DataMotion SecureMail
Administration Guide

TABLE OF CONTENTS

REVISION HISTORY

This section summarizes significant changes, corrections, and additions to the document. The history appears in chronological order with the most recent changes listed first.

Version 9

Small changes to the DomainKeys Identified Mail sections were made to provide easier clarification for readers.

Chapter 1): DataMotion SecureMail Company Administration

- *DomainKeys Identified Mail (DKIM)* (*below*): Minor changes to the screenshot and the inclusion of a DNS TXT record sample showing an in place DKIM TXT record have been included to provide better clarification.

Version 8

This version documents the DomainKeys Identified Mail information.

Chapter 1): DataMotion SecureMail Company Administration

- *DomainKeys Identified Mail (DKIM)* (*below*): This new section covers the settings to configure the DKIM feature via the web portal.

Version 7

This version documents a setting that will restrict a user's methods of logging into SecureMail. This is only configurable via user type.

Chapter 1): DataMotion SecureMail Company Administration

- *Social Media Logins* (*on page 18*): This new section covers the setting to disable or enable the social media logins on the web portal.
- *Secure Contact Us* (*on page 17*): This new section describes setting up SecureContact.us.

Version 6

This version documents a simple feature which allows company administrators to enable a Group Mailbox feature in the Admin Console without the need of DataMotion Support. This setting is specifically labeled as Allow delegates to delete messages from group boxes.

Chapter 1): DataMotion SecureMail Company Administration

- *Group Mailbox Setup* (*on page 22*)
    - Changed the image in the steps to setup Group Mailbox to display the new **Allow delegates to delete messages from group boxes** setting in the Admin Console.

- n   Added the following NOTE regarding the new NOTE: The **Allow delegates to delete messages from group boxes** setting can be configured for admins to enable or disable on their own if configured by an integrator.

n   *Bulk User Import* (*on page 46*)

- n   Updated this section to include the latest screen from the Bulk User Import page which now allows an admin to select a .csv file to upload or enter the information into a text field if desired.

n   *Transfer Users to Your Company* (*on page 42*)

- n   This section was changed from its previous title Importing Existing Recipient Users. The section now includes updated screenshots which highlight the current name of the link on the Manage Users page which is now Transfer User instead of Import Recipient.

Version 5

This version documents a couple of new features such as the capability to disable email address editing as well as the Group Mailbox functionality. Both of these features have their own sections in the document.

Chapter 1): DataMotion SecureMail Company Administration

- n   *Disabling Email Edit* (*on page 21*): Added this new section describing how to disable the capability of users to edit their email address on the web portal.

- n   *Group Mailbox Setup* (*on page 22*): Added this new section to describe how to enable the Group Mailbox feature for users within a company. The instructions are mostly for on-premise users since the Company Properties need to be accessed to enable the feature.

- n   *Safe TLS Properties at the Company Level* (*on page 24*): Changed the screenshot of the company level settings to reflect the new changes made to the description as well as the added DISCLAIMER.

- n   *Group Mailbox Access Report* (*on page 53*): Added this section to the Reports section of the document. This section describes how to run a Group Mailbox Access Report and its specific use towards only Group Mailboxes.

Version 4

Documented new features including the capability for administrators to import recipient users into their companies, and the Safe TLS delivery features that are now available. Document wide changes were made in order to remove the Galactic Seats company and replace it with the Your Organization sample company.

Chapter 1): DataMotion SecureMail Company Administration

- n   *Transfer Users to Your Company* (*on page 42*): Added this new section describing how administrators can bring recipient users into their companies as either SecureMail 500, SecureContact US, or SecureMail 500 Admin users.

- **_Safe TLS Configuration_** (_on page 24_): Added this new section to highlight the available features of Safe TLS and inform on-premise admins that they can change and alter these settings at will.

- **_DataMotion SecureMail Email Flow via the Web Portal_** (_on page 16_): This new section contains identical information from the previous section titled DataMotion SecureMail Email Flow.

- **_DataMotion SecureMail email Flow via Safe TLS_** (_on page 16_): This new section describes the email workflow when Safe TLS is enabled.

- **_Company Configuration_**: Removed this section from the document as it does not apply to the information being provided.

  » Instead this section has been moved to the On-Premises Administration Guide since only on-premise customers can access these settings themselves.

Chapter 2): DataMotion SecureMail Integration with Typical Environments

- SendSecure Button for Microsoft Outlook: Group Policy Network Installation: Removed this section from the document as it references an outdated procedure.

  » Added this section as an example procedure to the DataMotion SecureMail for Outlook Quickstart Guide. The information will remain there until a newer installation example can be set up and provided. Please note that there are many ways to install the Outlook plugin, and that this procedure was not the single required method.

- **_SendSecure Button for Microsoft Outlook: Installation with Citrix/Terminal Services_** (_on page 60_): Added information regarding the need to change the DMConfig.xml file from the default "tagging" DMConfig.xml to the "desktop encryption" version of the DMConfig.xml file.

Version 3

Documented new features including company hierarchy administration, which supports administration of a company tree structure, allowing administrators to manage users for tenant companies.

Chapter 1): DataMotion SecureMail Company Administration

- **_Moving Existing Users_** (_on page 44_): Added this new section describing how administrators can move existing users to tenant companies and among tenant companies.

- **_Who Sets up a Cobrand?_** (_on page 28_): Updated this Cobranding section to highlight the ability for administrators to set up cobrands.

Version 2

Chapter 1): DataMotion SecureMail Company Administration

Added new information on Company Cobranding:

- *Company Cobranding* (*on page 17*).

- *Cobranding the Web Portal* (*on page 27*).

Added new description of the differences between Administrators who perform Company Administration and Super-Administrators who perform Multi-Company Administration:

- *DataMotion SecureMail Administration Levels* (*on page 19*).

Version 1

Initial version of this document. This document assembles content from previously published documents. Information in this document was previously published in the following documents:

- *DataMotion SecureMail Administration Guide* (last published August 27, 2012) has been incorporated into Chapter 1, "*DataMotion SecureMail Company Administration*."

- *SendSecure Button for Microsoft Outlook: Group Automatic Distribution via Group Policy Management* (last published October 27, 2011) has been incorporated into Chapter 2, "*DataMotion SecureMail Integration with Typical Environments*."

- *SecureMail for Lotus Notes Installation Guide* (last published October 27, 2011) has been incorporated into Chapter 2, "*DataMotion SecureMail Integration with Typical Environments*."

- *DataMotion eForms Overview* [AppNote] (last published December 15, 2011) has been incorporated into Chapter 3, "*SecureForms Standard*."

- *DataMotion eForms Cookbook* [AppNote] (last published August 21, 2012) has been incorporated into Chapter 3, "*SecureForms Standard*."

About This Publication

ABOUT DATAMOTION SECUREMAIL

This publication describes how to manage DataMotion SecureMail.

DataMotion SecureMail provides easy-to-use encrypted email messaging and data transfer via the Internet for protecting all of the important information flowing between you, your business partners and your clients.

SecureMail protects sensitive messages with military-grade encryption, and it allows users to send secure messages and files using one click, with built-in tracking of all messages and files sent, received, and opened. It works with popular email clients such as Microsoft Outlook, as well as on the iPhone and other mobile devices, and it is intuitive for senders and recipients, so it can be up and running in minutes with no outside IT support. With integrated large file support, DataMotion SecureMail seamlessly delivers documents, images, and other large files, eliminating a significant bottleneck in data exchange.

Providing effortless secure sending from email clients and direct delivery to the recipient's inbox, plus the ability to transfer large files easily from desktop clients or mobile devices, DataMotion SecureMail offers exceptional flexibility, capability, and user experience.

INTENDED AUDIENCE

This publication is intended for a technical audience, including system administrators and system integrators, primarily those who are responsible for the management of DataMotion SecureMail. They are not expected to be security experts, but knowledge of security policies and email is helpful.

Additional technical documentation, as well as user documentation, is also available from DataMotion. See *DataMotion Documentation* (on page 14).

DATAMOTION SECUREMAIL PLATFORM OVERVIEW

The following information describes the DataMotion SecureMail platform, including the components of the User Interface (for end-users) as well as the System Interface (for developers).

While an understanding of the DataMotion SecureMail platform is not needed to use the product, this broader picture of DataMotion SecureMail may interest those who like to understand the larger context for what they are doing.

DataMotion offers a technology architecture in DataMotion SecureMail that is mature, robust, scalable and time-tested. The following **DataMotion SecureMail Platform Block Diagram** shows the DataMotion SecureMail User and System Interfaces (a description follows the diagram).

DataMotion SecureMail Platform Block Diagram

DataMotion SecureMail

User Interface	DataMotion Platform	System Interface

User Interface

Webmail Portal

Mobile / Tablet	Desktop

Provider Directory & Address Book

Email Client Integration

Mobile / Tablet	Desktop Clients

File Transfer

Portal	Drag & Drop

Inbound Contact

eForms	Messages

System Interface

Management Console

Provisioning	Settings	Reporting

Management APIs

Provisioning	Settings	Reporting

Data Transport

Messaging APIs	File Transfer APIs	Protocols

Embedded Webmail Client with SSO

Email Compliance Filter

PHI, Lexicons, Pattern & Exact Matching

The left side of the diagram shows the **DataMotion SecureMail User Interface**. The User Interface has been designed for simplicity and ease so that end-users can accomplish the secure transport of messages and data in the quickest way possible. The User Interface components of the block diagram represent the principal aspects of the system as experienced by users. This includes:

- A Webmail Portal and Email Client Integration for sending and receiving secure messages
- SecureFileTransfer for sending files securely (including large files), and
- Inbound Contact for enabling secure incoming messages and data from any person.

The *DataMotion SecureMail Administration Guide* contains instructions on using the Webmail Portal, Email Clients, and SecureFileTransfer. The information on using Email Clients is divided into categories specifically describing how to use tablets, smartphones, and desktop clients such as Microsoft Outlook*.

Although not addressed in this manual, the right side of the diagram shows the **DataMotion SecureMail System Interface**. The System Interface has been designed for partners, developers, system integrators and administrators so that they can quickly and easily deliver Secure Messaging and Data Transfer to their clients and customers.

PRODUCT TERMINOLOGY

Because the various technology components shown in the *DataMotion SecureMail Platform Block Diagram* have been time-tested, they have acquired synonyms in the documentation that are useful to know.

The following table provides synonyms that you may encounter for some of the **User Interface** components. The synonyms may refer to the component or an identifiable part of the component.

Synonyms for User Interface Components

Component	Sometimes Referred to as:
Webmail Portal	Web Portal, DataMotion SecureMail Portal
Email Client Integration	SendSecure Button, Desktop Client Program, Email Client Add-In
Electronic Forms	eForms, SecureForms
Inbound Contact	SecureContact and SecureContactMe

HOW TO USE THIS PUBLICATION

The *DataMotion SecureMail Administration Guide* contains detailed information on the integration, maintenance, and administration tools provided by DataMotion to companies implementing and customizing DataMotion SecureMail.

The chapters are written independently and can stand alone to minimize dependencies between them. The content is organized as follows:

About This Publication.
> Provides an overview of the content of this publication and how to use the publication.

Chapter 1) DataMotion SecureMail Company Administration
> Describes how to manage your DataMotion SecureMail accounts, including how to use the Admin Console tools for report generation, cobrand creation, and user administration (e.g., adding, changing, or deleting users, setting user type privileges, managing passwords, and managing security questions).

Chapter 2) DataMotion SecureMail Integration with Typical Environments
> Describes how to integrate DataMotion SecureMail in some typical environments, including step-by-step instructions for installing the SendSecure Button add-in, which allows users to send secure messages from within their normal email interface.

Chapter 3) SecureForms Standard
> Describes how to create DataMotion SecureForms Standard, including PDF and HTML SecureForms, and how to access SecureForm data.

RELATED INFORMATION

DATAMOTION DOCUMENTATION

- *DataMotion SecureMail Software Development Kit Reference Manual* (part # 050030)
  Documents the Application Programming Interfaces (APIs), and system development, maintenance, and administration tools for developers.

- *DataMotion SecureMail User Guide* (part # 050006)
  Provides instructions for using the products including setting up SecureMail on mobile devices, and using the features of the web portal itself.

Additional documentation is available on many other topics. Please contact DataMotion Customer Service for more information.

1
DataMotion SecureMail Company Administration

DATAMOTION SECUREMAIL FEATURE OVERVIEW

DataMotion SecureMail provides secure email delivery with integrated tracking. Designed to easily fit into existing work flows, DataMotion SecureMail leverages standards-based technology such as SMTP, SSL, TLS and AES encryption to ensure compatibility with how you work and while providing maximum security.

DATAMOTION SECUREMAIL FEATURES

DataMotion SecureMail is a highly flexible platform which can provide a variety of secure transport services for your organization. Using DataMotion SecureMail, your organization can securely send emails, files and forms as well as have outside organizations or even customers securely contact you.

A short list of features available to you through DataMotion SecureMail is:

- Secure email delivery
- SecureContact.me to allow anyone to send inbound secure messages to your users
- No software is required by the recipient
- Web Portal for sending, receiving and tracking messages
- Customization of the Web Portal with company cobranding for a branded user experience
- Multiple delivery methods for secure emails including web notifications, TLS plain text, and encrypted PDF attachments
- Large attachment delivery outside the limits of your mail servers
- Message tracking including when it was delivered and when it was opened
- Automatic message expiration
- Secure replies from recipients

DATAMOTION SECUREMAIL EMAIL FLOW VIA THE WEB PORTAL

The basic flow of messages through DataMotion SecureMail does not differ much from the flow of messages without DataMotion SecureMail. Messages can be sent to the system through a variety of interfaces depending on your needs and use and can also be delivered through multiple mechanisms.

In general, the message flow when using DataMotion SecureMail is as follows:

1. The message is sent to the DataMotion SecureMail service.
2. The message is processed, and the recipient list is determined. For recipients that do not already have DataMotion SecureMail accounts, a "recipient" account is created for the user.
3. The message is placed in the Inbox for each recipient.
4. The recipients are sent notifications that a new message has been securely delivered to them.
5. The recipients follow the embedded link in the notification message to access the Web Portal to read the message. First time recipients are enrolled when they come to the portal for the first time.
6. Tracking information is recorded for the sender when the message is delivered and read.
7. The sender is sent a receipt that the message has been read.

DATAMOTION SECUREMAIL EMAIL FLOW VIA SAFE TLS

The availability of the Safe TLS feature for DataMotion SecureMail causes the general workflow of sending a secure email to differ from the original workflow stated above. The key difference being the web portal is not included in this workflow unless the recipient cannot receive recipient connections. Also, this workflow only applies when the Safe TLS features are enabled for a tenant company.

1. The message is sent to the DataMotion SecureMail service.
2. The SecureMail service checks whether the recipient's mail server accepts TLS delivery. If it does, the message is delivered in clear text with an HTML footer stating that the message has been securely delivered.
3. Tracking information is recorded for the sender when the message is delivered and read.
   » Should the recipient be unable to accept inbound TLS connections, the footer can be used to click a link sending the recipient to login to the web portal.
   » At this point the workflow will proceed as highlighted in step 5 of the DataMotion SecureMail Email Flow via the Web Portal

SECURECONTACT.ME

SecureContact.me is a feature where someone can send you a new secure message, not just a reply to one you have sent. This feature is available for all your users and provides a simple

method for someone to securely send new inbound messages that are not replies to previous ones.

SecureContact.me works by providing each user with a simple, unique URL in the form:

`https://securecontact.me/jsmith@yourorg.com`

This URL can be placed into an email signature, on a business card or a profile page. When someone clicks on the link they will be taken to a page where they can send a new secure message directly to the specified email address, but to no one else.

Each user will have a SecureContact.me link under their **My Account** heading in the Member Center. When they click on this link it will generate the specific URL for that user and provide them with information about how to copy and use the link.

SECURE CONTACT US

All Secure Contact Us setup is performed via setting up a company Cobrand (see the *Cobranding the Web Portal* section for information regarding a cobrand) and providing a special link to recipients. Once your cobrand is setup take note of the cobrand name which is in the parenthesis next to the drop-down at the top of the Cobrand Console page.

Cobrand Console

▼1. Cobrand Information

	Your Organization (15734) ▼
Company Name:	Your Organization
Default URL:	

Once you have the Cobrand name all you need to do is place the Cobrand name at the end of the following URL:

`https://ssl.datamotion.com/register/cureg.aspx?cb={cobrand_name_here}`

COMPANY COBRANDING

Company Cobranding is a feature of DataMotion SecureMail that allows an organization/company to place its brand identity on the DataMotion secure messaging portal. The simplest cobranding can include a company logo (with a hyperlink on the image), a custom color, and other options. You can also use HTML coding in place of the image for advanced cobranding customization.

Cobranding can reinforce one's brand identity, as well as provide a familiar look and feel that encourages adoption of DataMotion SecureMail by employees and customers.

See *Cobranding the Web Portal* (on page 27) for detailed information.

SOCIAL MEDIA LOGINS

Users may be presented with the option to utilize single sign-on options to login to their SecureMail accounts on the platform. These include the following identity providers:

- Google
- Facebook
- LinkedIn
- Microsoft

This might not be desirable for all companies and a method to disable these types of logins is available.

This can be further broken down for the users within the company on a user level for each user type within the company. Since this setting is configured by user type it should be noted that any users outside of the company such as recipients will have all sign-in options available (this can be changed if you have an on-premise installation).
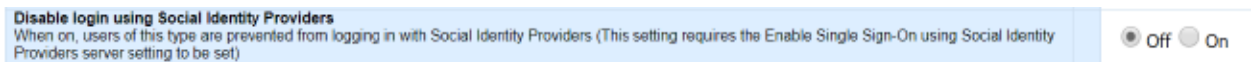
NOTE: This setting may not be available to all administrators and may require DataMotion support to configure. Please contact support in the event that you need to have this setting configured.

NOTE: For any users that utilize the DataMotion SecureMail for Microsoft Outlook plugin it is required that they create a password to use the button. Your users can find this information in the DataMotion SecureMail User Guide under the section Creating a Unique Password.

NOTE: The NOTE above applies to any usage of the API or the SecureMail Adapter as well.

DATAMOTION SECUREMAIL COMPANY ADMINISTRATION OVERVIEW

DataMotion SecureMail **Company Administration** allows you to manage the DataMotion SecureMail accounts for your company or organization.

For the difference between Company Administration and Multi-Company Administration, see *DataMotion SecureMail Administration Levels* (on page 19).

EXAMPLE COMPANY

Throughout this publication, a fictitious, example company called Your Organization is used to illustrate how to perform administration, including cobrand creation, user administration, and report generation. This company is to be considered a template company for the administrator to use. So wherever "**Your Organization**" is seen, that means their actual company's name would be displayed, and whenever "**@yourorg**" is seen that symbolizes email addresses where their company's domain would be.

DATAMOTION SECUREMAIL ADMINISTRATION LEVELS

There are two levels of DataMotion SecureMail administration used by different types of customers. Although the majority of customers perform Company Administration, some larger customers have contracted with DataMotion to oversee the administration of multiple companies. This higher level of administration is referred to as Multi-Company Administration.

Company Administration refers to the management of DataMotion SecureMail for a single company. It provides company *Administrators* with tools for user administration, cobrand creation, and report generation. The company may be an autonomous business entity, or it may represent a division, branch, department, business unit, subsidiary, affiliate, etc., that is associated with a larger organization. The information in this chapter primarily describes Company Administration.
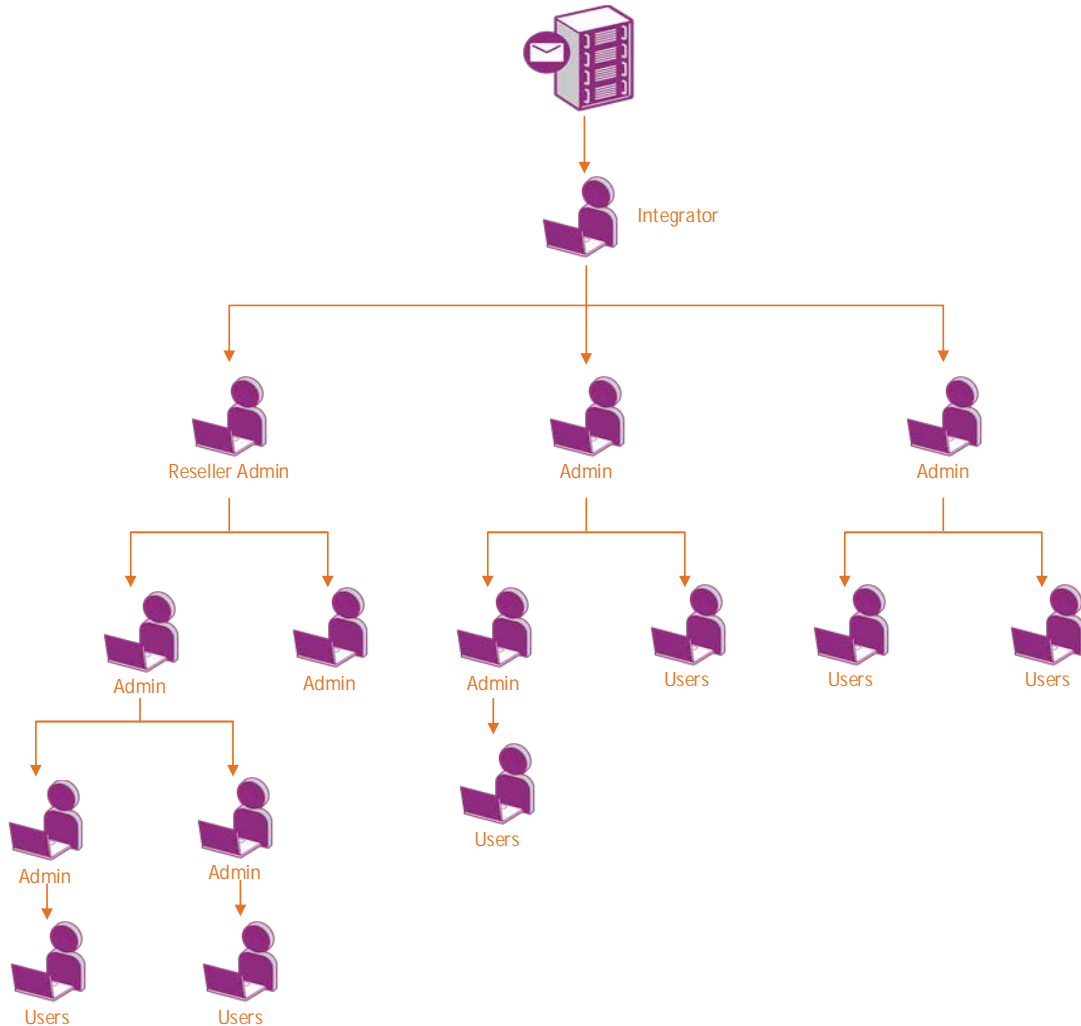
Multi-Company Administration refers to the management of DataMotion SecureMail for multiple companies or organizations. It requires a higher level of authority to perform Multi-Company Administration. Typically, Multi-Company Administration can be performed by a DataMotion partner or a larger corporation under special agreement with DataMotion. This central "landlord" company manages the DataMotion SecureMail accounts for the "tenant" companies or organizations it serves. In DataMotion SecureMail administration, the landlord company is also known as the **Default Company**.

The **Default Company** is actually the top-level company on the DataMotion SecureMail server under which all other companies or organizations are created. The administrator of the default company manages the settings for the company and also has the ability to create and maintain subordinate companies, among other things. It's also important to note that a company can only have one parent company, while the parent company can have multiple child companies.

The information in this chapter documents the administrative tools used by DataMotion SecureMail administrators for Company Administration.

Administrators can manage users within their own company, and if a company hierarchy exists, they can also manage users for tenant companies, including moving existing users to tenant companies and among tenant companies. For more information, see the following diagram and

Moving Existing Users (on page 44). Administrators also possess the capability to import their company's recipient users into the company tree. For more information, and the steps to perform this action see the *Transfer Users to Your Company* section on page 42.

DataMotion SaaS

USER TYPES AND PRIVILEGES

DataMotion SecureMail Company Administration is primarily focused on user administration. Your company account will feature several user types with unique privileges based on the services you have purchased.

The **User Type** is how privileges, permissions, capabilities, and configurations are assigned. Based on the set of services your organization has purchased, DataMotion will provision several User Types into your company account. Each User Type is identified by a descriptive name.

When you assign users to a specific User Type, they will receive the privileges and configurations established by DataMotion for that User Type. A user can only be assigned to a single User Type, but DataMotion can work with you to make adjustments to your User Types if your users need different capabilities than what has been provided. (If the DataMotion SecureMail account for your company is managed by a corporate parent or a DataMotion partner, their admins will also be able to manage your User Types.)

There is always one User Type with administrative capabilities. Typically, it is named "Admin" or has a name that ends in "Admin." Only users assigned to an Admin User Type will be able to access the Administration Tools described in this publication. Admin users have the ability to manage users and use the cobranding and reporting tools.

ADMINISTRATIVE TOOLS

The administration of your company account is performed through the links shown in the Admin Console area of the Member Center. Only users who login with Admin privileges will see the Admin Console.

Member Center

SecureMail 500 Admin: <jsmith@yourorg.com>

▼Messages & Files	▼My Account	▼Download Console
Compose	Address Book	Client Downloads
Track Sent	User Information	
Inbox	Preferences	▼Admin Console
Drafts	SecureContact.me	Administrative Tools
Folders		Security Questions

The Administrative Tools will always be available for the Admin. The Security Questions will only be available if this has been turned on for your company.

DISABLING EMAIL EDIT

By default it is possible for users to edit their email address that they use to login to the portal with. For some companies this is not desirable and as a result it can be disabled with a simple request to the DataMotion Support staff or for on-premise users, editing the company properties.

1. From the Member Center click on the **Administrative Tools** link.
2. Click the **Administer your corporate accounts** link.
3. Click the 📧 icon next to your desired company to enter Company Configuration.
4. Click the **Company Properties** link in the box on the left side of the page.

5. Scroll down to the **Users** section.

6. Click the On radio button on the right of the **Disable email address editing** feature.

To ensure that the setting is on, go to your User Information and take note that the Email Address field is no longer a text box, but a static label as shown below.

GROUP MAILBOX SETUP

By default, the options for Group Mailboxes are not fully enabled by default. A request will have to be put in to the DataMotion Support staff in order to have the feature enabled. For on-premise based customers the instructions provided below describe how to enable the feature through the admin console.

1. From the Member Center click on the **Administrative Tools** link.
2. Click the **Administer your corporate accounts** link.
3. Click the ⬚ icon next to your desired company to enter Company Configuration.
4. Click the **Company Properties** link in the box on the left side of the page.

Company Configuration

Company Information

Company Properties

User Types

Full User

Recipient User

Certified Gold Admin

Integrator

Summary

5. Scroll to the bottom of the page to find the **Group Mailbox** fields.
6. Click the On radio button to enable the Group Mailbox features desired.

Group Mailbox		
Use Group Mailbox When on, users will be able to use the Group Mailbox features from the links on the Member Center	*	○ Off ● On
Group Mailbox owners can add delegates from other companies When on, group mailbox owners will be able to add delegates who are not in their company.	*	○ Off ● On
Group Mailbox delegate status track sent visibility When on, senders who send to group mailboxes will be able to see the individual delegates' status in the messages in Track Sent items.	*	○ Off ● On
Allow delegates to delete messages from group boxes When on, Group Mailbox delegates will be able to delete messages from the Group Mailbox.	*	○ Off ● On

NOTE: For the Group Mailboxes to appear on the Member Center at all it is critical to set the Use Group Mailbox setting to On.

NOTE: The Allow delegates to delete messages from group boxes setting can be configured for admins to enable or disable on their own if configured by an integrator.

7. Scroll to the top of the page and click the Save button to confirm the changes.

The completion of these steps will cause the Group Inboxes link and the Group Mailbox Configuration link to appear on the Member Center of all users within the company.

Member Center

Certified Gold Admin: <test3@test123.com>

▼**Messages & Files**
Compose
Track Sent
Inbox
Group Inboxes
Drafts
Folders

▼**My Account**
Address Book
User Information
Preferences
Group Mailbox Configuration
SecureContact.me

▼**Admin Console**
Administrative Tools

SAFE TLS CONFIGURATION

The features available for Safe TLS configuration are not able to be edited by Administrator's unless the company has an on-premise solution or is a reseller with multiple tenants. However, these features are important to how a company delivers messages should they be enabled and are described in this section so that company administrators have an understanding of how they work. This knowledge is particularly useful if a company requires changes to be made to their account regarding the Safe TLS settings. Having the settings changed will require the assistance of DataMotion Support, which can be contacted at support@datamotion.com.

Safe TLS Properties at the Company Level

Safe TLS Company Configuration Properties

Safe TLS

Before changing these values, the Gateway must be configured properly.

Send Safe TLS
Full message contents will be sent via TLS encryption for message security. Note: notification links will continue to be sent along with full message content until the recipient establishes a password and logs into the portal once.

DISCLAIMER: DataMotion guarantees security of messages delivered over TLS to the recipient mail servers that accept such delivery. DataMotion's responsibility ends upon such delivery to these mail servers. Thereafter, DataMotion has no visibility into and is not responsible for how the messages are routed by the recipient's mail server to the recipient's inbox.

◉ Off ○ On

Safe TLS Override Read Confirmation
When set, will send via Safe TLS, messages that have read confirmation requested.

◉ Off ○ On

Safe TLS Footer
The footer displayed when a message is sent via Safe TLS. Changing this changes the footer for all Safe TLS messages for the company. Use the %%url%% variable in the footer to specify where in the footer you would like the URL to be placed.

This message has been securely sent using encrypted communication. If you reply and are notified that your reply is unable to be securely delivered, refer to this link:

These settings fully describe themselves in the screenshot above, and can be altered upon requests made to DataMotion Support. In the case of On-Premise users it is simple to alter these settings via the Admin Console's **Administer your corporate accounts** link and clicking the 🖳 icon.

NOTE: The Safe TLS Footer can be altered to contain any text that is desired or no text at all. It is not advised to have no text in the footer. More specifically, having

no %%url%% will cause users that can receive TLS messages, but not able to reply with TLS, left with no way to respond to messages they receive.

Safe TLS Properties at the User Level

The features that are directly configured at the user level required changes to already existing properties shown in the screenshot below.

Safe TLS User Configuration Properties

These settings were previously for the original plain text delivery features that SecureMail provided. They will take precedence over the company configuration properties if the Receive messages via Plain Text setting is set to **On** and the Plain Text Delivery Path is set to a valid SMTP drop path with forced TLS connections.

DOMAINKEYS IDENTIFIED MAIL (DKIM)

The DKIM Management console is available to all company administrators who are required to setup DomainKeys Identified Mail or DKIM as part of their corporate compliance strategy.

NOTE: A working knowledge of DKIM is required in order to properly setup and configure DKIM for DataMotion SecureMail.

DKIM MANAGEMENT CONSOLE

In order to access the DKIM Management console, administrator level permissions are required and upon logging into the web portal, go to the Administrative Tools and click on DKIM Management. See below for details:

You will see something similar to the following:

DKIM Management

Company

Your company

Domain Name

yourdomain.com

Selector

securemail

Canonicalization Algorithm

Simple ▾

Save Cancel Close

yourdomain.com ⇨ 🗐 ✎ 🗑

Selector
securemail

Canonicalization Algorithm
Simple

12/16/2019 5:49:07 PM
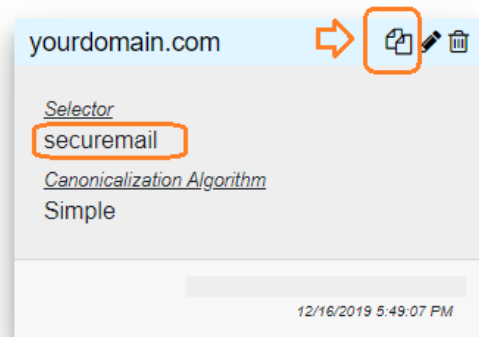
Each field on this screen corresponds to the following:

- Company
  - » This field is pre-populated with the name of the company that you are an administrator of and cannot be edited.
- Domain Name
  - » The name of the domain that you wish to add.
- Selector
  - » The type of selector to be set for your DKIM public key record. We recommend defining the selector as *securemail* to distinguish it from other DKIM records you may be adding in the future.
- Canonicalization Algorithm
  - » Contains the options Simple or Relaxed.

Once you add the Domain Name and a Selector and save your changes, a new DKIM public key will be created and can now be copied and pasted into your DNS TXT records.

An example of what the DKIM Key name should look like in your DNS configuration portal for securemail._domainkey.yourdomain.com along with record values: v=DKIM1;h=sha256; k=rsa;

TXT records

HOST	TEXT	TTL
_domainkey.yourdomain.com	v=DKIM1; h=sha256; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgK...	300 sec

NOTE: It is possible for on-premise customers or by request to DataMotion Support to enable sub domains or allow multiple domains for DKIM.

COBRANDING THE WEB PORTAL

WHAT IS COMPANY COBRANDING?

Company Cobranding allows a company or organization to place its brand identity on the DataMotion secure messaging portal. With cobranding, the message delivery notification sent to DataMotion SecureMail recipients contains a link with a cobrand tag. When DataMotion SecureMail **recipients** use this link to access the portal, it will take them to the cobranded portal. Also, when **senders** log in to the portal, it will display their company's cobranding.

The following login screens illustrate a few of the differences between a standard DataMotion web portal and a cobranded portal.

Example of DataMotion Branded Web Portal Login
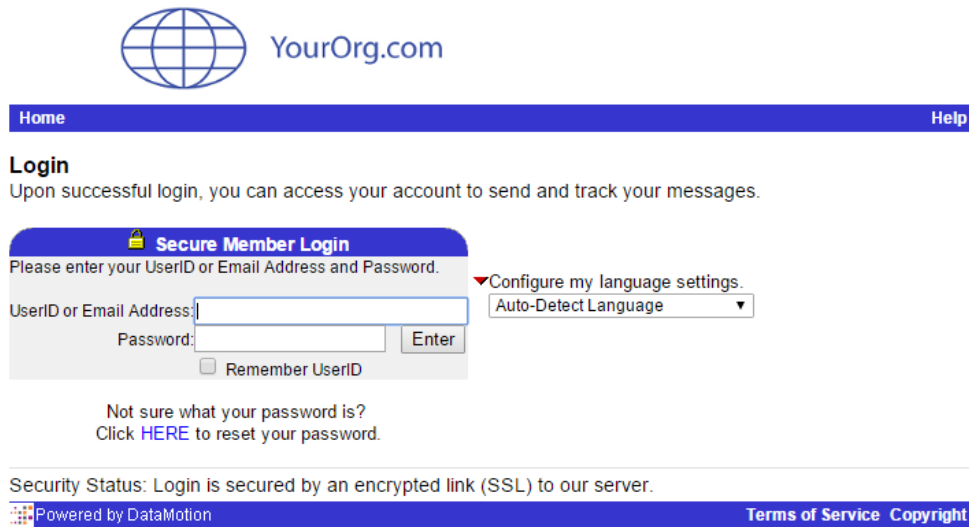
Example of a Co-Branded Web Portal Login

WHO SETS UP A COBRAND?

Administrators have permission to create cobrands for their companies. In addition, within a company hierarchy, an administrator of the parent company can cobrand any of its subtenants. It is also possible for an administrator of a subtenant to cobrand other subtenants beneath itself within this new hierarchy. If no cobrand exists for a company, it will use the default branding, which will be either the standard DataMotion branding or the standard cobrand inherited from a corporate parent, or landlord company, that is established as the default company.

COBRANDING FEATURES

Cobranding features include the following:

- You can specify an **Image** (usually an organization or company logo) that will be displayed at the top of all portal pages.

- You can specify a **Hyperlink** that will be used if users click on the image.

- You can specify a **Custom Color** that will be used for common style elements on web pages, such as the login panel on the login screen, and the top menu bar and bottom status bar common to the portal pages.

- You can insert **HTML Coding** to be used in place of the image and accomplish advanced cobranding customization. The HTML can contain text, links, graphics, and columns and follow an HTML style sheet.

- You can control how long to **Allow users to stay signed in** (days, hours, minutes) without activity.

- You can specify whether to **Filter Messages**, which allows you to limit the messages that users see in their mailbox to the messages related to the cobranded company. It is primarily used to add another level of cobranding to the **recipient** experience. With cobranded message filtering, the DataMotion SecureMail recipient's mailbox will display

only those messages from or to the cobranded company as long as the recipient accesses the portal using the notification email link.

CREATING A COMPANY COBRAND

1. Log in to your DataMotion SecureMail portal as an Administrator. (The URL for the portal was determined during installation.) The Member Center page should be displayed, similar to the following. (If it is not, click Member Center on the menu bar at the top of the page.)

   NOTE: Some of the items on the following screens may be different or may not be shown on your screen depending upon your administrative rights.

2. On the Member Center page, click **Administrative Tools**. The Administration Console is displayed, similar to the following.

Administration Console

▼**Corporate Account Management**
  Administer your corporate accounts.

▼**Company Settings**
  Cobrand Management Console

▼**Reports**
  Message tracking report
  User logon report
  User reports by message size, volume, date and summary
  TotalView report
  Form Tracking report

3. Under the Company Settings heading (or Server Settings heading), click **Cobrand Management Console**. The Cobrand Console is displayed, similar to the following.

Cobrand Console

▼**1. Cobrand Information**

  Create a New Cobrand   ▼ (To Edit an existing cobrand, simply select it from this list)

  Company Name:
  Default URL:
  Cobrand Color: 000000
  Top HTML (Optional):

  Loaded Image (Optional):   /img/cobrand/   Clear Image
  Allow users to stay signed in
  Filter Messages

▼**Select Image**
  Choose File   No file chosen

▼**2. Save/Apply**
  Save
▼**Quick View**
  Quick View

4. In the first field (which is a drop down list), select **(Create a New Cobrand)**.

5. Fill in the applicable cobrand fields according to the information that follows:

   » **Company Name** (optional) is a descriptive name that will be associated with the cobrand. This name will be displayed in the Edit cobrand drop down list.

   » **Default URL** (optional) is the URL where users are directed when they click on the cobrand image. You must include the protocol/scheme (e.g., "http://") in the URL. If not specified, the URL will be the host server, e.g., http://www.datamotion.com.

   » **Cobrand Color** (optional) defines the web color used for common style elements on the web portal pages, namely, in the login panel on the login page, as well as the top and bottom ribbon bars (menu and status bars) common to the portal pages. It is a 6-character hexadecimal identifier. The six-digit identifier is actually a hex triplet, or three-byte hexadecimal number, used to represent colors in HTML, CSS, SVG, and other computing applications. The bytes represent the Red, Green and Blue (RGB) components of 24-bit "True Color," ranging from 00 for least intensity to FF for greatest intensity. (000000 is black or no color, and FFFFFF is white or all colors.) This offers 16,777,216 different color possibilities. (Optional: You may precede the color code with a # sign, which is common with hex color codes.)

   You may enter a color code using the keyboard or you may use the built-in color picker tool. (The color picker tool will pop up when you click in the Cobrand Color field.) To use the color picker:

   A) Point to the Color Selector box (the RGB "spectrum") that is displayed, and using the cross-hair cursor, click on a spot to select a hue.

   B) To the right of the Color Selector box is a Shade Selector that allows you to select a lighter or darker shade. Click and drag the slider triangle up or down to select a shade, or click on a spot within the Shade Selector bar.

   Most imaging software will also allow you to view and select hex color codes. The ColorPix tool http://www.colorschemer.com/colorpix_info.php can be particularly helpful when trying to match the color in an existing image or logo. You may also use their on-line color tool to find a color.

   NOTE: If you specify the color as #FFFFFF (white), it will result in ribbon bars that

cannot normally be seen (including the menu bar), because they will have white text on a white ribbon bar against a white background.

» **Top HTML** (optional) allows you to accomplish advanced cobranding customization by specifying a block of HTML coding to be used in place of the cobrand image in the page header. The HTML can contain text, links, graphics, and columns and follow an HTML style sheet.

(The page header is probably the most important element in the cobranding design, and either the **Top HTML** method or the **Select Image** method should be used to cobrand the page header. A selected cobrand image takes precedence over Top HTML if any HTML code is inserted in Top HTML. To give the HTML precedence when an image is also loaded, you must use the **Clear Image** button. If you want to use a loaded image in Top HTML, you would first upload an image through Select Image plus Save, and then copy the path of the Loaded Image into the Top HTML, as well as any safe location on your computer, plus Save; then you can use Clear Image to give the Top HTML precedence.)

NOTE: If the Top HTML field contains some boilerplate code, do not delete it unless you intend to replace it with customized HTML.
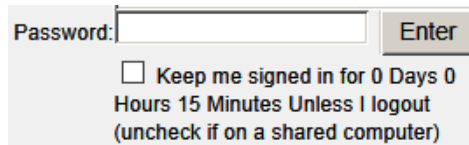
» **Loaded Image** (non-editable field) displays the database server path and internal filename for the uploaded cobrand image that was Selected and Saved.

» **Clear Image** button immediately removes the image from the cobrand. This action goes into immediate effect (a "Save" is not required to apply this action). It is important to wait for the action to complete and then click the Quick View button to see the result. Clear Image is only used to remove an existing cobrand image and give Top HTML precedence. It is not necessary to use Clear Image to replace a cobrand image (in this case, simply select another image). Clear Image does not remove the image from the database, so it can be referenced in the Top HTML, as long as you stored a copy of the Loaded Image path and file name so you can reference it.

» **Allow users to stay signed in** (optional) allows you to enable those users who login through the cobranded portal the opportunity to stay signed in for the time period that you specify here. You can specify how long in days, hours, and minutes these users can be signed in without activity. When you click the check-box to put a checkmark in it, the controls for selecting **Days**, **Hours**, and **Minutes** will appear.

Allow users to stay signed in   ☑
For [0 ˅] Days [0 ˅] Hours [15 ˅] minutes

When users log in through the cobranded portal, it will offer them the option to select the login time that you have specified:

Password: [   ] Enter
☐ Keep me signed in for 0 Days 0
Hours 15 Minutes Unless I logout
(uncheck if on a shared computer)

» **Filter Messages** (optional) allows you to limit the messages that users see in their mailbox to those messages related to the cobranded company. It is primarily used to add another level of cobranding to the **recipient** experience. With cobranded message filtering, the DataMotion SecureMail recipient's mailbox will display only those messages from or to the cobranded company as long as the recipient accesses the portal using the notification email link.

Note that the recipient cobrand experience will take priority over the sender cobrand experience in those infrequent cases where this may occur. For example, if a DataMotion SecureMail sender ("Joe") from one cobranded company is also a recipient of a DataMotion SecureMail message from second cobranded company, and Joe accesses the portal by clicking on the link in the notification message, the portal will be controlled by the second company's cobranding, including any Filter Messages setting.

» **Select Image** (optional) allows you to select a *cobrand image* (usually an organization or company logo) that will be displayed at the top of all portal pages. This provides an easy way to create professional branding without requiring the use of HTML. Click the **Browse** button to find and select the image that you want assigned to the cobrand. Image formats supported include GIF, JPG, BMP and PNG. For the best viewing experience, your images should have 700 x 110 pixel resolution. Images with widths less than 250 pixels will be aligned to the left of the navigation bar. (The page header is probably the most important element in the cobranding design, and either the **Top HTML** method or the **Select Image** method should be used to cobrand the page header. A selected cobrand image takes precedence over Top HTML if any HTML code is inserted in Top HTML. To give the HTML precedence when an image is also loaded, you must use the **Clear Image** button.)

The following example shows the Your Organization cobrand with an image (company logo) selected but not yet saved.

6. Click the **Save Cobrand** button to save your changes and apply the cobrand to the company. (This also applies the cobrand to the browser/portal session until you override it with a Quick View, another Save, or until you leave the website.)

The following example shows the cobrand saved and applied.

The creation of your cobrand is complete.

7. To verify the cobrand information was saved, **select** the cobrand in the Edit drop-down list (which is alphabetized by Company Name with the Cobrand Name following in parentheses), and **wait** a little bit until the cobrand fields are populated on the screen.

» When you **select** a cobrand, it immediately displays the color scheme on the cobrand page.

» Once the cobrand information appears, you may edit it if desired, or click **Quick View** to display the selected cobrand, including the image or Top HTML in the page header. (The Quick View button is used to apply the selected cobrand to the browser/portal session until another Quick View or Save overrides it or until you leave the website.)

» After you have made any changes to the cobrand, click **Save** to Save/Apply the cobrand.

» If you want to view the <Default> company cobrand, select the <Default> company from the drop-down list, and then click **Quick View**. If you want to return to using the <Default> company cobrand for this company (i.e., set the company to use the default cobrand), select the <Default> company from the drop-down list, and then click **Save**.

8. To get out of the cobrand display mode, log out, close the browser window, and then open a new window to log back onto the portal.

This concludes the information on Cobranding.

USER MANAGEMENT

To provide users with access to DataMotion SecureMail, you need to create accounts and have them assigned to the proper User Type. Once users have been created, they will be allowed to login and begin sending secure messages.

ACCESSING USER ACCOUNT MANAGEMENT

To manage your user accounts you need to login and access the **Administrative Tools**.
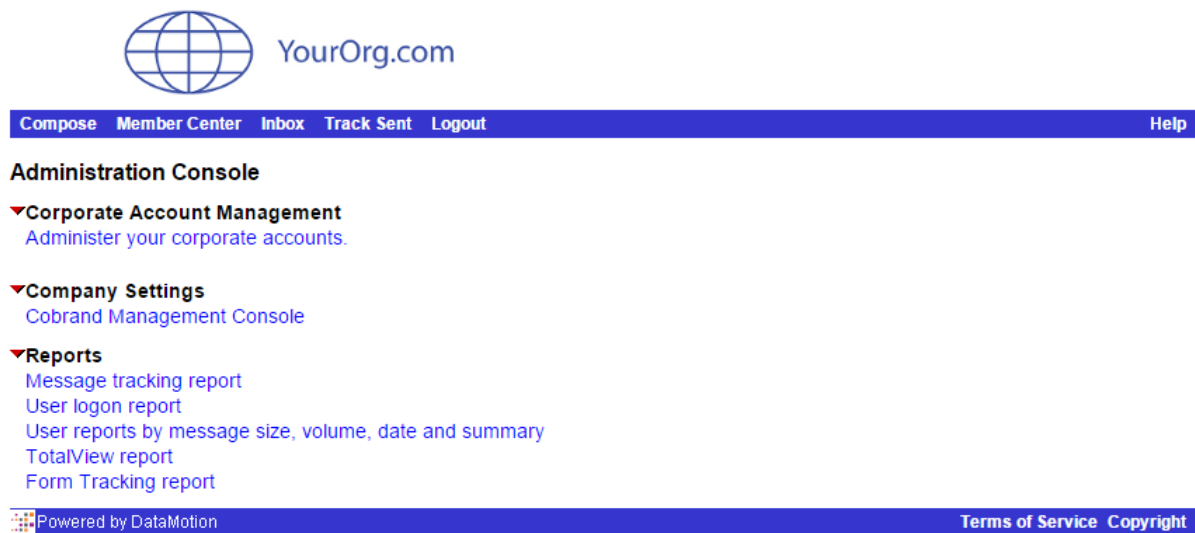
Click the **Administer your corporate accounts** link to display the list of your companies/tenants.
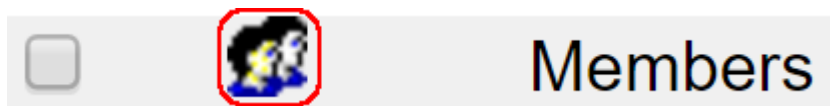
Find the company you wish to manage users for and click on the Heads icon as illustrated above.

MANAGE USERS PAGE

When you first open the Manage Users view you may only see your own account listed. As you add more users you will be shown a full list here when this is opened.

This page is where you will perform all the user administration for your organization.

This page will provide a snapshot of your company user accounts, including the number of licenses you have and the number currently in use.

The Close link at the bottom will return to the **Administrative Tools** page.

Finding your Users

As the number of users grows, you can quickly search for specific accounts using the Search window. In the new hierarchy it is now possible for the parent company admins to see not only users within their company, but every user in its subtenants as well. This can be accomplished by selecting any of the parent's subtenants and searching for users. The results can be further filtered by selecting a User Type from the dropdown.

When searching it is possible to use wildcards to find multiple matches. The % symbol is used for the wildcard. For example, searching for "j%" would return jsmith@yourorg.com in the picture above.

Additionally you can sort based on column by clicking on the column header. Clicking will alternate between ascending and descending order on that column.

Viewing/Editing User Accounts

To see the details of any existing account, click on the email address for that user. This will open the Update User page. From this page all the fields of an account can be edited.

Click **Update User** to save the changes to the account. See *Adding New Users* (on page 39) for information about the account properties.

Adding New Users

It will likely be necessary to add new users to your company account. To create a new user account:

1. From the Manage Users page, click the **Add** link at the bottom.

2. The Add User screen, similar to the following, is displayed:

3. Fill in the account information according to the information in the table that follows.

   The following table describes the properties associated with each user account. Only the user type and email address are required when creating the account; all other fields are optional.

   NOTE: When you choose a new User Type, wait for the page to refresh before starting to enter the properties.

User Account Properties

Account Property	Description
User Type	Determines the privileges assigned to the user. DataMotion Technical Support can provide guidance about the privileges associated with each User Type.
Email Address	The email address for the user.
Password	Assigns an initial password for the account. If a password is not entered here, the user will be sent a message to create a new password for their account.
User ID	Assigns a user ID to be used for the login instead of the user's email address.
Single Sign-On ID	Used for providing a method for single sign-on. Primarily used in conjunction with the SecureMail Administration API.
First Name	User's first name.
Last Name	User's last name.
Phone	A contact phone number.
Company	This is blank when adding a user. When updating a user, it is auto-filled with the company account name.
Offers	This field is not currently in use.
Employee ID	If your company assigns identification numbers, it could be entered here.
Optional Field	Free-form field for any other information.
Account Status	Whether the account is enabled or disabled.
Button User	This is auto-filled by the system.

The following example shows the Add User screen with information entered for adding a user to Your Organization.

Your Organization - Full Account - Add User

User Type:	SecureMail 500 ▼	*
Email Address:	pdavis@yourorg.com	*
Password:		

Password Requirements (if entering a password)
- Minimum 6 characters in length.
- Must contain 1 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

User ID:	padavis
Single Sign-On ID:	
First Name:	Paul
Last Name:	Davis
Phone:	123-456-7890
Company:	
Offers:	☐
Employee ID:	
Optional Field:	
Account Status:	Enabled ▼
Button User?	☐

Add User   Close

4. Click **Add User** link to create the user account, and a screen similar to the following is displayed:

Your Organization - Full Account - Add User

Successfully added: pdavis@yourorg.com

User Type:	SecureMail 500 ▼	*
Email Address:		*
Password:		

Password Requirements (if entering a password)
- Minimum 6 characters in length.
- Must contain 1 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

User ID:	
Single Sign-On ID:	
First Name:	
Last Name:	
Phone:	
Company:	
Offers:	☐
Employee ID:	
Optional Field:	
Account Status:	Enabled ▼
Button User?	☐

Add User   Close

5. Click **Close** to return to the Manage Users page.

The user account is now created.

Transfer Users to Your Company

Transferring users into your company is accomplished via the Transfer User page. The admin can only transfer a single user at a time, and the process does require manual input on the recipient's side for security purposes. The transferring of users can be performed using the following steps:

1. From the Manage Users page click the **Transfer User** link.

2. The new **Transfer User** page will open.

3. Enter the **E-mail address** of the user to transfer.

4. Select the **User Type** that the user will have once they have been successfully transferred into the company.

   » The available user types are three of the standard user types available on the SecureMail system. They are as follows:

   » Secure Contact Us: For Secure Contact Us Subscribers only.

   » SecureMail 500: The standard user type that grants users access to the Compose feature to send messages.

   » SecureMail 500 Admin: Has the same capabilities as a SecureMail 500 user, and access to the Administration Console.

5. Click the **Transfer** button.

6. An onscreen prompt will appear.

   » If the E-mail address entered is not a valid recipient in the DataMotion system, it will not be possible to transfer them.

   » The following error will appear to inform the administrator that this is the case.

7. The user must accept this transfer request notification email before they will be moved to the company.

8. At this point it is up to the user to either accept or decline this request.

NOTE: This request notification was designed to ensure that the administrator correctly inputted the email address of the recipient for security and privacy purposes. This is due to the fact that the notification will be sent no matter what email address is entered so long as it is a valid email that exists within the DataMotion SecureMail system.

NOTE: Once the user makes their decision regarding the transfer request it will be permanent. The links inside the request email will no longer be functional, and a new request will have to be sent to the user should it be necessary.

NOTE: The user must respond to the first transfer request in some way (accept or decline) before a second request can be sent.
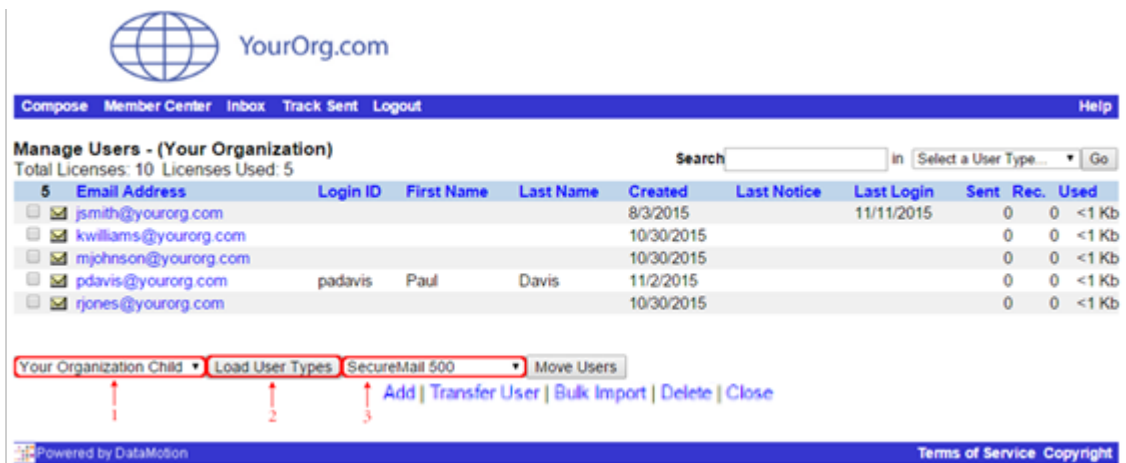
Moving Existing Users

It is possible for an admin to move existing users within subtenants. The admin is capable of moving users between their company and subtenants beneath them, but they cannot raise anyone above their company into the parent itself. Moving users can be performed by:

1. From the Manage Users page, ensure the destination is correct via the drop-down on the left.

NOTE: Please note that the company list contained within this drop-down is not alphabetized but ordered by company ID. While inconvenient it is recommended that a list be created of these companies with their corresponding company IDs for ease of use later.

2. Click the Load User Types button to load the available user types of the destination company.

3. Select the User Type from the drop-down on the right.

4. Click the check box next to the user you wish to move, and then click the **Move Users** button.

5. The user will now be in the company chosen.

Password Management

Once a user account has been created, managing passwords is the primary administrative task for the account. Users are created and managed from a common page allowing the fields to be filled in during account creation or edited later. This includes the password field.

Passwords When Creating an Account

While it is obviously necessary to have a password assigned to a user account for authentication, it is not necessary to set this password during the initial account creation. As such, the Password field is not marked as required for creating a new account.

When a new account is created, if the password field is left blank, a message will be sent to the user's address providing instructions on how to set their password. This is the most common method for creating new users, allowing them to set their own unique passwords.

When a new account is created and the password field is filled, the account will be set with that password. The password will not be sent to the user and it is expected in this case that the user will be informed of the password by other means such as a phone call.

Administrator Password Resets

The other use for the password field is administrator password resets. Users are provided multiple means for resetting their passwords without the need to call support (or the administrator), but there are times when the administrator may need to reset a password manually. The administrator can then use the password field to explicitly set a new password for the user account.

The most common use of this functionality is when a user is no longer in a position which requires DataMotion SecureMail (such as having left the company) but there is a need to preserve access to the account for audit purposes. The administrator can then reset the password to something new for access to the messages in the account.

Bulk User Import

There are times when you may need to create more than one user account at a time. For this scenario you can use the Bulk Import function to create multiple accounts at once.

The Bulk Import function uses a comma-delimited format for importing the information. The list of fields is:

```
Email Address, UserID, Password, First Name, Last Name, Optional Field
1, Optional Field 2, Account Status, Single-Sign-On
```

NOTE: These fields are listed on the Bulk User Import page itself next to the Format: label.

NOTE: The Account Status takes a 0 or a 1 to specify if the account is enabled or disabled. A 1 will enable the account, a 0 will disable the account. The default is 1 (enabled).

To create multiple accounts using Bulk Import:

1. From the Manage Users page, click the **Bulk Import** link at the bottom.

Manage Users - (Your Organization)
Total Licenses: 10 Licenses Used: 5

0Email Address	Login ID	First Name	Last Name	Created	Last Notice	Last Login	Sent	Rec.	Used

To view users, you must select a user type from the above list. You may also specify an optional search criteria to narrow the lookup.

Your Organization ▼ | Load User Types | Secure Contact Us ▼ | Move Users

Add | Transfer User | Bulk Import | Close

Bulk User Import

Bulk User Import allows you to easily import many users at one time. The only required field is "Email Address". After a user is successfully added to the system, they will automatically receive a registration email inviting them to the system. If no password was supplied, the user will be prompted to create one. If "Account Status" is not supplied the default is 1 (Enabled).

Step 1: Select destination UserType

SecureMail 500   ▼

Step 2: Provide comma-delimited user information below

Format: Email Address,UserID,Password,First Name,Last Name,Optional Field 1,Optional Field 2,Account Status,Single-Sign-On

◉ Upload File ○ Copy/Paste

☐ File Includes Headers
Choose File   No file chosen

Example:
johndoe@somewhere.com,johnd,123456,John,Doe,11-1111,555-555-5555,1,SOMEWHERE.COM\johnd

janedoe@somewhere.com

jackdoe@somewhere.com,jackd,,Jack,Doe,,,0

Step 3: Click the "Import Now" button to add users
Accounts will be created for all users in the list. Registration notifications will be automatically sent to each user individually inviting them to the system.

[Import Now] [Close]

2. Select the User Type.

3. Select either Copy/Paste or Upload File.

    a. If Upload File is chosen, a .csv file must be used. Also the header information in the .csv file must match those listed above.

    b. Enter the comma-delimited information for the import into the page if you selected Copy/Paste either by typing or pasting the information.

NOTE: It is possible to specify a list of addresses and no other information to quickly create multiple users, because no other fields are required. These users will all be notified to set the password for their new account.

4. Click **Import Now** to create the user accounts.

5. Click **Close** to return to the Manage Users page.

Deleting User Accounts

User accounts can be deleted from the Manage Users page. To remove a user account (or multiple accounts):

1. Select the account(s) by checking the box at the left of the account line.

2. Click the Delete link at the bottom of the page.

3. Click OK to confirm deleting the account(s).

CHALLENGE QUESTIONS FOR PASSWORD RECOVERY

OVERVIEW

DataMotion SecureMail provides multiple methods for password recovery. By default, there are two methods for resetting passwords: 1) an administrator can reset users' passwords, and 2) an email-based sequence can allow users to reset their passwords. Some organizations prefer using challenge questions to provide confirmation of the user's identity. This feature can be activated for your organization by contacting DataMotion Technical Support.

Once this feature has been activated, a new link appears below the Admin Console called **Security Questions**.

Working with Technical Support, the administrator can specify two options related to this function: the number of questions a user needs to have answers for, and then the number the user needs to answer to allow the password reset. When enabled, the default settings would require a user to have answered three different questions for future use, and then be required to answer one of those questions for verification. These numbers can be changed according to the needs of your organization.

For more information about how a user interacts with the Challenge questions, see the *DataMotion SecureMail User Guide.*

CHALLENGE QUESTIONS

To quickly get you started with configuring your challenge questions, DataMotion SecureMail provides a number of commonly used questions for user verification:

- What year was your mother born?
- What year was your father born?
- Which city did you graduate from High School in?
- What is the name of your first pet?
- Which model was your first car?

- **n**   What is your paternal grandmother's first name?
- **n**   What is your maternal grandmother's first name?
- **n**   What is your mother's maiden name?

These questions are always available.

Adding Customer Challenge Questions

It is possible to create custom challenge questions for your users. These questions will be listed in addition to the built-in set.

To create custom challenge questions for your users:

1. Click the **Security Questions** link under the Admin Console.

Security Questions for Password Recovery

Add New

Question	Company	Visible	Actions
What year was your mother born?	Global Default		
What year was your father born?	Global Default		
Which city did you graduate from High School in?	Global Default		
What is the name of your first pet?	Global Default		
Which model was your first car?	Global Default		
What is your paternal grandmother's first name?	Global Default		
What is your maternal grandmother's first name?	Global Default		
What is your mother's maiden name?	Global Default		

1

2. To add a new question to the list, click **Add New**.

3. In the new field, enter a question.

Security Questions for Password Recovery

Question	Company	Visible	Actions
What year was your mother born?	Global Default		
What year was your father born?	Global Default		
Which city did you graduate from High School in?	Global Default		
What is the name of your first pet?	Global Default		
Which model was your first car?	Global Default		
What is your paternal grandmother's first name?	Global Default		
What is your maternal grandmother's first name?	Global Default		
What is your mother's maiden name?	Global Default		
What is your favorite color?	Galactic Seats		Save Cancel

4. Click **Save**.

Security Questions for Password Recovery

Add New

Question	Company	Visible	Actions
What is your favorite color?	Galactic Seats		Edit Publish
What year was your mother born?	Global Default		
What year was your father born?	Global Default		
Which city did you graduate from High School in?	Global Default		
What is the name of your first pet?	Global Default		
Which model was your first car?	Global Default		
What is your paternal grandmother's first name?	Global Default		
What is your maternal grandmother's first name?	Global Default		
What is your mother's maiden name?	Global Default		

1

NOTE: This is the last chance to edit this specific question. Once it has been published it will not be able to be edited.

5. Click **Publish** to make the question active.

Security Questions for Password Recovery

Add New

Question	Company	Visible	Actions
What is your favorite color?	Galactic Seats	✓	
What year was your mother born?	Global Default		
What year was your father born?	Global Default		
Which city did you graduate from High School in?	Global Default		
What is the name of your first pet?	Global Default		
Which model was your first car?	Global Default		
What is your paternal grandmother's first name?	Global Default		
What is your maternal grandmother's first name?	Global Default		
What is your mother's maiden name?	Global Default		

1

The question is now added to the list.

Changing Custom Question Visibility

Once a question has been published, its visibility to users can be changed. By default, when a new challenge question is added, it is made visible.

Questions that are visible will have a red check mark in the **Visible** column. To change the visibility of a question, click the checkbox to toggle the checkmark. If the box is empty the question will not be shown to users.

NOTE: Questions listed as Global Default are the built-in questions and their visibility cannot be toggled.

REPORTS

DataMotion SecureMail provides Administrators with a range of usage reports they can use to monitor and track how services are being used. All reports are accessed from the Administration Console.
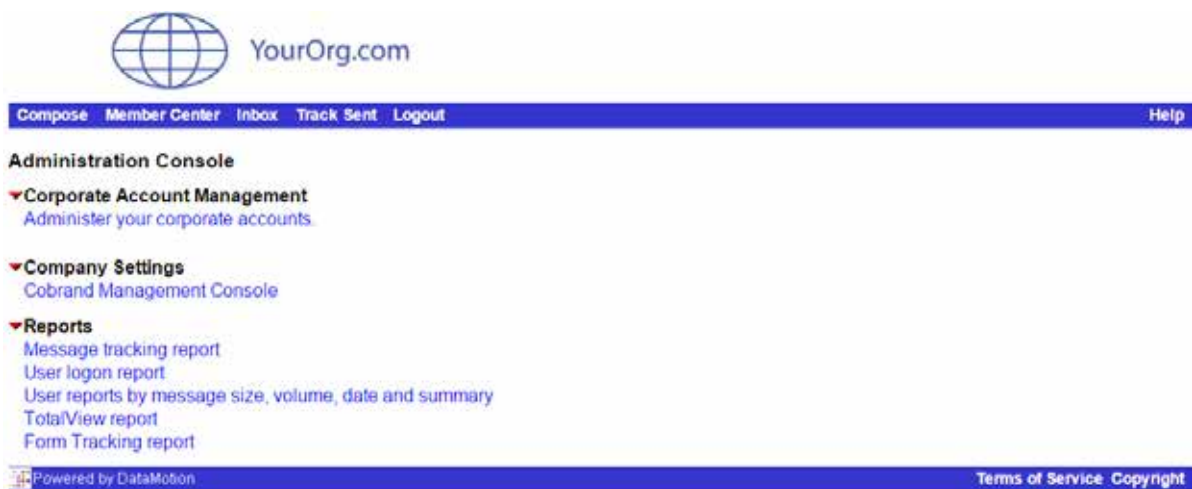
REPORT GENERATION FILTERING INTERFACE

There are two fields commonly found in reports and that can be used for filtering the results shown in the reports.

The first field is the Email Address or Pattern. This field can be used to filter results based on a text pattern related to the messages. When it is left blank, it will show all messages (subject to any other filters that may be defined).

The % symbol is used as a wildcard for this field. It can be placed anywhere in the string to provide flexibility in matching. For example, searching for "j%" would return results beginning with the letter "j", such as jsmith@yourorg.com.

See the section Finding Your Users for more information about using the wildcard in searches.

The second field is a date filter. Here you can specify starting and ending dates for your report. The calendar icon will show the dates visually.

Start Date:

End Date:

If a field is left blank it will not be used in the filter. For example, if you specify an End Date but not a Start Date, then all messages from the earliest sent until the specified End Date will be shown in the report. If both are blank, all messages would be shown (subject to any other filters that may be defined).

GROUP MAILBOX ACCESS REPORT

The Group Mailbox Access Report tracks all delegate access to Group Mailbox messages and who they were opened by. This report only pertains to Group Mailboxes and shows no data pertaining to regular mailbox activity.

To generate a Group Mailbox Access Report:

1. Click the Group Mailbox Access Report link from the Administration Console.

Group Mailbox Access Report

Start Date:

End Date:

Generate Report   Download Report   Close

2. Enter the Start Date and End Date via the calendar image.

Group Mailbox Access Report

Start Date: 01/06/2016

End Date: 01/07/2016

Generate Report   Download Report   Close

3. Click on Generate Report or Download Report in order to view or save the report to your machine.

Back to Reports

DataMotion SecureMail Server Report
Group Mailbox Access Report

Report Generated On: 12/07/2016 19:01:47 (UTC)   Number of Records: 3

ID	Date Sent	From	To	Opened By	Open Date
100022	12/07/2016 18:59:28 (UTC)	jsmith1134015@gmail.com	test@test.com	test@test123.com	12/07/2016 19:00:12 (UTC)
100022	12/07/2016 18:59:28 (UTC)	jsmith1134015@gmail.com	test@test.com	test2@test123.com	12/07/2016 19:01:03 (UTC)
100022	12/07/2016 18:59:28 (UTC)	jsmith1134015@gmail.com	test@test.com	test3@test123.com	12/07/2016 19:01:28 (UTC)

To sort by the Group Mailbox being accessed, click the To column.

MESSAGE TRACKING REPORT

The Message Tracking Report enables you to look for messages based on pattern matching. The search will look at the email addresses and subject lines to find the matches (message bodies are not searched).

To generate a Message Tracking Report:

1. Click the Message Tracking Report link from the Administration Console.

Message Tracking Report

E-mail Address or Pattern:	
Start Date:	10/12/2015
End Date:	11/12/2015
To / From:	From ▼

Generate Report   Download Report   Close

2. Enter the search parameters into the Email Address or Pattern and Date fields. The To / From field specifies whether to search for the Email Address or Pattern in the message To or the From field.

Message Tracking Report

E-mail Address or Pattern:	%jsmith
Start Date:	10/12/2015
End Date:	11/12/2015
To / From:	From ▼

Generate Report   Download Report   Close

3. Click the Generate Report link or the Download Report link to save the report as a .csv to a local machine.

Back to Reports

DataMotion SecureMail Server Report
Message Tracking Detail
Between 10/12/2015 12:00:00 AM (GMT-05:00) and
11/12/2015 11:59:59 PM (GMT-05:00)

Report Generated On: 11/12/2015 1:03:14 PM (GMT-05:00)   Number of Records: 3

ID	Date	FromEmail	ToEmail	Subject	NumTo	NumRead	MsgSize
24511165	11/12/2015 11:23:28 AM (GMT-05:00)	jsmith@yourorg.com	kwilliams@yourorg.com	Account Security	1	1	87 b
24511166	11/12/2015 12:58:43 PM (GMT-05:00)	jsmith@yourorg.com	mjohnson@yourorg.com	Insurance Estimate	1	1	92 b
24511167	11/12/2015 1:01:55 PM (GMT-05:00)	jsmith@yourorg.com	rjones@yourorg.com	Total Shipment Costs and Applicable Fees	1	1	156 b

1

Powered by DataMotion   Terms of Service Copyright

The report displays all the messages matching the specified criteria.

USER LOGON REPORT

The User Logon Report generates reports about user logon activity. You can look at activity for specific users, defined timeframes and also how the user logged into the service.

To generate a User Logon Report:

1. Click the User Logon Report link from the Administration Console.

User Logon Report

E-mail Address or Pattern:

Start Date: 10/12/2015

End Date: 11/12/2015

Logon Source: All

Generate Report   Download Report   Close

2. Enter the search parameters into the Email Address or Pattern and Date fields. The Logon Source field specifies which service the user accessed. The default is All which will show every service the user has used.

User Logon Report

E-mail Address or Pattern: %jsmith

Start Date: 10/12/2015

End Date: 11/12/2015

Logon Source: All

Generate Report   Download Report   Close

3. Click the Generate Report link or the Download Report link to save the report as a .csv to a local machine.

The report displays all the logon events for the user based on the specified criteria.

USER REPORTS

There are several types of user reports, each of which can be filtered for sent or received messages (or both) for each user. These reports are summaries of user statistics as compared to the detailed reports like the Message Tracking Report.

The following types of reports can be seen:

Report Type	Description
Message Size Statistics	Shows the size of messages sent and received by each user.
Message Date Statistics	Shows when messages have been sent by the users (first and last messages for each user).
Message Volume Statistics	Shows the number of messages sent/received by the user.
Message Summary Data	Shows the fields of the other statistics reports on one screen.

To access any User Report:

1. Click on the User reports by message size, volume, date and summary link.

User Reports

▼ Message Size Statistics			▼ Message Date Statistics		
Sent by each user	View	Download	Sent by each user	View	Download
Received by each user	View	Download	Received by each user	View	Download
Complete statistics by user	View	Download	Complete statistics by user	View	Download
▼ Message Volume Statistics			▼ Message Summary Data		
Sent by each user	View	Download	Sent by each user	View	Download
Received by each user	View	Download	Received by each user	View	Download
Complete statistics by user	View	Download	Complete statistics by user	View	Download

2. Click on the report to be shown; for example: Message Size Statistics: Sent by each user. (shown in the following screen).

DataMotion SecureMail Server Report
Message Size Statistics - Sent by Each User   Back to Reports

Report Generated On: 11/12/2015 4:43:02 PM (GMT-05:00)   Number of Records: 4

Email	#Sent	Total Size Sent	Avg. Size Sent	Max. Size Sent
jsmith@yourorg.com	4	676	169	341
kwilliams@yourorg.com	1	72	72	72
mjohnson@yourorg.com	2	680	340	600
rjones@yourorg.com	1	66	66	66

1

Powered by DataMotion   Terms of Service Copyright

TOTALVIEW REPORT

The TotalView Report is one of the most powerful tools for the DataMotion SecureMail administrator. The TotalView Report provides complete tracking of all messages sent through the DataMotion SecureMail system. The report contains a record of every message sent along with the tracking data for the message and any attachments in a single report. This report is provided as a CSV file (comma-separated value file) which can be evaluated in other programs, such as Microsoft Excel.

The TotalView report includes the following fields:

- Message ID
- Custom ID
- Date
- From
- To
- Subject
- Notification Timestamp
- Message Status — Not Opened, Opened
- Message Open Time
- Attachment Name
- Attachment Status – Not Accessed, Accessed
- Attachment Open Time

Each message and every attachment within a message is reported individually. For example, a message to two recipients with two attachments will generate four rows of data, two for each recipient, with one attachment listed on each line per recipient.

To generate a TotalView Report:

1. Click the TotalView Report link.

TotalView Report
Please select a start and end date and click Generate Report.

Start Date: 10/12/2015

End Date: 11/12/2015

Generate report   Select the last day / 30 days / 60 days   Close

2. Specify the Date range for the report.

   » There are quick options for the last **day**, **30 days**, and **60 days** below the standard Date fields. These will automatically select the specified time period.

3. Click the Generate Report link.

TotalView Report
Please select Download Report.
Start Date: 10/12/2015 12:00:00 AM
End Date: 11/12/2015 11:59:59 PM

Download Report   Select Different Dates

4. Click Download Report to save the CSV file for local use.

The following is an example Total View report opened in Microsoft Excel.

Message ID	CustomID	Date	FromEmail	ToEmail	Subject	Notification Timestamp	Message Status	Message Open Time	Attachment Name	Attachment Size	Attachment Status	Attachment Open Time
24511165		11/12/201	jsmith@you..	kwilliams..	Account 5	11/12/2015 11:23:33 AM	Opened	11/12/2015 11:24:27 AM (GMT-05:00)			Not Accessed	
24511166		11/12/201	jsmith@you..	mjohnson	Insurance	11/12/2015 12:58:47 PM	Opened	11/12/2015 12:59:06 PM (GMT-05:00)			Not Accessed	
24511167		11/12/201	jsmith@you..	rjones@y..	Total Ship	11/12/2015 1:01:57 PM (+	Opened	11/12/2015 1:02:24 PM (GMT-05:00)			Not Accessed	
24511168		11/12/201	kwilliams@	rjones@y..	New Acco	11/12/2015 4:38:06 PM (+	Opened	11/12/2015 4:38:25 PM (GMT-05:00)			Not Accessed	
24511169		11/12/201	rjones@you..	kwilliams..	Thank You	11/12/2015 4:39:01 PM (+	Opened	11/12/2015 4:39:15 PM (GMT-05:00)			Not Accessed	
24511170		11/12/201	mjohnson@	jsmith@y..	Password	11/12/2015 4:41:25 PM (+	Opened	11/12/2015 4:41:35 PM (GMT-05:00)			Not Accessed	
24511171		11/12/201	jsmith@you..	mjohnson	RE: Passw	11/12/2015 4:42:11 PM (+	Opened	11/12/2015 4:42:25 PM (GMT-05:00)			Not Accessed	
24511172		11/12/201	mjohnson@	jsmith@y..	RE: Passw	11/12/2015 4:42:38 PM (+	Opened	11/12/2015 4:42:52 PM (GMT-05:00)			Not Accessed	

FORM TRACKING REPORT

Similar to the TotalView report for messages is the Form Tracking Report for SecureForms. This report will show all SecureForms that have been sent through the DataMotion SecureMail server and all the tracking information associated with the SecureForm. This report is provided as a CSV file (comma-separated value file) which can be evaluated in other programs, such as Microsoft Excel.

The Form Tracking report includes the following fields:

n   Form ID
n   Tracking ID
n   Mailbox ID
n   Format
n   IP Address
n   Submit Status
n   Submit Date
n   Downloaded
n   Download Time
n   Download Status
n   Message Size

To generate a Form Tracking Report:

1. Click the Form Tracking Report link.

Form Tracking Report
Please select a start and end date and click Generate Report.

Start Date: 10/13/2015

End Date: 11/12/2015

Generate Report for the above dates
Generate Report for last month
Close

2. Specify the Date range for the report.

3. Click one of the Generate Report links.

» The **Generate Report for last month** will ignore the dates specified in the Date fields and automatically calculate the last month.

Form Tracking Report
Please select Download Report.

Start Date: 10/1/2015
End Date: 10/31/2015

Download Report
Select Different Dates

4. Click Download Report to save the CSV file for local use.

This concludes the information about DataMotion SecureMail Reports.

2

DataMotion SecureMail Integration with Typical Environments

This information describes how to integrate DataMotion SecureMail with some typical environments, including the following:

- *SendSecure Button for Microsoft Outlook: Installation with Citrix/Terminal Services* (below)
- *SendSecure Button for Lotus Notes: Installation* (on page 61).

The SendSecure Button add-in allows users to send secure messages from within their normal email interface.

SENDSECURE BUTTON FOR MICROSOFT OUTLOOK: INSTALLATION WITH CITRIX/TERMINAL SERVICES

The SendSecure Button add-in for Microsoft Outlook allows users to send secure messages from within their normal email interface.

The SendSecure Button add-in can be installed in a Terminal Services/Remote Desktop/Citrix environment. The Corporate version of the SendSecure Button must be used.

NOTE: By default the Corporate version of the Outlook plugin uses a tagging configuration by default. In order to use the Corporate button with Citrix/Terminal Services without involving the use of the DataMotion Gateway, the "tagging" DMConfig.xml file will have to be replaced with a "desktop encryption" DMConfig.xml file. This must change must be performed before running the installer.

NOTE: To replace the existing "tagging" DMConfig.xml file, simply copy the DMConfig.xml file in the Desktop Encryption folder, and paste it into the directory containing the SecureMailSetup.msi. Overwrite the existing DMConfig.xml when prompted.

The Corporate button uses a single encryption key shared by all customers/users with that version of the add-in. (This is different from the Personal SendSecure Button, which users can download

individually from the DataMotion webmail portal. The Personal button uses an individual encryption key that is different for each user, so users must download and install their own unique version of the button that cannot be installed for any other user.) The SendSecure Button looks the same to users whether it is the Corporate or Personal button.

The Corporate version of the SendSecure Button can be installed normally on the server running Terminal Services. Make sure to close Microsoft Outlook before you install. After installation, desktop clients (up to the number of licensed users) can use the SendSecure Button.

SENDSECURE BUTTON FOR LOTUS NOTES: INSTALLATION (LEGACY)

NOTE: This section is considered to be Legacy software due to the rebranding of Lotus Notes to IBM Notes, and a lack of any ability to test or investigate solutions to problems should they arise.

NOTE: The procedures provided in this section apply only to those who have currently implemented this solution, and any other customers or prospects who possess the versions of the software being discussed throughout this section.

OVERVIEW

DataMotion SecureMail integrates with the Lotus Notes client to provide one-click sending of secure messages.

DataMotion SecureMail for Lotus Notes is implemented in LotusScript and is added to your existing mail template in a standard manner using Lotus Domino Designer where it can be distributed to specific workstations using Notes Template Replication.

This document was written for Lotus Notes developers to allow them to integrate DataMotion SecureMail functionality with Lotus Notes Mail templates v5 and higher. Screen images and descriptions were made using Domino Designer v7. Prior or later versions work in a similar way, but will differ slightly from the version shown.

KEY ASPECTS

The following are the high level components that are involved in the integration process.

DataMotion SecureMail "Send Secure" Script File

You will use one of the following files to add LotusScript to the Notes Mail template:

```
SecureMail.txt OR
SecureMail-Redirection.txt or SecureMail-Tagging.txt
```

Mail Template Modifications

Forms Modified:

```
Memo
Reply
Reply with History
```

Fields Added:

```
None
```

New Actions

```
Added to forms Memo, Reply, Reply with History
Send Secure
```

These actions are added just below Send in the Action Pane.

New Resources

```
None
```

INSTALLATION INSTRUCTIONS

The following instructions are shown using the IBM Lotus Domino Designer released for Notes/Domino v7.x. This procedure has been used on Notes versions 5 and higher.

DataMotion SecureMail Button Options

There are two ways to integrate DataMotion SecureMail into your Lotus Notes mail system. These are called Redirection and Tagging. In either case the end user experience is the same (they click the SendSecure button), but the two methods result in different mail flow.

Redirection Description

When using Redirection, messages sent via the SendSecure button have the recipient list replaced with the email address of the DataMotion SecureMail server, where it will be encrypted and then securely delivered to its destination. This requires configuration on the Domino server to ensure a secure route between your mail server and the DataMotion server.
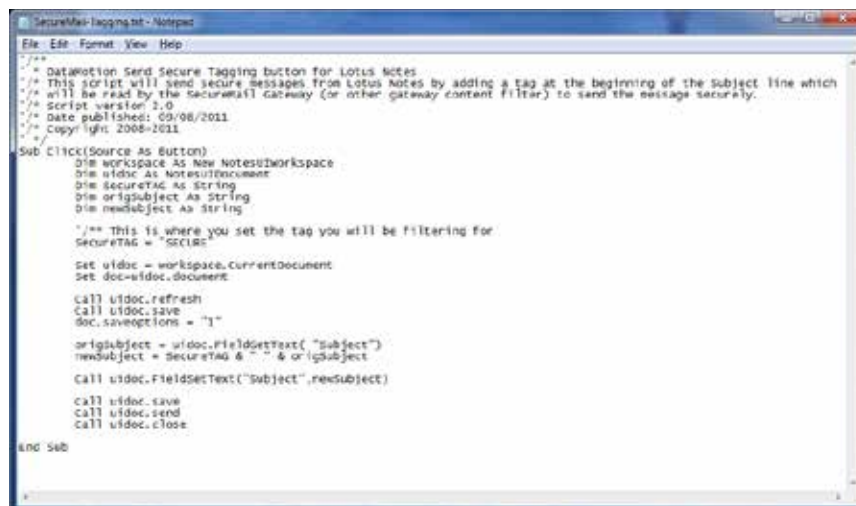
Tagging Description

When using Tagging, messages sent via the SendSecure button have a special tag (e.g., SECURE) inserted at the beginning of the Subject line. This requires that the outbound mail flow include a server containing a content filter (typically the DataMotion SecureMail Gateway) that is used to scan for the tag and then securely route the message to the DataMotion SecureMail server.

NOTE: When using the Tagging configuration, if there is not some sort of content filter that can scan for the subject line tag, the emails will not be sent securely.

Each configuration is installed the same way, the only difference being the selection of the file with the configuration you need to use.

Adding the DataMotion SecureMail LotusScript to your Mail Template

1. Open the appropriate script in a text editor (e.g. Notepad). The files below are named according to the type of button you are installing.

   » SecureMail-Redirection.txt

   » SecureMail-Tagging.txt

NOTE: If you are running DataMotion SecureMail locally, you must change the two instances of "ssl.datamotion.com" to refer to your own local server.

2. From Lotus Domino Designer, open your existing Mail template:
   File à Database à Open
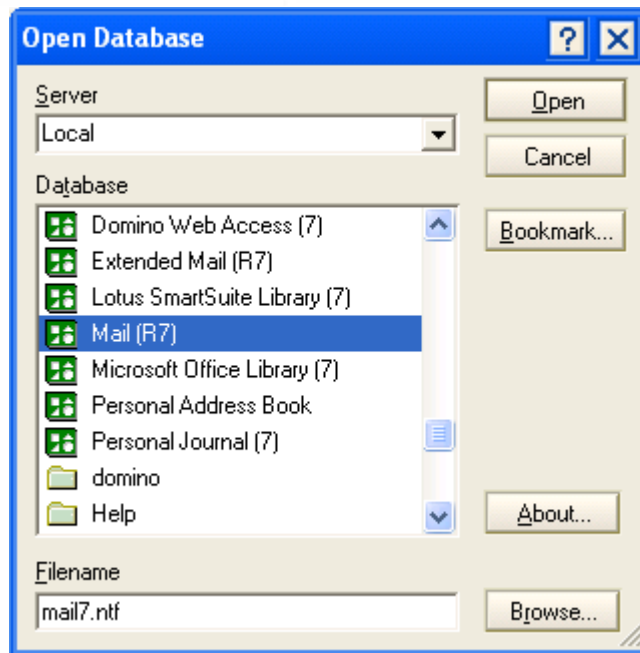
3. Your Lotus Domino Designer screen should now look similar to the following:
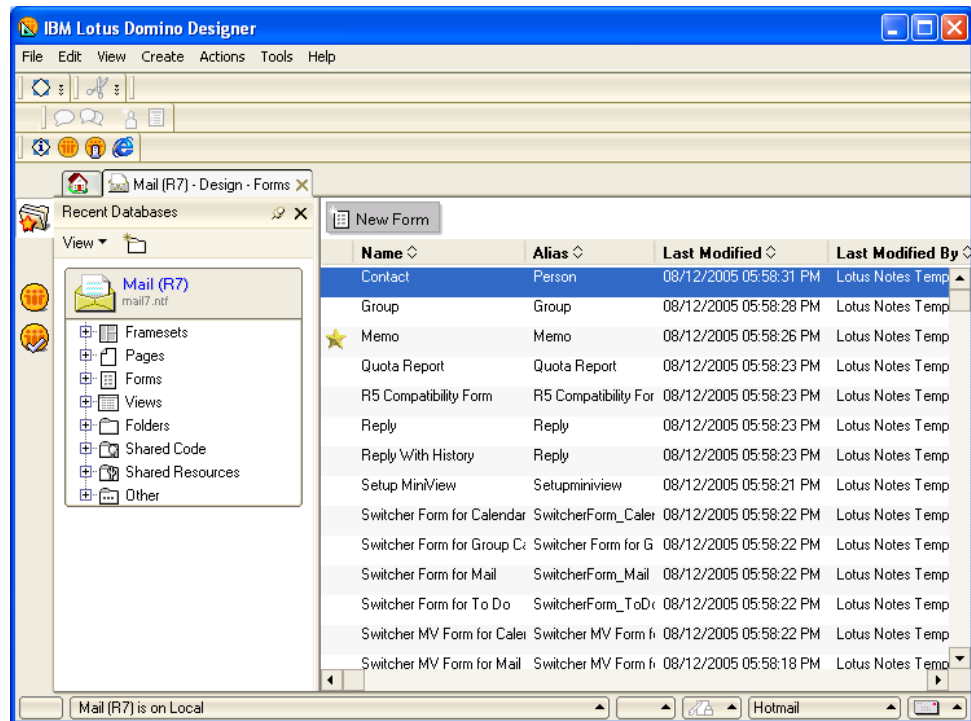
4. Select and open the **Memo** form in the right panel.
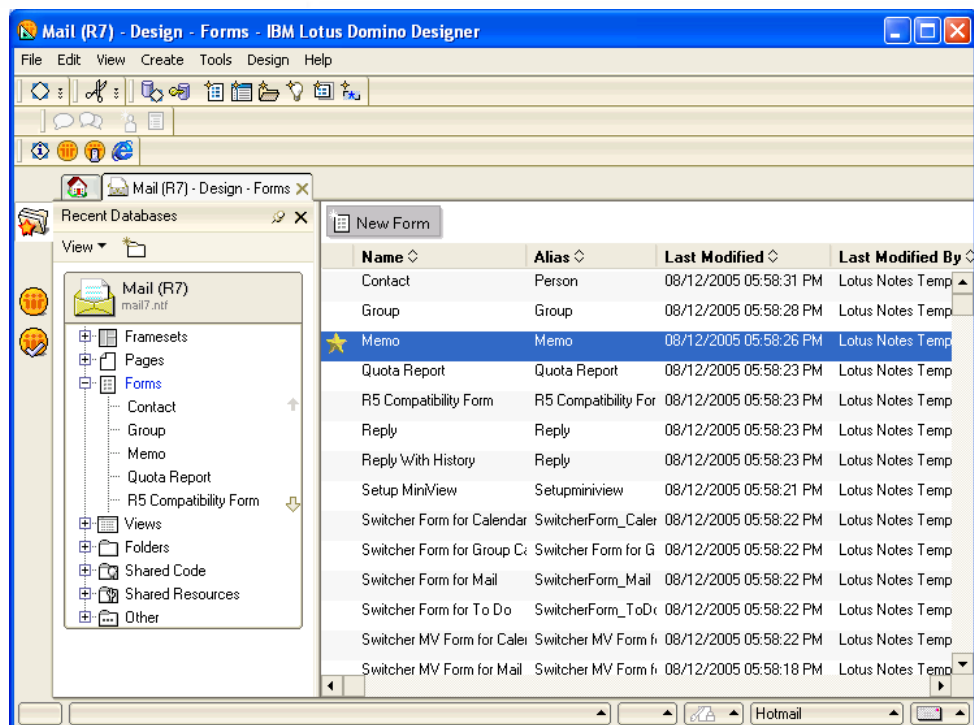
5. Ensure that the menu "View ➔ Action Pane" is checked, which will display the Action Pane on the right side of the Domino Designer.
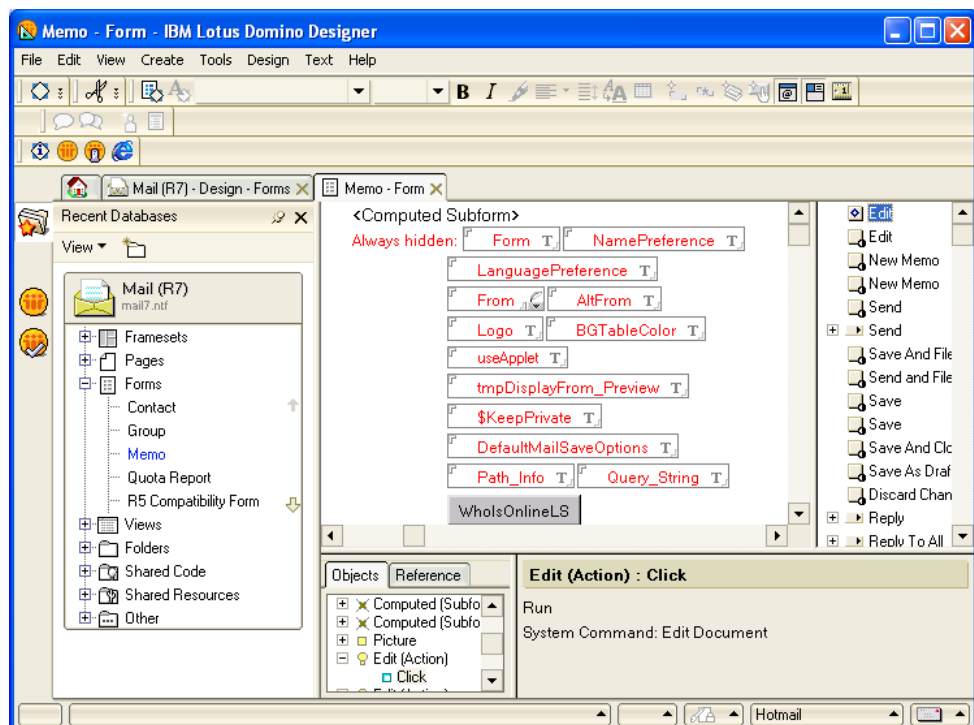
6. Highlight the first Send item in the Action panel in the right side of the screen. Then right click to display the pop-up menu and choose the "Create Action" menu choice.
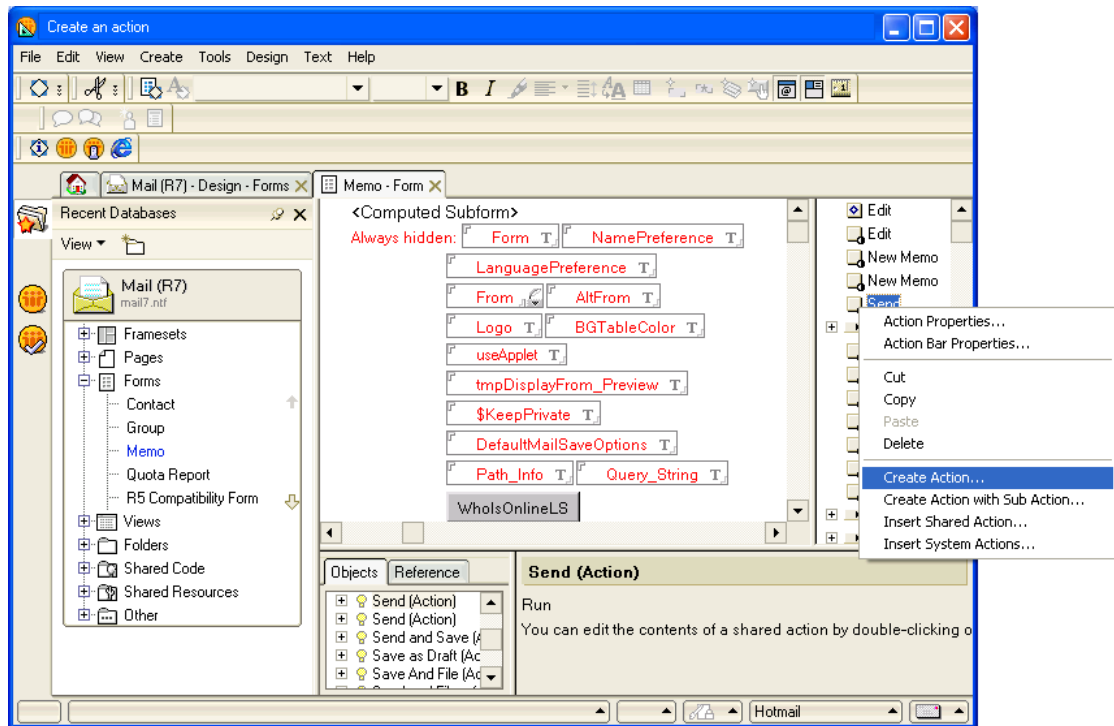
7. In the Action pop-up dialog, type "Send Secure" in the action's Name field. Then close the dialog by clicking the "X" in its top-right corner.

8. The Send Secure action should now be highlighted, and the bottom script area should reference this new action.

9. Change the script area pull downs to "Client" and "LotusScript".
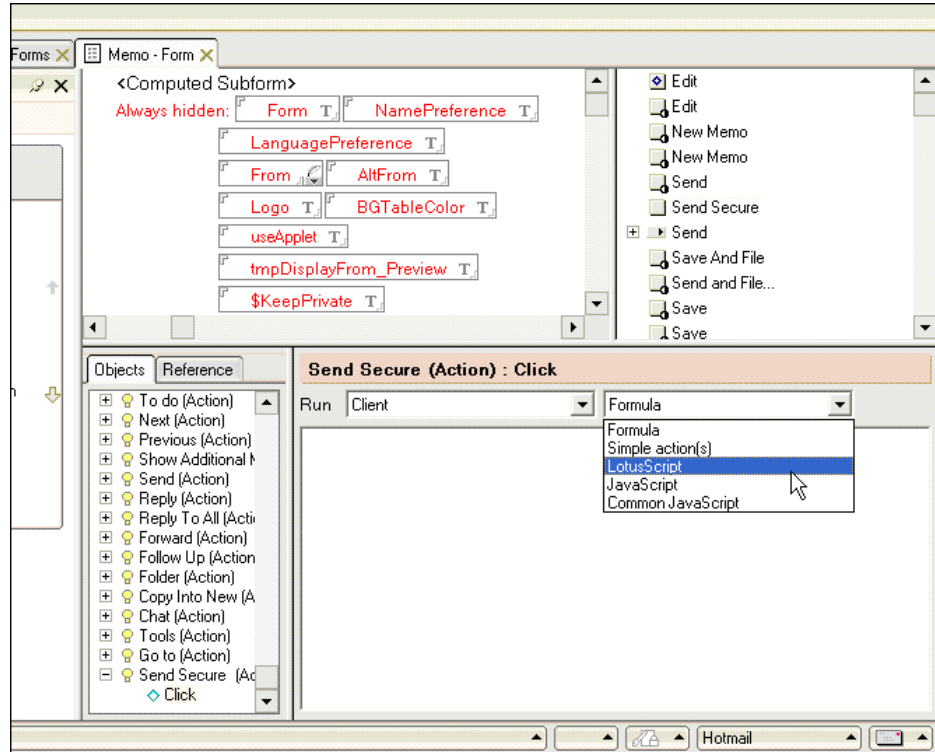
10. Select and delete the empty "Sub Click (Source As Button)" routine including the "End Sub" statements.

11. From your text editor where the DataMotion script file is open (SecureMail-Redirection.txt or SecureMail-Tagging.txt), select and copy all of the text to the clipboard.

12. Return to the Domino Designer and paste the text from the clipboard into the blank script area.
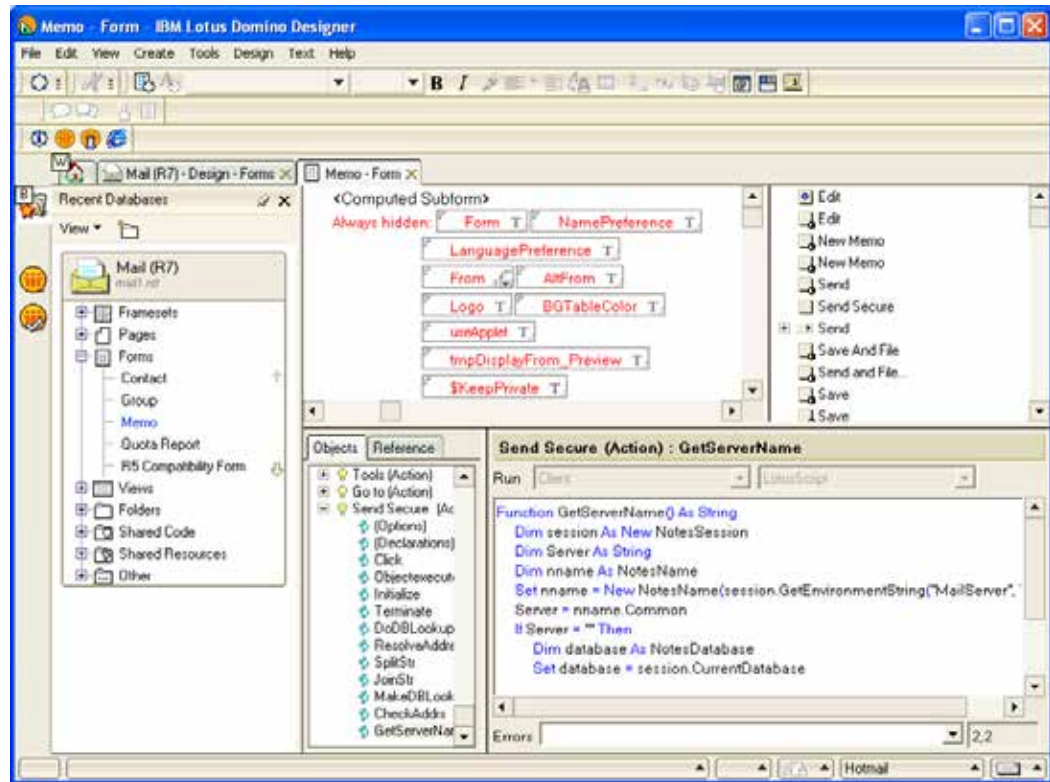
The **Send Secure** action and its supporting LotusScript functions have now been added to the **Memo** form.

13. Save the form.

14. Repeat the preceding steps to add the **Send Secure** action to the **Reply** and **Reply with History** forms.

After saving the **Memo**, **Reply** and **Reply with History** forms, the update of your Lotus Notes Mail template is complete.

3
SecureForms Standard

This information describes how to create DataMotion SecureForms Standard, including PDF and HTML SecureForms, and how to access SecureForm data. It does not describe the features and operation of DataMotion SecureForms Enhanced.

> NOTE: This information applies only if your license includes DataMotion SecureForms Standard.

SECUREFORMS STANDARD OVERVIEW

DataMotion SecureForms are a simple yet powerful way to extend your business processes and provide your constituents an easy way to send you sensitive information through a secure, compliant tool. SecureForms leverage the same platform as DataMotion SecureMail, and integrate into your existing workflows to improve efficiencies, save time, and cut costs.

DataMotion SecureForms automates, secures and tracks the method of collecting and processing confidential information from your customers, employees and partners. Using SecureForms eliminates the need to manually read information from a form and enter it into an application – an error prone activity. The end user provides data into form fields that are specific to your business process needs. This data is transported over an encrypted channel and delivered in XML or CSV formats to the email address chosen by your organization. Data can also be displayed within the original form for printing and reference.

Best of all, with SecureForm Tracking and TotalView reporting, SecureForms provides you with visibility into the movement of information all the way to the destination email address or business workflow. Form recipients embrace SecureForms because it allows them to complete and submit the form in one easy step, at their convenience and right from their local machine.

TYPES OF SECUREFORMS

DataMotion supports different two types of SecureForms to meet your needs: SecureForms PDF and SecureForms Web.

SECUREFORMS PDF

These are PDF forms that can be sent to end user customers, patients, employees, etc. as an attachment or downloaded from your website. The forms can be completed at the recipient's convenience using any PDF reader such as Adobe Reader.

SECUREFORMS WEB

These are web-based forms, typically created in HTML that are hosted on your web site, and are accessed, completed, and submitted by end-users during an active web session.

CREATING SECUREFORMS

Most existing web-based or PDF forms can be converted to a DataMotion SecureForm by adding routing instructions code to the form. The code enables the completed forms data to be securely submitted to the DataMotion Portal, where it is then securely delivered into your organization.

TECHNICAL REQUIREMENTS

While DataMotion provides the proper routing instructions code, the actual creation and maintenance of the eForms is handled by customers.

To create PDF SecureForms, you will need a PDF Editor with forms creation capabilities. Examples include:

- Adobe Acrobat Standard/Pro
- Nitro Pro
- Foxit PhantomPDF

To create HTML SecureForms, any HTML editor can be used. An example of a freeware HTML editor is Microsoft Visual Studio Express (Web Developer Express).

The DataMotion Support team will provide your developers the code, documentation, and a test account to enable data routing to the DataMotion portal.

SECUREFORMS ARCHITECTURE

Web-based SecureForms are hosted on your own web site. PDF SecureForms can be distributed to external users as a file attachment or you may provide them on your website for downloading as needed. You decide the best way to deliver them to your users.

An end user accesses a DataMotion SecureForm as they would any other form, such as by using a PDF reader or a web browser, and the user enters the requested data in the fields. When the user submits the completed form, the data is encrypted and securely delivered to the DataMotion Portal over an SSL connection.

After the data is received by the DataMotion Portal, it is queued for delivery to your specified DataMotion account. Data from multiple SecureForms can be delivered to the same account if

desired. The SecureForm data can then be retrieved in several ways: it can be downloaded as a DataMotion SecureMail message, downloaded via SecureFileTransfer, or your internal systems can pull the data from the DataMotion portal using the DataMotion Adapter.

Once the data is delivered to your environment, it can be imported directly into your own systems or databases or reviewed manually by employees as needed.
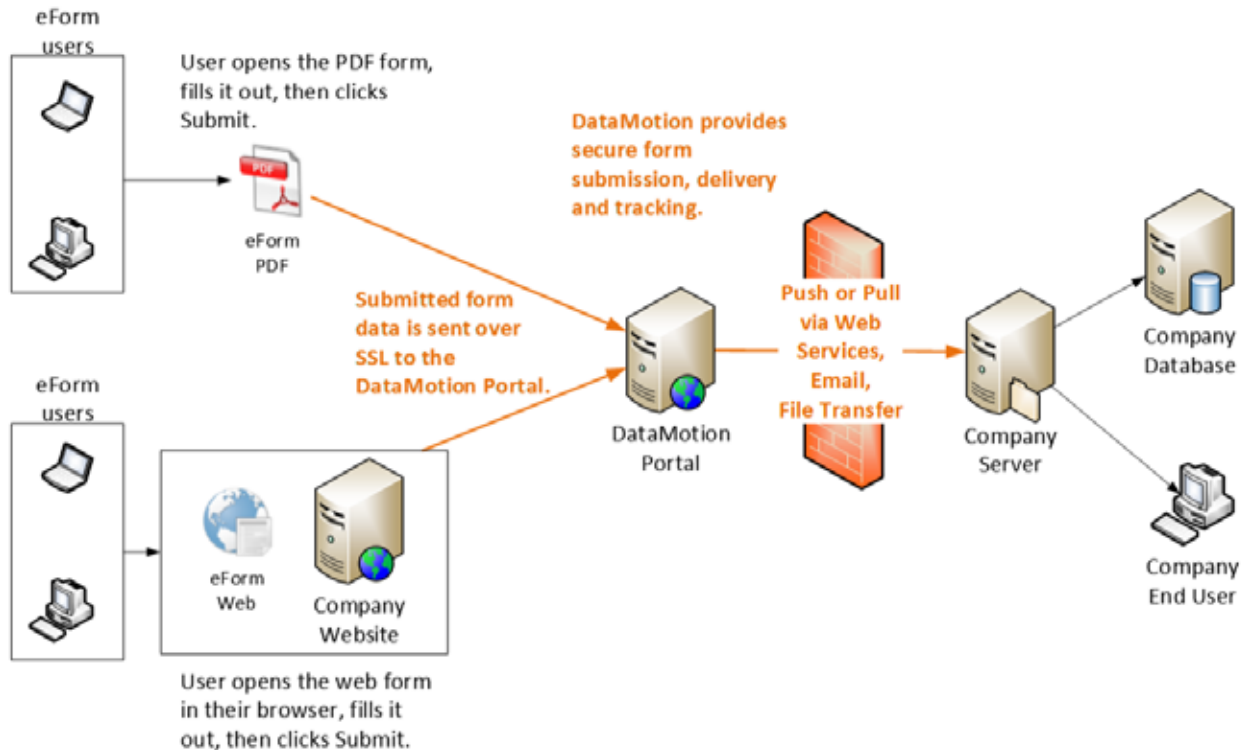
WORKFLOW INTEGRATION

DataMotion SecureForms can be integrated directly into your forms workflow using tools from DataMotion. These include the DataMotion Adapter and the Large File Transfer Client. These tools automatically retrieve submitted SecureForms data from the DataMotion Portal, and place it into your local systems for processing without any manual intervention by your users.

SECUREFORMS PDF CREATION INSTRUCTIONS

To create a SecureForms PDF form, the following hidden fields must be added:

- **co** – the company ID (coid) of the company that is provisioned with the secure forms (provided by DataMotion)
- **txtto** – the email address that will be receiving the form
- **txtsubject** – the subject line of the message when the form is submitted
- **datesubmitted** – a data variable

The following is an example of the hidden fields in a SecureForm:

The Submit Button settings on the form should have the following values:

- **Enter a URL for this link:**
  - » For *DataMotion SecureMail* customers: https://ssl.datamotion.com/form2.aspx
- **Export Format:** FDF Include – Field Data.

Adobe Acrobat 9 or higher is required to edit forms and open the FDF (Forms Data Format). End-users may use Adobe Reader or another compatible PDF reader to fill out forms.

SAMPLE SUBMIT BUTTON CONFIGURATION IN ADOBE ACROBAT PROFESSIONAL
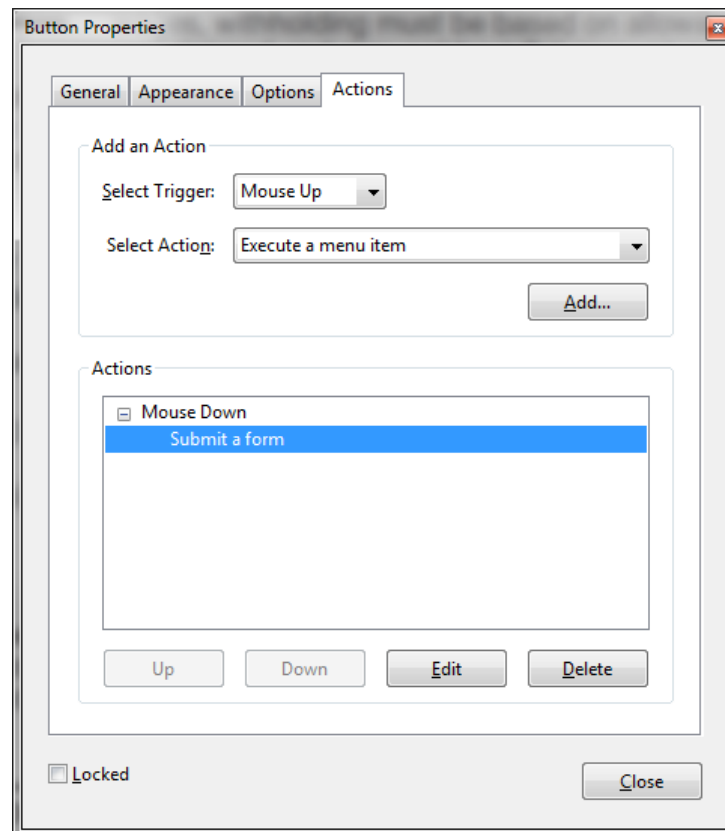
NOTE: This example screen shows the URL for DataMotion SecureMail customers: https://ssl.datamotion.com/form2.aspx.

FORM FIELD NAME RESTRICTIONS

Form field names have a number of restrictions. If a form contains fields with a restricted name, the form will not properly submit. The following is the list of field name restrictions:

- Field names cannot contain the following characters
  - » % - percent sign
  - » / - forward slash
  - » \ - backward slash
  - » . – period
- Field names cannot start with a number (they may contain numbers, just not start with them)

SECUREFORMS WEB CREATION INSTRUCTIONS

The customer is required to provide DataMotion with a reasonably generic form including JavaScript validation if validation is required.

HTML SECUREFORM CREATION

Some basic knowledge of HTML is required. Visual Web Developer Express 2010, which can be downloaded for free is a great tool to build the form. This tool can be used to drag and drop all items onto the form, and do HTML editing and customization. The HTML customization is required to display all the fields properly to the recipient user of the form, and provide the proper names for the fields in the XML attachment. Care should be taken because things can work differently in different browsers, and even between different versions of the same browser.

FIELD VALIDATION

If the information being submitted in the field must be validated (such as verifying that a phone number is in the form XXX-YYY-ZZZZ), this must be performed in the code of the SecureForm. Data validation is not performed by DataMotion after the submission. If field validation is required on the SecureForm, you must create the validation code and implement it within the SecureForm, most likely with JavaScript.

GUIDELINES

The form should contain the following form fields:

- **txtto** – the email address that will be receiving the form. If the customer requires the recipient of the secure form to change based on the URL used to access the form, the txtTo field can be replaced with a procedure: DataMotion will configure the recipient domain for the customer's Corporate License. The URL that the customer uses to point to the Secure Form can specify the recipient's prefix via the "to=" query string value. For example, if the server is configured with the domain @customer.org, the recipient of the secure form will be user@customer.org when the URL is:

  » For *DataMotion SecureMail* customers:
  https://ssl.datamotion.com/form.aspx?co=100&frm=TestForm&to=User

- **txtsubject** – the subject line of the message when the form is submitted

- **txtDone** – the name of the page that will be displayed after the form is posted to the DataMotion Portal -- i.e. "done" would display "done.html" when the message is successfully posted. This custom page is supplied by the customer as well; otherwise a generic "Message Sent Successfully" page is displayed.

All other form fields are placed in the body of the DataMotion message using field name and value pairs. To exclude a field from the message body, it should start with a double underscore "__". This is useful for input buttons, etc. that you do not want to be included in the message body.

ACCESSING SECUREFORM DATA

Once a form has been created, the data can be accessed two ways:

- **Manual Process** – all form data is delivered in an email and with attachments containing the form data in CSV or XML format.

- **Data Adapter** – an automated tool that will receive the form data from the specified DataMotion SecureMail account where it can then be integrated into workflows.

<div align="center">*   *   *</div>

This concludes the *DataMotion SecureMail Administration Guide*.