



Biscom Delivery Server Architecture and Overview

Biscom Delivery Server is a Secure File Transfer solution that enables people to share confidential or large files securely. With a Web interface and Outlook add-in, BDS offers the most common methods for users to send files from their preferred interface quickly and easily. As a platform running multiple client applications, BDS meets the two major business requirements that drive companies to look for methods superior to e-mail and FTP for sending ad hoc files and folders.

The first requirement is the increasing need to send, receive, and collaborate on confidential and sensitive files and documents such as medical records, financial data, corporate intelligence, protected personal information, and intellectual property. Federal, state, and local regulations and compliance requirements are forcing additional layers of protection of confidential data, and many organizations are beefing up their security policies to deal with the increasing frequency of data breaches.

The second requirement is the increasing strictness imposed by IT administrators on existing communications channels like e-mail and FTP. Large files delivered through e-mail, and the associated attachment management problem, add up to a serious concern for IT. As an unmanaged service, FTP is difficult to lock down, track, and report on. In addition, FTP is often technically challenging for many users, putting more demands on help desk personnel.

Together, the two requirements are pushing companies into implementing a file transfer solution that is both more secure than e-mail and more user-friendly than FTP.

How Biscom Delivery Server Works

Using the Web application, a sender would sign in and initiate a secure delivery. Like a standard e-mail client, senders enter the recipients' e-mail addresses, a subject, and optionally attach one or more files. Senders can also enter a secure message that is only available to recipients once they've been authenticated. In addition to this, senders can define delivery options for collaboration, expiration, notification, and a second level password. Once sent, the files are uploaded to the BDS secure server and encrypted. E-mail notifications are delivered to the recipients and contain the notification message and a unique URL or hyperlink that is specific to the recipient and cannot be forwarded to another person. When a recipient clicks on the embedded link, he or she is redirected to a Web sign in page for authentication. Once signed in successfully, the recipient can view the secure message, download any files, and reply to the sender and attach their own files through the secure connection.



The Outlook add-in is a seamless extension for Outlook clients. A sender simply composes a standard new message and attaches files. Administrators of the BDS system can define custom policies for triggering a secure delivery from Outlook. If any server policies are matched, or if the sender chooses to expressly use BDS from Outlook, the message and attachments are re-routed through BDS, the attachments off-loaded, and the e-mail body stored as a secure message. BDS will automatically generate a notification message to the recipients. The Outlook add-in runs solely in the Outlook client, with no impact on the mail server. The add-in communicates with BDS through a Web services API to verify user credentials, query server policies, and transfer files.

Open Architecture, Flexible Platform, and Web Services API

BDS is a pure Java application and is capable of running on both Windows and Linux operating systems. BDS's three-tier architecture natively supports separation of each tier into separate physical or virtual machines. These tiers – presentation, business logic, and data – can be clustered at each level, providing high availability and increased performance. BDS uses XML heavily in the platform – not just in the Web services API, but also for importing data, communication between the various components of the product, and as a control mechanism in the SMTP interface.

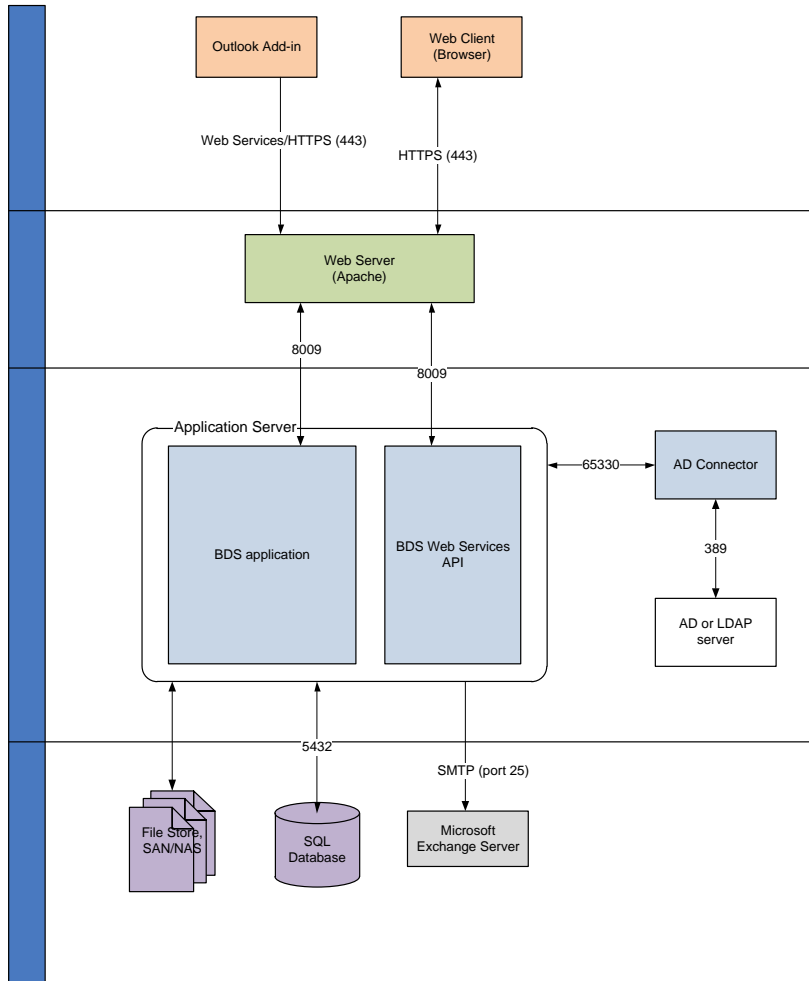


Figure 1: BDS component architecture

Security

BDS security is embedded in several levels – application, data, and network.

Application security and governance

- User authentication using an internal database or LDAP/Active Directory
- Checks for SQL injection, cross-site scripting, and buffer overflow/overrun attacks
- User roles and permissions
- Automatic delivery expiration

- User expiration
- Quotas
- File type restrictions
- Recipient inclusions and exclusions (set globally and at user level)
- Password strength requirements
- Client access to back-end and data tier through API only
- Security logic enforcement via API layer
- External user restrictions

Data and network security

- Back-end file encryption (protection for “data at rest”) using AES 256-bit encryption
- Encryption of files in transit using Secure Sockets Layer (SSL)
- Key management utilities for administrators with multiple encryption key support (Figure 2)
- Three-tier separation of presentation, application, and data layers
- Automatic file deletion/purging schedule
- Obfuscated file system keeps file names and owners hidden

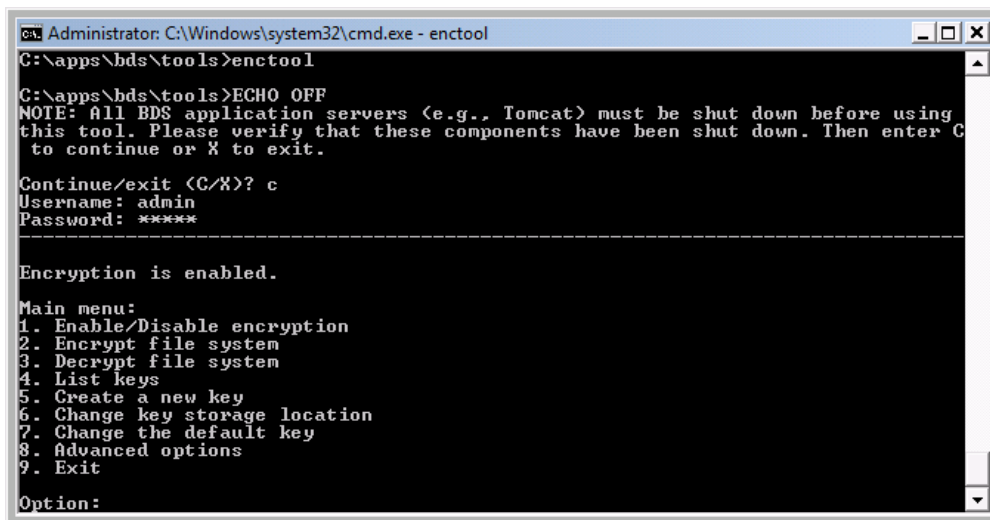


Figure 2: Encryption Tool

Files are stored using AES 256-bit encryption, the encryption algorithm ratified as a standard by the National Institute of Standards and Technology. AES was picked by NIST for its speed, as well as its support of large key sizes to reduce vulnerability from brute force attacks. Administrators can configure BDS’s encryption settings, and multiple keys can be managed from the encryption tool’s interface. Encrypting files in the file repository helps maintain internal and external security and prevents data breaches from inside and outside the company. Encryption is handled transparently by BDS, so end



users do not have to understand or cope with the complexities of private and public keys, or manually encrypt and decrypt files, when sending and receiving deliveries.

Deployment

The *three-tier architecture* provides flexible deployment of components that can better map to a company's existing security infrastructure. The *platform neutrality* of BDS enables the server to be deployed in any multiple operating environments and in multiple configurations, utilizing existing components. For example, companies may already own and have support for a Web server, application server, database, directory service, and SAN or NAS storage server. BDS easily scales from the departmental level to corporate-wide use – without IT having to worry about hardware upgrades or storage limitations – by simply updating a license key.

Since many companies already have considerable investments in networked storage solutions, Biscom chose to work with existing file storage systems natively rather than limit customers to using on-board storage or charging for a network, UNC, NAS, or SAN storage connector. BDS also supports migration from different storage locations, with only a simple configuration change necessary to point to a different location if data needs to be moved to a larger system. This flexibility enables a company to retain its backup and data retention policies without having to worry about a new storage pool to add, manage, and back up.

Virtualization

BDS runs on physical hardware platforms as well as virtual platforms equally well. Virtualization is becoming increasingly popular with companies for its convenience in deployment, elimination of hardware servers, reduction in costs associated with running hardware, and the desire for *greener* technologies. But virtualization also has additional benefits with respect to BDS. One configuration that we recommend is running the application server as a virtual machine. Taking a snapshot of a virtual BDS server provides a simple backup server in case the primary server fails. A snapshot will have all the configuration options and application policies of the primary server, and administrators can restore service in a matter of minutes. Some virtualization vendors provide hot backups and robust failover capabilities that can minimize downtime due to hardware failures. Additionally, multiple VMs can be clustered and used in a failover and load balanced configuration to increase performance as well as provide a redundant architecture for increased uptime.

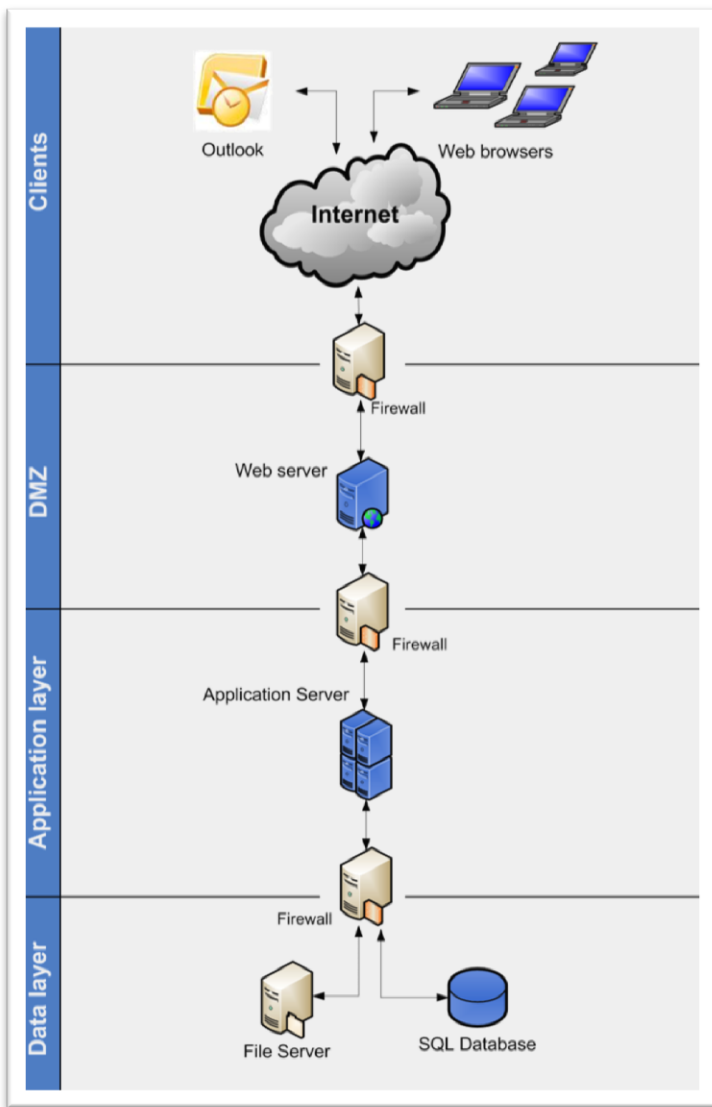


Figure 3: Deployment example

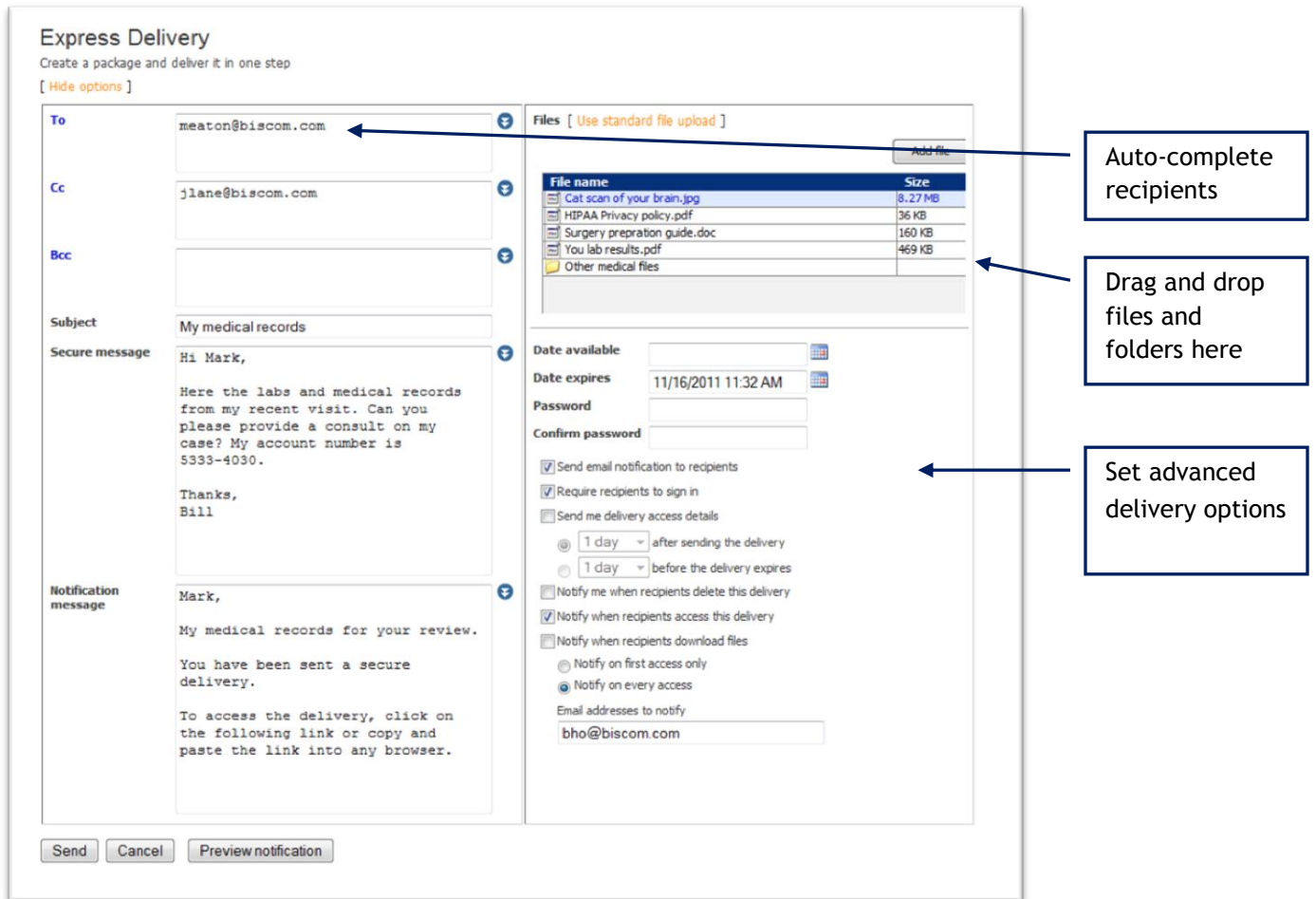
Multiple Instances

Since BDS has the capability to run multiple logically-separated instances on a single server, it can provide custom instances for specific departments or groups within an organization. Each instance can have its own copy of the database, its own data repository, and configuration options that apply solely to that instance. Moreover, the number of instances that can run on a single server is limited only by the CPU and memory of the underlying hardware platform, and the level of usage of the system as a whole.

Choice of Easy-to-Use Client Interfaces

BDS can be accessed through multiple interfaces – a ubiquitous Web interface (Figure 4) and an Outlook add-in that is transparent to the end user (Figure 5). BDS also support scripting languages so agents can be developed to automate processes such as watching folders for files, batching deliveries, and retrieving files.

All clients supports desktop-like features, such as e-mail address auto-completion, real-time integration with global address lists, drag-and-drop, and the ability to download multiple files with a few simple mouse clicks.



The screenshot shows the 'Express Delivery' web application interface. It features a form for creating a package and delivering it in one step. The form includes fields for 'To', 'Cc', 'Bcc', 'Subject', 'Secure message', and 'Notification message'. The 'Files' section shows a table of files being uploaded, with an 'Add file' button. The 'Advanced delivery options' section includes checkboxes for 'Send email notification to recipients', 'Require recipients to sign in', 'Send me delivery access details', 'Notify me when recipients delete this delivery', 'Notify when recipients access this delivery', and 'Notify when recipients download files'. There are also dropdown menus for 'Date available', 'Date expires', and 'Password', and a 'Confirm password' field. Callouts point to the 'To' field (Auto-complete recipients), the 'Files' section (Drag and drop files and folders here), and the 'Advanced delivery options' section (Set advanced delivery options).

File name	Size
Cat scan of your brain.jpg	8.27 MB
HIPAA Privacy policy.pdf	36 KB
Surgery preparation guide.doc	160 KB
You lab results.pdf	469 KB
Other medical files	

Figure 4: Web application – delivery

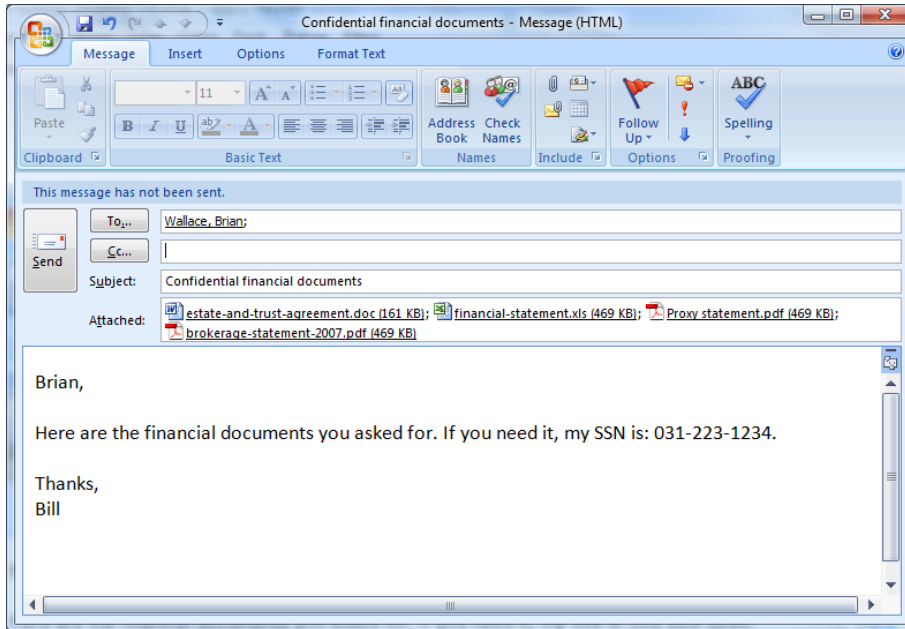


Figure 5: Outlook Add-in

The Future of Secure File Transfer

Biscom Delivery Server is deployed in many industries, including healthcare, financial services, legal, federal, state, and local government, construction, manufacturing, technology, and retail. It's clear that SFT is an important application across multiple industries and sectors, with several that have needs based on legal, regulatory, or contractual requirements.

The message we hear from our customers and prospective customers is clear and consistent: sending files securely, or sending large files, needs to be *extremely easy* for their users, or it won't be accepted and adopted. We also find that no two customers are alike in their needs – and flexibility in configuring the application is absolutely critical – whether it's customizing text, logos, colors, and fonts, or modifying the behavior of the application and setting policies for data retention, file restrictions, delivery parameters, and registration.

BDS works well as a standalone application used in a single department or enterprise-wide. Existing and legacy applications can be tied to BDS to integrate secure delivery features and extend the life of their investments. The broad and granular programming interfaces enable customers to build new applications from the ground up to solve complex and unique problems. Ultimately, SFT has the capacity to be an integral part of an organization's mission critical infrastructure, and as a service that can be used by multiple departments with diverse requirements and applications.