Email Server Essentials

A practical and straightforward guide when considering the best solution to meet the needs of small and medium business

alt-n technologies

Trusted Messaging Solutions

Alt-N Technologies, Ltd.
2550 SW Grapevine Parkway, Suite 150
Grapevine, Texas 76051
Phone: (817) 601-3222
Fax: (817) 601-3223
http://www.altn.com/

Table of Contents

Introduction

> *The Internet and email can enable businesses to improve communications, access information and cut costs. Used effectively they can also help you to improve efficiency, find new business opportunities and work more closely with customers and suppliers.*—Business Link

Selecting an email system to fulfill the needs of a small-to-medium business (SMB) with 5-500 employees can be easy to do by following some practical and straightforward guidelines. Choosing a productive system involves finding the best combination of security, mobility, collaboration and ease-of-use, in addition to the basic functions of sending and receiving electronic messages.

The email industry offers a variety of software and services suitable for use by SMBs. These products and services can be placed in two broad categories—in-house email servers and outsourced, hosted applications. While in-house servers almost always run on the Windows, Linux or Mac OS X operating systems, they are also available as standalone email appliances, comprised of bundled hardware and software. Outsourced email services generally provide off-site management of hardware and software, plus some basic administrative tasks, while leaving most account maintenance to their SMB customers.

Selecting the correct type of service for each business is essential. Mismatching an email system and a small business can quietly and quickly grow into a wasteful expense. In an extreme case, a poorly matched messaging system can even cost more than the value it provides. The need to thoughtfully choose a system applies to both in-house servers and hosted services, with each having its own advantages and disadvantages. Careful choice is becoming even more important as conventional email evolves into mobile and collaborative messaging, creating both deployment challenges and productivity opportunities for SMBs.

The current design of some email systems make them difficult to use for SMB applications. For example, while some email server products are adding functions—such as support for PDAs, smart phones and team collaboration—their growing administrative complexity plus their increasing requirements for more powerful hardware and the newest operating system software can exceed the IT expertise and budgets of smaller organizations. In fact, the complexity of some email servers often requires at least one full-time employee dedicated to installing, monitoring, maintaining and updating the system, adding the overhead of an employee to the other monthly capital expenses.

On the opportunities side, more developers and hosted-service providers are designing their offerings for the usability, IT staffing and economic requirements of SMBs. In addition to conventional email services, these messaging solutions provide the SMB market with the following:

- In-house mobility and collaboration servers having:
  - Minimal hardware requirements
  - Easy to use administrative interfaces for non-professionals
  - Licensing tailored for SMB needs
  - Enterprise-class security and features
- Hosted email and messaging services with:
  - Hardware support
  - Software maintenance
  - Basic administrative functions

This paper highlights some of the major considerations for selecting an in-house or hosted email solution for SMB usage. While the details of various products and services may differ, the primary factors facing SMBs when selecting an email system are:

Security—This issue is becoming extremely important for SMBs. While they have been historically less targeted by email threats and exploits, SMBs are increasingly drawing the attention of the burglars and thieves of cyberspace because of their more relaxed security practices, especially when compared to the higher level of security now in place at larger enterprises.

Mobility—With more employees being on the road, mobility is also becoming vitally important for SMBs. Anywhere-to-anywhere communications provide mobile staff with more accurate and realtime data, helping on-the-road workers stay in touch and within reach through their PDAs, smart phones or laptops.

Collaboration—Productivity almost always improves when local and remote team members interact and work collaboratively by sharing emails, calendars, contacts, task lists, notes and more. Many email servers and hosting services are now offering affordable and easy-to-use groupware collaboration tools.

Administration—For the SMB, an email server should be easy to use, requiring about the same amount of knowledge required to use a personal workstation. The email servers for the SMB should provide secure messaging, mobility and collaboration and require very little attention or intervention. They should also provide for fast and easy disaster recovery for businesses with limited IT professional support.

Email for small-to-medium businesses can be secure, mobile, collaborative and easy to use, plus affordable. It can also provide services such as wireless access, groupware collaboration, secure instant messaging, SyncML data synchronization, web mail, mailing lists and, if needed, integration with the groupware functions of Microsoft Outlook. Archiving and backing up, plus fast and easy disaster recovery procedures should also be available. While offering new and innovative features, email designed for SMBs can run on economical hardware with older operating systems, plus require little, if any, IT professional support.

The Essentials of Choosing an Email Server

Essential 1—Security

> *Small businesses are indeed the latest target for spammers. Most small businesses—unlike their big business counterparts—have less sophisticated anti-spam protection, and spammers have shifted their tactics to take advantage of an easier target.*—Business Week Online

> *Spammers adapt quickly. One day they're sending out mortgage leads using a computer server in Shanghai. The next day, they're sending pitches for Viagra using a zombie PC in Detroit. It's all part of their efforts to avoid getting caught, and to trick ISPs' spam filters into letting their messages through.*—Tom Spring, PC World

According to some analysts, email abusers are shifting their efforts to SMBs because they are perceived as being easier targets with less security for protection against threats.

The majority of email security problems originate from spam, phishing scams, viruses and other types of malicious software hidden in messages or attachments. An email system should provide multiple and diverse ways of detecting and neutralizing security threats. Also, the email software developer or hosted service provider should have an industry-recognized reputation for understanding security issues and providing effective protection for their users. Because security is a highly technical issue, SMBs should be able to trust the email vendor to configure effective defaults and then use them with confidence. This is especially important for the sophisticated security technologies used to detect and counteract spam and viruses.

While no security system is flawless, the protection provided in SMB messaging servers have in many ways surpassed the enterprise products for large businesses by including leading edge technologies. Ideally, the servers should have security defenses such as:

Outbreak Protection—As a first line of defense, Outbreak Protection provides a near-instant, zero-hour defense against new onslaughts of spam, viruses, spyware and phishing scams within minutes—and sometimes seconds—of their release on the Internet. The 'zero-hour' speed of outbreak protection analyzes Internet email patterns in realtime to detect security threats, separating them from legitimate

messages. In tests, Outbreak Protection has correctly identified more than 97%[1] of unwanted mail with virtually no errors.

Content Analysis—Content Analysis probes the internals of individual messages to detect security risks. The primary methodologies for content analysis include pattern matching, signature detection, attachment restrictions and content filtering. To achieve accurate content analysis, email servers implement various layers of threat detection technologies such as Bayesian classification, heuristic learning, sender address verification, keyword matching, virus signature identification and attachment removal.

Authentication and Access Restrictions—Strengthening the credentials required to access an email server makes unauthorized usage more difficult to achieve. Email servers should be able to do this by requiring authentication for sending messages, using strong passwords and restricting the addresses for incoming and outgoing email. Some servers can automatically restrict access through the realtime analysis and response to security-risk behavior patterns exhibited by specified senders.

Verification, Reputation and Behavior Assessment—Spammers and other online predators exhibit common behavior patterns when sending email. These detectable characteristics include using unrestricted open-relay servers, falsifying or spoofing sender identities, tampering with mail in transit and sending millions of messages each day. To identify illicit sources of email or detect altered message content, email servers should use technologies such as DNS Black Lists, DomainKeys Identified Mail, Sender ID, reverse lookups, greylisting and tarpitting. Using multiple layers of identification and behavior analysis helps detect unwanted email, without restricting the delivery of legitimate messages.

Encryption—Industry-standard Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption technologies should be part of any SMB email solution. These technologies use authentication certificates and data encryption to protect against eavesdropping, tampering and forgery.

Security measures for an email server complement desktop virus detection software and should largely eliminate email-borne threats before they reach personal workstations and laptops. Because it focuses on the primary point of entry to a business network, security deployed at the email server is usually more consistent, reliable and effective than security software implemented on personal computers.

Essential 2—Mobility

Mobility solutions allow individuals to exchange email and data from any location with an Internet or wireless connection through PDAs, Smart Phones, laptops and publicly available computers. Mobility access can satisfy the needs to stay in touch and be within reach while out of the office, making mobile workers more capable and productive by providing accurate, realtime access to data. Mobile users should be able to both receive and update changing information as it becomes available.

As practical examples, a mobility-enabled solution allows:

- Insurance agents to exchange information with their underwriters and clients
- Sales representatives to easily interact with sales support staff and customers
- Financial advisors to inform their clients about possible changes in their investment portfolios
- Doctors to stay in touch with their patients, labs and medical equipment suppliers.

Well-implemented mobility should enhance business by helping:

Speed up realistic decision making—Because mobility enables two-way, fluid data communications, decisions can be made by using the most current information available.

Improve customer service and satisfaction—Accurate and timely mobile communications can help solve problems and eliminate costly, embarrassing errors resulting from incomplete or faulty information.

[1] Osterman Research for CommTouch

Enhance resource management—Mobile email helps keep users aware of current plans and projects. When everyone on a team works with common information, there is less chance of wasteful duplication or redundant work.

Email solutions for SMBs should support mobility through secure wireless access, web mail with groupware collaboration, data synchronization via SyncML, IMAP for message access from almost any connected computer and email support for PDAs, Palms and other wireless devices.

The mobility protocols of an SMB server should favor open standards such as IMAP and SyncML over proprietary communications systems. Using open standards protocols gives the servers greater flexibility to work with a wide variety of mobile devices. In addition, mobility should work without requiring complicated administrative support.

In short, mobile access should give busy people freedom of movement while they continue to conduct their business.

Essential 3—Collaboration

From a practical point of view, collaboration through an email server encourages interaction and the exchange of ideas among separate but related parts of a business. For example, during the creation of a new product or service, email-based collaboration can bring together the requirements of customers, developers, customer service, technical support, marketing, manufacturing, shipping, billing and accounting. Collaboration helps increase productivity by improving interaction as people share their calendars, messages, contacts, distribution lists, task lists, notes and more.

Collaboration technologies in an email server should help people become more productive by enabling them to:

Schedule projects and meetings jointly—Team members can create appointments on their personal or shared calendars, using free/busy scheduling to invite others. They can also authorize others to view and alter their appointments.

Work together on email communications—Individuals can share one or more mailboxes, specifying others to view, add, change and delete both messages and message folders.

Share contact information—Users can create and share both private and public address books and distribution lists, with various levels of authority to use and update the contacts.

Centralize documentation—Employees and customers can share documents through shared and public email folders. Shared folders belong to individuals and are available only to their owners, plus others authorized by the owners. Public folders have no owner and are available to anyone with access rights. Both types of folders can contain almost any type of information. Authorized users can view and alter their contents.

Share task lists and notes—Team members can keep lists of things to do and give others access to view, add, change and delete individual notes and tasks.

Use Mailing Lists—List members can send and receive group-wide messages at any time at any email location, pooling the creative input of everyone in the group. Mail lists can be for a few or for hundreds, with controlled membership or subscription options. For reference and documentation purposes, mailing lists can be centrally archived.

Because of its collaborative nature, groupware works well for applications such as conflict resolution, idea generation, issue discussion, negotiation, planning, problem solving, analysis and design. Both common sense and common experience prove the value of collaboration through the groupware functions of an email server.

Essential 4—Easy Administration

A well-designed email service should make email tools work while otherwise staying out of the way of daily activities. Compare email to the telephone. When a user lifts the handset, they expect to hear a service-tone, and then make a call. Little thought is given to the underlying technologies allowing the call to be completed. Similarly, a robust SMB email server should provide uninterrupted messaging, mobility and collaboration services without requiring all-day attention. This allows businesses to concentrate on work without worrying about the email technology.

For SMBs, the email server software should be easy to install, configure, maintain and operate, requiring little if any IT professional help. If someone can competently use a word processor, spreadsheet or presentation software, they should be able to use the email server or hosted service. While there may be a minor learning curve, the basics should be easy, with the more customized details of email messaging being added when and if needed.

The primary maintenance required after installation should be adding, changing and deleting accounts, plus occasional software updates. From the beginning, an SMB should be able to trust the default settings of the email server, including its account and security options.

Because email has become extremely important to the daily operations of most small businesses, system backup and disaster recovery should be fast and easy to accomplish. The design and deployment of the email server should facilitate recovery within hours, at the most. To assure fast recovery, the email server should store its system data—including configuration options and account messages—in a centralized location, making it easy for manual or automated backing up. In addition the system data should be stored in safe and stable industry-standard file formats, not proprietary database structures, which are subject to data corruption. Disaster recovery should be able to be accomplished efficiently and easily from regular system backups.

To provide convenient access, the email server should offer both simple and advanced user interfaces, plus administrative access through a web browser.

Overall, email for the SMB should provide enterprise-level features without requiring heavy IT professional support.

Summary

Questions to Consider

Today, in-house messaging is available and affordable to any small or medium business, even sole proprietorships. Some specific questions to ask when evaluating messaging alternatives include:

Email Services—Does the server offer all of the basic email services: SMTP, POP and IMAP, plus web mail? Do the services support industry standard communications methods? Are files stored in industry-standard formats or proprietary databases?

Multiple Domains—Does it allow the business to set up more than one domain? Multiple domains can be useful for even the smallest businesses.

Local and Web Configuration—Does the product allow administration from both a traditional application as well as from the web? Web administration is beneficial for making quick changes, particularly from remote locations. Can users set options for their own accounts through web administration?

Account Flexibility—Can accounts be set up individually for POP, IMAP and web mail? Can the administrator configure account defaults? Can the defaults be applied to existing accounts? Does the server support alias accounts? For example, email messages sent to the 'sales@yourdomain' and 'customerservice@yourdomain' aliases are received by the 'bob.pare@yourdomain' account.

Security—What measures does the server have to automatically protect itself and account holders against spam, phishing, breaks-ins and other unauthorized use? Essentials include the industry standard DKIM, Sender ID and SPF, plus HashCash, Bayesian filtering, heuristic learning and content filtering.

Mailing Lists—Does the server offer both discussion lists and announcement lists? Can users subscribe and unsubscribe themselves?

Gateways—Can businesses set up email gateways for security and backup purposes?

Collaboration—What types of data can users share through web mail or other collaboration functions? Basics should include mailboxes, calendars, contacts, distribution lists, tasks and notes. Does the calendaring feature offer free/busy information for setting up meetings? Are there public and shared folders?

Instant Messaging—Does the server have a private instant messaging service for engaging in quick and confidential contacts as well as online group discussions?

Mobility—Does the server support Windows Mobile, Blackberry, Palm and other mobile devices? Does web mail offer an interface for the small screens of mobile devices? Is collaboration part of the mobility functions? Is SyncML available for a flexible variety of devices, not just for Windows Mobile devices?

Backup and Restore—Is the email server designed for easy backing up and restoring of configuration options, user email accounts and email messages? What is the experience of other businesses trying to restore email services following a hardware failure, for example? Does the recovery take minutes, hours or days?

Archiving—Does the server include built-in archiving with support for searching the archives?

Other Features—Businesses should also consider email servers having features that exceed common industry standards, but work cooperatively with those standards – rather than superseding them. For example, a business might need the ability to collect mail for one account from multiple separate accounts on multiple separate servers.

Requirements—Will the server run reasonably on a machine the business already owns? Will an operating system update be required? Does installation and configuration require professional help? What are the licensing arrangements? Are there artificial or technology limits on disk space usage?

In-House or Outsource?

During the days when email server software and hardware were costly, time consuming and technically demanding, outsourcing email to a professional service provider was an obvious choice for many small-to-medium businesses because of the benefits—no startup capital costs, predictable monthly fees and little, if any, need for IT professional staffing.

With some email software now designed specifically for small-to-medium businesses, in-house hosting is a practical, affordable and secure solution for many organizations, regardless of their budget and IT expertise.

The table on the next page compares hosting with in-house email.

Characteristic	Hosted	In-House
Startup Costs	Hosted email offers low upfront costs.	Startup costs for in-house email include computer hardware and software, plus installation time.
Monthly Expenses	Fees continue monthly, with possible add-on costs for multiple domains, added accounts, account aliases, disk space usage, IMAP access, email volume, bandwidth usage and others.	One-time startup costs are usually followed by immediate and dramatic drops in monthly expenses. Fees can occur for additional account licenses.
Administration	Hosts take care of software installation and maintenance. Customers often add, change and delete their own accounts.	Email software designed for small-to-medium businesses is easy to install and maintain, including account management and security.
Hardware Maintenance	The host company maintains email server hardware.	Email servers often run on an existing computer. Today's hardware is reliable, requiring minimal maintenance.
Message Security	Confidential email is stored at the host location, often on shared systems with email for other businesses and with other open services such as Telnet and FTP, making email vulnerable to tampering, deletion and theft.	Messages are stored on a machine under the control of the business, allowing the owner to know exactly what security measures are in place and how they are configured.
Spam & Viruses	General settings for detecting spam, viruses and other email-borne security threats can make security either too tight or too loose.	Easy to use options allow businesses to control their own security settings, stopping unwanted email while making sure important messages are not accidentally blocked.
Customization Options	When customization options are available, additional fees often apply.	Businesses can set options for email, security and accounts as needed, maintaining control of their own messaging.
IT Support	The implication behind hosting is the need for professional support outside of the business.	With modern server software, most small-to-medium businesses need little if any professional assistance to install, configure and maintain email, keeping it under their control.

MDaemon for SMB Applications

> *Although free email services are convenient for sending personal correspondence, you should not use them to send messages containing sensitive information.*—National Cyber Alert System

The Windows-based MDaemon email server from Alt-N Technologies offers most of the features mentioned in this document and more. Since 1996, MDaemon has, in the words of one reviewer, "set the standards" for others to follow when it comes to providing messaging services for SMBs, and especially as an alternative

to the large and costly enterprise servers. MDaemon is designed for beginners and professionals alike, installing easily, offering intelligent defaults, and working securely, reliably and silently—staying out of the way of daily business.

MDaemon is built on the industry standards for multi-domain, web mail, groupware collaboration, IMAP, POP3 and SMTP services, plus mobile communications and SyncML. It also offers complete account management, including an optional non-intrusive link to Active Directory for managing accounts. As an industry pioneer in email security, Alt-N Technologies has continually enhanced the MDaemon email server to make it an excellent platform for detecting threats and preventing unauthorized access.

For account management, MDaemon offers account data storage in flat files or company wide databases using ODBC or LDAP technology. The administrator can import and export accounts and provide self management for account holders.

The server also supports mailings list, gateways and catalogs.

Serving the international marketplace, MDaemon is localized in multiple languages, with more than 25 available for its web mail and groupware clients, plus seven for the MDaemon GUI and documentation.

MDaemon can be installed and running in minutes, often on current hardware and operating systems.

MDaemon is currently in use by health care facilities, education institutions, government agencies, financial businesses and individuals, plus more. A 30-day fully functional trial license is available for MDaemon Pro.

MDaemon Requirements

Computer with Pentium III 500 MHz (or higher) processor (Pentium 4 2.4 GHz or higher recommended)

512 MB of memory (1 GB recommended)

Typical Hard disk space required: 100MB, plus additional space for any mail to be stored

Microsoft Windows XP/2003/2000 operating systems

Internet Explorer 5.5 or higher

Ethernet Network Card

TCP/IP network protocol installed

Internet or Intranet communication capabilities.

About Alt-N Technologies

Alt-N Technologies delivers innovative, affordable and secure messaging and collaboration solutions used by businesses in over 90 countries and 20 languages worldwide. Headquartered in Grapevine, Texas, Alt-N Technologies' flagship solution, the MDaemon email server, is a Windows-based, feature-rich platform that is installed in minutes, includes a strong arsenal of security tools and requires minimal administration and maintenance.