

Securely Sending/Receiving Email Attachments

Secure File Transfer Reduces the Risk of Intercepted Information

The employees in human resources do it at work. The IT director does it at work and sometimes at home. Even the vice president of Sales does it at work and frequently on the road. They all send sensitive company information in email attachments.

Email is the main collaboration and communications tool used to conduct business today. When employees want to share files internally or with customers, partners, and others outside the businesses, they typically use email attachments. This ubiquitous use of email attachments can be a problem not only for storage, but also for administrative controls. When sensitive files leave an organization's network, administrators no longer have control over what happens to them or where they go.



Some organizations limit attachment size to alleviate the storage problem. Limiting the attachment size that can be sent through the Exchange server leaves employees to transfer larger files using other, less secure methods, which may include:

- Using personal email accounts on Yahoo, Gmail, Hotmail, or other services, which are unlikely to have the same security as internal email servers
- Copying files to a USB device to send to the recipient
- Using other web services outside of IT control to transfer files

Using personal, potentially insecure, email accounts, USB devices, and external web services can expose your enterprise to risk.

You Need Control and Visibility Into Email Attachments

Using unapproved methods introduces a lack of centralized control over files exchanged with partners and customers. IT departments can set policies regarding attachment security, but it's up to the individual employees to adhere to those policies.

If files contain data that is subject to privacy or other industry regulations, companies are required to track and audit access to those files. Ideally, the administrator wants to ensure that only the intended recipient receives the file; however, without visibility into the transfer, the administrator has no way of verifying who received the file. This lack of visibility into email attachments creates a glaring hole in security.

The challenge is to manage email attachments without hindering collaboration and productivity. If a company wants employees to use a more secure file transfer method, IT needs to make it easy and transparent.

Globalscape® Mail Express® Replaces Email Attachments with Secure File Transfer

Using Globalscape Mail Express, IT can take control of email attachments without interfering with employee productivity or file sharing. Mail Express replaces email attachments with secure file transfer, while maintaining the mechanics of the email attachment from the sender's perspective. Available as a Microsoft Outlook add-in as well as a secure web portal, Mail Express allows individuals to send attachments as they always have, while adding audit/reporting, policy-based control, and efficient behind-the-scenes storage.

When a user attaches an email using the Mail Express Outlook add-in, Mail Express automatically examines the attachment. Depending on the rules that the business has established for email attachments, Mail Express removes the attachment from the email and stores it on the secure Mail Express server. It then replaces the attachment in the email with a link to the file on the Mail Express server, and Outlook sends on the email.

Mail Express notifies the sender when the recipient downloads the attachment, and tracks/audits all file access. IT can set policies for which attachments are managed and how long links remain active, and can monitor and report on which files are leaving the enterprise.

For employees that do not use Outlook, Mail Express offers a web portal where internal users can create emails and attach files using a web browser, with the same tracking, auditing, and business rules. Also, recipients can send files back to the sender from outside the company using a web portal, ensuring secure communications and tracking from the outside in.

The power of Mail Express is that it fits easily, even transparently, into existing practices for employees.

- From the sender's perspective: Employees using Outlook just keep doing what they're already doing—attaching the files to the emails—except that they don't have to find alternative means to send large files. Additionally, senders can add extra layers of security to the file, such as requiring a password for access.
- From the recipient's perspective: The email contains a link to the file, rather than an attachment, thus freeing up the allotted email storage space. By simply clicking the link, the recipient can download the file when it is most convenient to do so. (The expiration date of the link, if specified, is included in the email.)

Mail Express fits seamlessly into existing ways of working, and adoption throughout the organization is rapid and thorough—no one has to attend training on how to use it.

Using secure file transfer instead of email attachments reduces the risk of information being intercepted or misappropriated.

- Files are uploaded and downloaded from the Mail Express server using HTTPS, replacing potentially insecure email paths.
- For sensitive files, the sender can require the recipient to enter a password when downloading the file.
- Links expire after a time specified by the administrator; senders can explicitly set a shorter expiration period, if desired.
- Recipients outside of the organization can use Mail Express's web portal to return files to the sender, reducing the use of unapproved or insecure file transfer methods, and providing the same level of audit/tracking as outbound transfers. This method provides secure file exchange with partners.

Globalscape offers an optional DMZ Gateway[®] module, which resides in the DMZ and offers secure communication with the Mail Express server behind intranet firewalls. Using this approach, no sensitive data is ever stored in the DMZ.

Email messages are a primary means for file exchange in the business world; however, email attachments have outgrown traditional email software. With growing file sizes, increased online collaboration, and escalating privacy and security concerns, businesses need more visibility and control into the files leaving their organizations.

Globalscape Mail Express helps businesses securely exchange files via email without interfering with the productivity of employees.