



ArcMail Defender is a self-contained email archiving appliance. Everything necessary to archive email is included within the Defender and there is no additional hardware or software to purchase.

After connecting Defender to the network, the Mail server is configured to send copies of all inbound, outbound and internal messages to Defender. This is called a journal process. The Defender receives copies of all messages that have been sent from the mail server's journal process and upon receipt of these messages it fully indexes and archives the *email headers*, *bodies* and *attachments* in real-time so they may be searched, viewed and retrieved with the Defender's advanced search engine. There are two processes that index the data contained within the email; the main indexer, which parses and indexes header information such as sender, recipients, subject, date, attachment names...etc. The second indexing process indexes all text within the email bodies and also opens common attachment types to index the text within those attachments.

After indexing information is stored in the database, the raw message bodies are compressed and stored in the Defender file system to improve database performance and system scalability. Each message is stored only once (Single Instance Storage) on the Defender to maximize storage efficiency.

Users and administrators may search, view and retrieve email by connecting to the Defender's web interface and logging in through its secure login interface. The Defender uses SSL and encrypts all data between itself and the user so email data does not travel unencrypted across the network. This is particularly useful in companies with multiple offices or when placing a Defender off-site in a data center for disaster recovery purposes. *Organizations may also make Defender available through the firewall so remote or traveling users can access it remotely using any web browser (including PDA devices) to search and view or restore email.* End users are able to search any email sent to or from them while administrators are able to search the entire archive for messages sent or received by any user.

The Defender administrator may choose to manage user accounts directly on the Defender, or alternatively, simply point the Defender's login authentication mechanism to use the existing Active Directory server for authentication. When using Active Directory for authentication, users logging into the Defender are authenticated by the Windows Domain Controller, eliminating the need for the administrator to have to manage users and passwords on the Defender.