google Message Discovery, powered by Postini
- Archiving & Discovery, powered by Postini

EMAIL ENCRYPTION

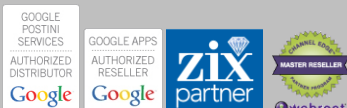
- Google Message Encryption
- ZixCorp Email Encryption
- Cisco IronPort Email Encryption

OFFICE COLLABORATION

- Google Apps for Business
- Google Apps for Government

WEB SECURITY

- Webroot Web Security SaaS





What is Google Message Security?

Google Message Security, powered by Postini, provides highly effective inbound and outbound email security for organizations of all sizes. Google Message Security is always on and always current, so organizations are assured of having effective and reliable protection for their email at all times. Google Message Security blocks spam, phishing, viruses, and other email threats before they reach your organization, reducing load on your email servers, conserving bandwidth and improving the performance of your existing messaging infrastructure.

Google Message Security conserves IT resources by eliminating the constant patching and updates that are required by other appliance or software solutions. End-users manage their own message quarantines and settings with an easy-to-use, web based interface.

What's Included?

- **Real-time** threat identification
- Automatically identifies and tracks internet protocol (IP) addresses that are issuing attacks such as **spam, viruses, denial of service (DoS), etc.**
- Patented real-time anti-spam technology examines thousands of elements of an email message in order to determine if it is spam
- Extremely effective spam filtering, and **exceptionally low false positive rates**
- Multiple commercial anti-virus engines
- **Content management & attachment management** allows you to define policies for both inbound and outbound email that provides an additional layer of protection against external threats

Industry Leader

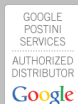
Google Message Security is the industry leading 100% hosted spam & virus filtering solution. Processing over 3 billion connections per day in real-time keeps clients protected from the latest email security threats. With a simple MX record change you do not need to worry about costly hardware, updates, maintenance, patches, or unexpected downtime. By having email security hosted you are freeing up IT resources to focus on more strategic projects and not worry about time consuming spam & virus filtering.

Requirements & More Information

Google Message Security requires a registered domain and an active email account. For more information on Google Message Security and a helpful video visit www.excelmicro.com/services/spam-virus-filtering. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

FEATURES & BENEFITS

- Comprehensive message security to stop spam, viruses, phishing, denial of service (DoS), directory harvest attacks (DHA), and other email attacks
- **Zero-hour anti-virus** protection with multi-layered protection, including heuristic and signature-based detection
- Extensive and detailed **quarantine summary reporting** to end users through a convenient web console
- Built-in **lexical analysis** for social security and credit card
- Real-time processing with scale & reliability
- Patented real-time, pass-through architecture ensures that there are no delays, message loss or disruptions to email service, regardless of how high spam volumes climb
- **99.999% availability** for message processing and capacity to handle billions of transactions a day
- Policy enforced domain to domain messaging encryption using standard **SSL or TLS** protocols
- **SAS 70 Type II** certified and **WebTrust** seal validates Google's stringent standards for physical and operational security, assuring the safety of your communications





What is Google Message Discovery?

Google Message Discovery, powered by Postini, goes beyond the functionality of our security offering to give customers maximum control and flexibility over your electronic records archive, meeting discovery, and compliance objectives.

In addition to the security provided by Google Message Security, powered by Postini, Google Message Discovery provides archiving, discovery, and compliance functionality. Whether you must respond to a discovery situation or want to prepare in advance for an eventual request, Google Message Discovery can help you find and manage the right information quickly and painlessly.

What's Included?

- All features & benefits of Google Message Security
- Centralized Message Center for each user to manage their individual archive
- Unlimited storage space
- Email Retention anywhere from 1 to 10 years
- Messages cannot be rewritten or deleted
- Detailed reporting and message holds for audit and other investigations
- Administrator full search & discovery access over the entire domain
- Export search results to PST or MBOX format for further review and analysis

Why Archive?

In today's world, electronic communications are both increasingly critical and growing in volume. Businesses know that they need to archive this critical communications data but struggle with keeping this data from clogging primary communications systems. Google Message Discovery helps companies accomplish both objectives at once.

Offered as a hosted service, Google Message Discovery includes everything you need to get started with an online digital archiving and discovery strategy. No need to worry about hardware, software, upgrades, maintenance, high availability and scalability. What could be easier than a simple, all-inclusive per-user fee? No more complicated math to put together hardware, storage, redundancy and labor costs! It's easy to budget and plan for archiving and discovery costs now with Google Message Discovery.

Requirements & More Information

Google Message Discovery requires companies to have their own mail server. If an ISP hosts your email, we suggest you consider Google Apps for Business, which doesn't require that you own your mail server. For more information on Google Message Security and a helpful video visit www.excelmicro.com/services/archiving. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

FEATURES & BENEFITS

Manage Archives

Centralize storage of message data into a single company archive to offload data from mail servers, enforce a standard retention policy, and provide an easily accessible repository for discovery efforts.

Discover Evidence

Effectively manage multiple investigations, inquiries, and discoveries with enhanced search, save, and restore capabilities. Place records on hold, such as necessitated by litigation notice, which temporarily discontinues automatic message deletion.

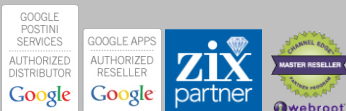
Best of all, it's hosted by Google. So there's no hardware or software to download, install or maintain. Google Message Discovery simplifies mailbox storage management, eases IT administration burdens, and lowers the total cost of ownership compared to software or appliance based solutions.

ADDITIONAL SERVICES



Historic Message Journaling

Historic Message Journaling is now available. HMJ is an additional solution offered through Excel Micro that will ingest historic emails into your new Google Message Discovery account. This will eliminate the needs to manage two separate archive solutions and have everything now searchable within your Message Center.





What is Google Message Encryption?

Google Message Encryption, powered by Postini, provides on-demand message encryption for your organization to securely communicate with business partners and customers according to security policy or on an “as needed” basis.

Without the complexity and costs associated with legacy on-premises encryption technologies, Google Message Encryption service makes encrypting email messages easy and affordable. The policy-based solution enables your organization to send encrypted email to any recipient.

What's Included?

- **Secure messaging** between business partners, customers, or individuals without any additional software, hardware, or technical training
- **Automatic enforcement** of organizational email encryption policies based on individuals, groups, or specific message content
- User-initiated encryption for confidential messages to **any email recipient**
- Auditable protection of emails containing regulated or company proprietary information
- Centrally-managed security policies and reporting

How Does It Work?

Google Message Encryption service secures outgoing email to the Postini data center using a secure SSL/TLS encrypted connection. At the data center, messages are scanned for viruses and messaging policy compliance. Based on centrally managed policies, messages are encrypted for each intended recipient. Encrypted messages are either delivered directly to the recipients' inbox or stored on a web-based portal for secure pickup.

Requirements & More Information

Google Message Encryption requires a Google Message Security or Google Message Discovery account. You must have the ability to redirect your outbound mail on your internal email server or have a Google Apps for Business account in order to use this solution. For more information on Google Message Encryption visit www.excelmicro.com/services/encryption/gme. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

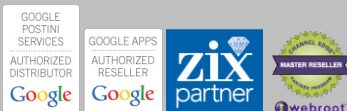
DELIVERY METHOD

Inbox Delivery

The inbox delivery method delivers email directly to the recipients' email application as an encrypted attachment. Recipients can view their messages by opening the attachment and providing their password. If the recipient does not have an existing password, the recipient is stepped through a simple, one-time registration. No additional software is required.

Portal Delivery

Using the secure portal delivery, email notifications are sent to intended recipients letting them know a message is waiting for them. The notification message includes a link to the portal and instructions on how to view the encrypted message using their web browser. Clicking on the link directs recipients to the secure portal. Using the full-featured messaging console, recipients can view, reply to, and compose new messages securely.



Google™ Apps for Business

What is Google Apps?

Google Apps is a suite of applications that includes Gmail, Google Calendar (shared calendaring), Google Talk (instant messaging and voice over IP), Google Docs & Spreadsheets (online document hosting and collaboration), Google Page Creator (web page creation and publishing), Start Page (a single, customizable access point for all applications) and Google Security & Compliance.

Google Apps for Business gives you the communication and collaboration tools to manage electronic communication, information sharing, and stay connected anywhere. Whether your business is moving everything to the cloud, just wants an affordable email solution or struggles to give employees access to critical information, Google Apps will help you stretch resources and work smarter. Google Apps for Business is 100% hosted by Google, so there is no hardware or software to download or maintain.

What's Included?

- **Google Mail** - 25GB storage, less spam, and a 99.9% uptime SLA, mail search tools, integrated IM, and enhanced email security
- **Google Docs** - Create, share and collaborate documents, spreadsheets, and presentations in real-time
- **Google Calendar** - Agenda management, scheduling, shared online calendars and mobile calendar sync
- **Google Sites** - Secure, coding-free web pages for intranets and team managed sites
- **Google Talk** - Instant messenger with free PC-to-PC voice calls worldwide
- **Security** - Spam and virus filtering powered by Postini

Access Anytime Anywhere?

With Google Apps you can access your email, documents, calendars, contacts, and more anywhere you have an internet connection.

Ready To Go Google?

Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email sales@excelmicro.com.



HOW SECURE IS GOOGLE APPS?

Having your mail, documents, and other information hosted in Google's **SAS70 Type II** and **FISMA Certified** data centers is more secure than using your own in-house mail server like Exchange.

Google is the first major cloud provider to offer **2-step verification**, default https encryption, attachment viewing and mobile device management in the browser, along with many other security & administrative capabilities. You can view more of Google's security and data protection measures outlined in their Security Whitepaper.

Google operates on of the most robust networks of distributed data centers worldwide. The data centers are protected around the clock and monitored by a **dedicated security team**, the facilities are held to **extremely high standards of scrutiny** every moment of the day.

Adding Postini services such as **Archiving & Discovery** will help you limit exposure to spam and virus, and will provide you with SAS70 compliant email archiving.

COMPATIBLE PRODUCTS

EMAIL SECURITY

- Google Message Security, powered by Postini

EMAIL ARCHIVING

- Archiving & Discovery, powered by Postini

EMAIL ENCRYPTION

- Google Message Encryption
- ZixCorp Email Encryption
- Cisco IronPort Email Encryption

EMAIL INGESTION

- Excel Micro Historic Message Journaling

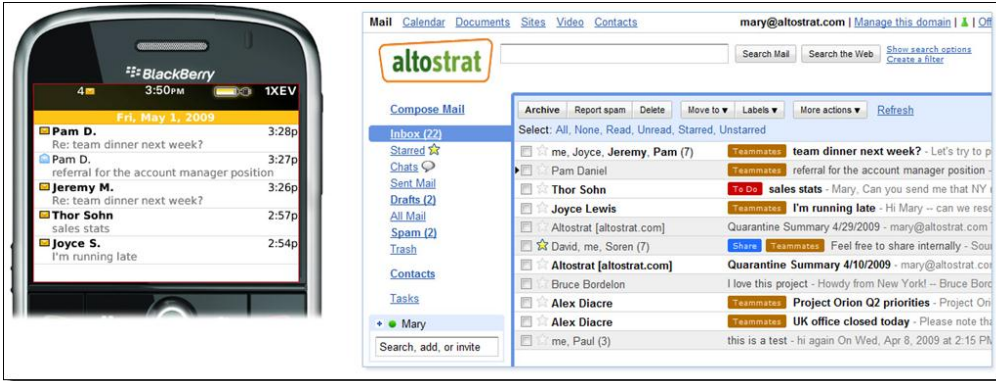
WEB SECURITY

- Webroot Web Security SaaS



Google™ Apps for Business

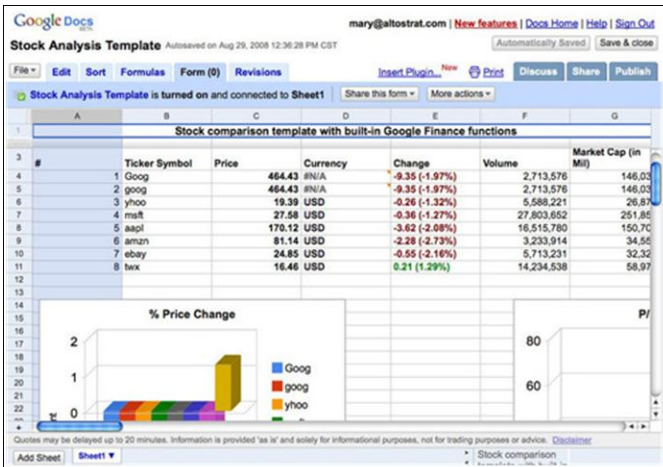
Google Apps for Business gives you the communication and collaboration tools to manage electronic communication, information sharing, and stay connected anywhere. Whether your business is moving everything to the cloud, just wants an affordable email solution, Google Apps will help you stretch resources and work smarter



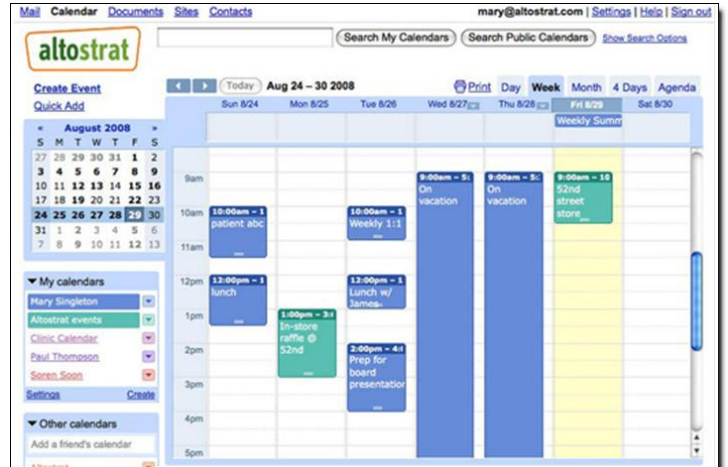
Google Mail- 25GB storage, less spam, and a 99.9% uptime SLA, mail search tools, integrated IM, mobile sync, and enhanced email security



Google Talk- IM with free PC-to-PC voice calls worldwide



Google Docs- Create, share and collaborate documents, spreadsheets, and presentations in real-time



Google Calendar- Agenda management, scheduling, shared online calendars and mobile calendar sync





What is ZixCorp Email Encryption?

ZixCorp is the leading provider of policy-based email encryption as a service for privacy and regulatory compliance.

As the largest hosted email encryption service provider, ZixCorp protects millions of email addresses, including those of some of the nation's most influential institutions. This easy-to-use service connects organizations with their customers and partners to protect and deliver sensitive information in healthcare, finance, insurance and government.

Features & Benefits

- Ability to send secure email to anyone
- Built-in content scanning
- No training for end users
- No software to install
- Policy management for regulatory compliance
- Automatic retrieval and distribution of encryption keys
- Full content scanning of subject line, messages and attachments
- S/MIME, OpenPGP and TLS support

ZixGateway

ZixGateway provides a secure and private channel for email communications between an organization and its customers and business partners. With ZixGateway, companies leverage the policy-based email encryption to **automatically scan outbound emails** for sensitive information, preventing security breaches caused by user errors and **meeting compliance requirements**. ZixGateway is the only enterprise email encryption solution to offer fully transparent email communication for the sender and recipient. When a ZixGateway customer sends encrypted email to another ZixGateway customer, the email is delivered securely without any additional effort from the sender or the recipient.

ZixGateway provides company-wide security with automatic content filtering and management of outbound corporate email. ZixGateway automatically encrypts sensitive data and determines the most efficient way to deliver messages using the **ZixCorp Best Method of Delivery**.

Requirements & More Information

You must have the ability to redirect your outbound mail to use ZixCorp Email Encryption. It is also required to have a version of Google Message Security & Compliance Solution (Postini) to use ZixCorp Email Encryption. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

ZixDirectory

ZixCorp's unmatched Email Encryption Service allows customers to **communicate seamlessly and securely**. Each ZixCorp customer is enrolled in the ZixDirectory, our global repository with more than **23 million members**. With ZixDirectory, customers eliminate the need to build their own directory of encryption keys to communicate securely with their partners and customers. ZixCorp's Email Encryption Service is easy-to-use and is the leading encryption service in the industry today.

ZixCorp provides email encryption services to WellPoint, Humana, the US Securities and Exchange Commissions (SEC), and more than 1,200 hospitals and 1,300 financial institutes.





What is IronPort Email Encryption?

Cisco IronPort Email Encryption overcomes the problems of earlier encryption technologies by providing a solution that meets compliance requirements for email encryption, while delivering powerful new email control features. The advanced technology allows organizations to improve their security and transparently protect users from the latest Internet threats.

Cisco takes the burden out of encryption key management through a hosted key management service. The Cisco Registered Envelope Service provides secure and transparent management of encryption key creation, distribution, and retention. Operating from multiple Cisco data centers, this service has high availability and 10-year key retention.

Cisco IronPort Email Encryption technology revolutionizes email encryption – satisfying compliance requirements while providing opportunity to extend into areas that can add tangible business value. Cisco provides the only email encryption technology that combines universal accessibility (send and receive on any email platform) with ease-of-use (no client software or PKI), and is proven in mission-critical deployments of up to 30 million recipients.

Features & Benefits

- Administrator Configured Policies (lexicons)
- Keywords or Phrases
- Email Client Plug-In (encryption on-demand)
- Meet regulatory requirements such as PCI, HIPAA, SOX, GLBA, as well as state privacy regulations and European directives.
- No training for end users
- No software to install

Opportunistic TLS

Servers attempt to negotiate a TLS connection with recipient servers but resort to a non-TLS connection if they are unable to make a secured TLS connection. If they are able to establish a TLS connection message are sent completely encrypted but arrive in the recipient's inbox in plain text with no further action needed to decrypt.

Requirements & More Information

You must have the ability to redirect your outbound mail to use ZixCorp Email Encryption. It is also required to have a version of Google Message Security & Compliance Solution (Postini) to use ZixCorp Email Encryption. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

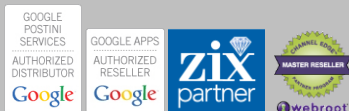
POWERFUL EMAIL CONTROL

Flexible Sender Encryption

The sender can initiate encryption through a wide variety of means, including installing an email client plug-in that allows them to encrypt a message with the click of a button, marking the message as urgent, or using a keyword (such as "encrypt") in the subject line. Emails can also be encrypted automatically through administrator-configured policies or Lexicons.

Support for All Email Platforms

Messages encrypted using Cisco IronPort Email Encryption can be opened by any AOL, Yahoo!, Gmail, or Hotmail user, as well as by traditional enterprise email clients such as Outlook, Lotus Notes, and Groupwise.





What is EXM Email Continuity?

Email continuity guarantees you that you will have 24x7x365 instant access to your email, even during a server outage. All inbound emails that you receive are stored on our backup server so in the event of a server outage, you will have a webmail portal that you can log into and send & receive new emails. As soon as your primary server comes back online, all new emails that were received during the outage event will sync up with your server so that all received emails will be available on your primary server. Continuity will work with most email environments. It is always on, always current & you will not lose productivity while your primary server is offline.

EXM Email Continuity Allows You To...

- Develop a complete email continuity and disaster recovery solution for your organization
- Maintain constant email access for users round the clock, even if your Exchange server is not available
- Minimize the risk of data loss due to on-premise server failures

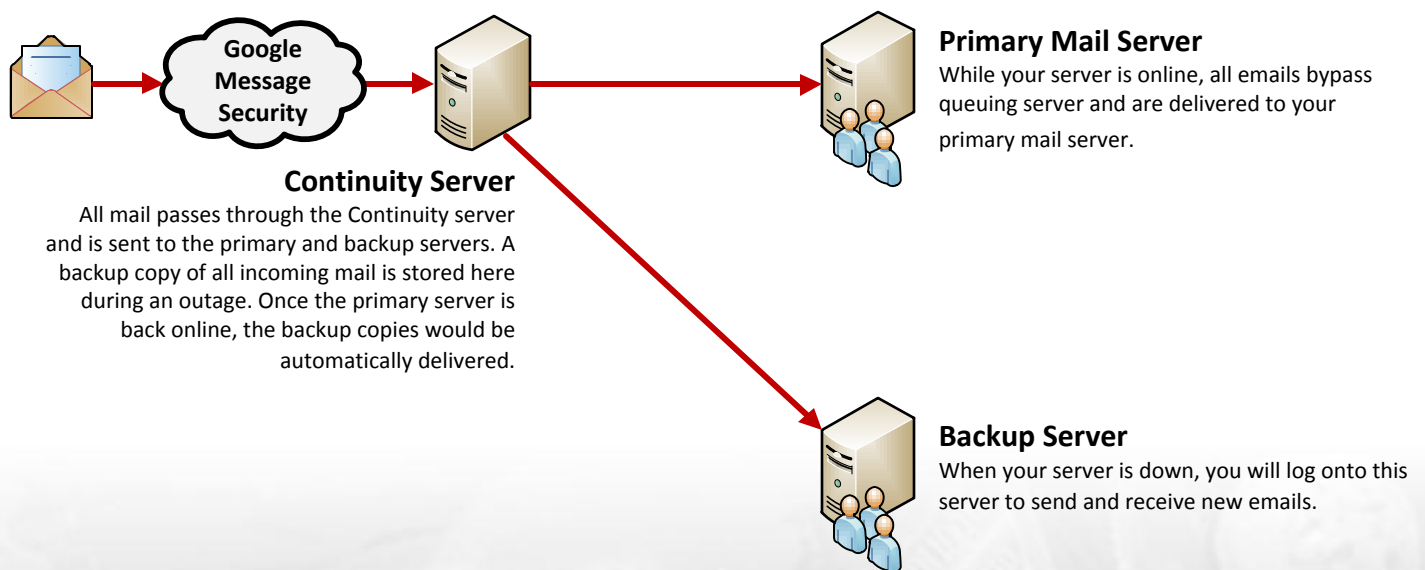
AVAILABLE EDITIONS

Enterprise Edition

Enterprise Edition of email continuity will give you the same functionality as the Standard Edition, but it will also give you 20 days of email retention on the backup server. During a server outage you will be able to access the previous 20 days worth of received emails on the backup server. All emails are purged from the backup server 20 days from the date received.

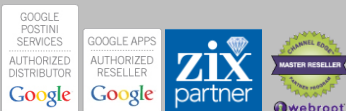
Standard Edition

Standard Edition of email continuity will give you 24/7/365 access to your email during a server outage. Email will only be stored on the backup server while your server is offline. As soon as your server comes back online, all new received emails will sync with your server and be purged from the backup server.



Requirements & More Information

Excel Micro's EXM Email Continuity requires either a Google Message Security or Google Message Discovery account. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.





What is Webroot Web Security?

Webroot® Web Security SaaS (Software-as-a-Service) provides proactive Web security that blocks threats in the cloud — before they ever reach your network. With no hardware or software to manage, a lower total cost of ownership and better protection against viruses, spyware, phishing attacks and inappropriate online usage. Webroot also guarantees 99.99% service availability to ensure that customers have consistent, reliable access to a secure web communications environment.

Web Threat Protection

- Webroot Web Security SaaS scans all HTTP and FTP over HTTP requests for viruses in the cloud, blocking threats before they ever reach an organization's network. Best-of-breed antivirus protection guarantees defense against 100% of known virus threats, and a zero-hour heuristic filter protects against new and unknown virus variants. Antispyware protection is powered by the industry's leading antispyware engine, Webroot Spy Sweeper, which protects over 10 million desktops worldwide. Anti-phishing detection is provided using advanced heuristics to identify phishing sites in real-time, ensuring sensitive personal and corporate data remains secure.

URL and Web Content Filtering

- Web content filtering enables the ability to enforce company Internet use policies, mitigate data loss, protect users from inappropriate content and improve productivity. Webroot filters web content based on website URL, web application, attachment type and file size. Millions of URLs are categorized into 12 main categories and 96 subcategories.

Internet Access Control

- Internet access policies can be set according to group or individual user level and applied by time and location. Administrators can also set website access to be "Allowed," "Blocked" or "Coached" in order to help inform users and manage Internet use.

Requirements & More Information

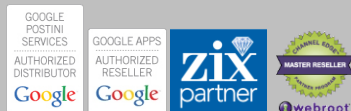
For more information on Webroot Web Security SaaS visit www.excelmicro.com/services/web_security. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

ROAMING USER PROTECTION

Webroot Web Security SaaS provides seamless enforcement of company Internet use policies regardless of where an employee is working — whether it's at home, the airport, a hotel or an Internet café. Mobile laptop users receive automatic and uninterrupted protection even while they are outside their organization's network. Because the Webroot service sits in-the-cloud, laptop users can authenticate directly with the service rather than establishing a VPN connection to the corporate network. This roaming user protection improves employee productivity and enhances network security.

REAL-TIME LOGGING & REPORTS

Real-time logs display which sites and downloads users have attempted to access and whether or not they were allowed. Detailed reports can be run ad-hoc or scheduled, allowing companies to accurately monitor Internet use by viewing graphs on web traffic trends, top blocked URLs, blocked malware, bandwidth use and more. Scheduled reports can contain up to 100 separate charts for maximum visibility into company and user Internet use.



Contact Us

www.ExcelMicro.com – Visit us on the web anytime for product information, our live webinar schedule, and to see what is new and exciting at Excel Micro.

www.MSPSupport.com – Our Resource Website with; Product Information, Screenshots, Datasheets, & Demo Logins.

<https://Portal.ExcelMicro.com> – Our Partner Portal where you can view Actual Usage Reports, Agreement Details, & Place New Orders.

www.twitter.com/ExcelMicro – Follow Us on Twitter for industry news, product updates, and promotions.

www.linkedin.com/in/excelmicro – Join our network on LinkedIn.

Sales Department

sales@excelmicro.com
877-4No-Spam (466-7726) ext. 6300

Support Department

support@excelmicro.com
877-4No-Spam (466-7726) ext. 6400

Marketing Department

news@excelmicro.com
877-4No-Spam (466-7726) ext. 6320

Billing Department

billing@excelmicro.com
877-4No-Spam (466-7726) ext. 6500

