DataMotion SecureMail On-Premise Planning Guide

March 31, 2022
Part # 050014–04

DataMotion SecureMail On-Premise Planning Guide v4

Publication Date: March 31, 2022

Printed in the United States of America.

DataMotion, Inc. Confidential and Proprietary Information.

Published By:

DataMotion, Inc.
67 Park Place.
East Suite 301
Morristown, NJ 07960
USA

1 800-672-7233 or +1 973-455-1245

http://www.datamotion.com/

TABLE OF CONTENTS

TABLE OF FIGURES

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 3

Updated Appendices A, B, and C with appropriate hardware and software information to match the current installation requirements for DataMotion SecureMail and the SecureMail Gateway.

Version 2

Updated Appendices A, B, and C with appropriate hardware and software information to match the current installation requirements for DataMotion SecureMail and the SecureMail Gateway.

Version 1

The initial version of this document.

ABOUT THIS PUBLICATION

INTRODUCTION

Before a successful secure messaging system can be implemented, basic information about the environment must be shared, understood, and documented. Details about the way email is to flow in and out of the organization, the volume of email, the number and location of users, the number and organization of email servers and any other pertinent information relative to the email environment must be understood before the intended environment is proposed. Based on this information, DataMotion will make configuration recommendations and hardware recommendations and document the pre-requisite software needed to support the solution. It is incumbent on DataMotion to fully understand the environment this solution is going to support and for you to be in agreement.

The express purpose of this manual to make sure that information was successfully exchanged and understood by you and DataMotion well before hardware purchases are made and implementation begun.

INTENDED AUDIENCE

This manual is intended for anyone who will be installing DataMotion software, either in a hosted (i.e., Software-as-a-Service) environment or behind a firewall behind customer premises.

OTHER REFERENCES

This document does not provide steps or information about using DataMotion products. Administrator and End user guides are provided for those products as applicable.

ARCHITECTURE OPTIONS

ARCHITECTURE DECISIONS

Before installing a DataMotion Server, several determinations must be made based on security and performance or the requirement for high availability of the email system. The answers to these questions will determine which of the following architectures might apply:

1. Decide whether you will be using a one, two, or three-tier server architecture.
2. Decide which DataMotion service(s) to install on which server
3. Prepare your server(s) to run DataMotion services

A representative from DataMotion Professional Services can help you assess your computing environment and message processing needs to decide on how many servers to use and which services they will run. Please consult the Server Pre-Requisites section for detailed information on how to prepare your servers to run DataMotion services.

This guide shows examples of basic configurations and reasons for choosing each.

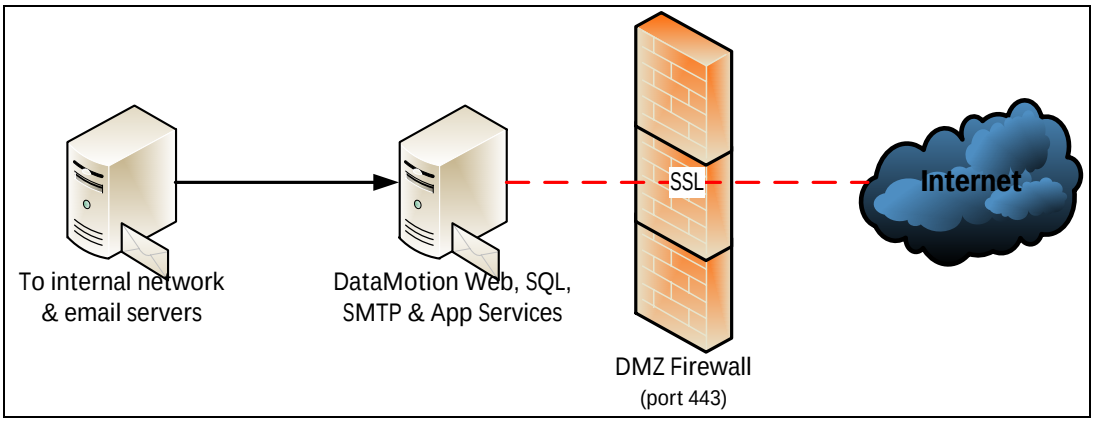
In addition, there are appendices in this manual that contain pre-installation to-do lists and hardware recommendations. These are useful for proper planning and must be reviewed and signed off on by representatives of both organizations at specific times during the lead up to implementation.

DataMotion systems are comprised of one or more Microsoft-compatible servers (e.g. Dell, HP/Compaq, IBM, etc). Your data center and architectural requirements will help you determine how many servers to use.

ONE SERVER SOLUTION

A one-server solution combines Web, SMTP, and database services, and is often referred to as an appliance. This type of system is placed in your DMZ, along with any existing Web or internet servers as shown in ***Figure A-1***. The near plug-and-play simplicity of this solution is its primary advantage. The main drawback is that message and user data, although stored using encryption in the database, reside in the DMZ, and may be less secure than multiple server solutions. In addition, a single server solution presents a single point of failure, and does not scale as well as multiple server architecture.

Figure A-1 – DataMotion Server Configuration (One Server)



NOTE: SMTP will relay outbound email waiting notices via your email server, or can send it directly with DMZ Port 25 open.

Suggested scenarios addressed by a one server solution.

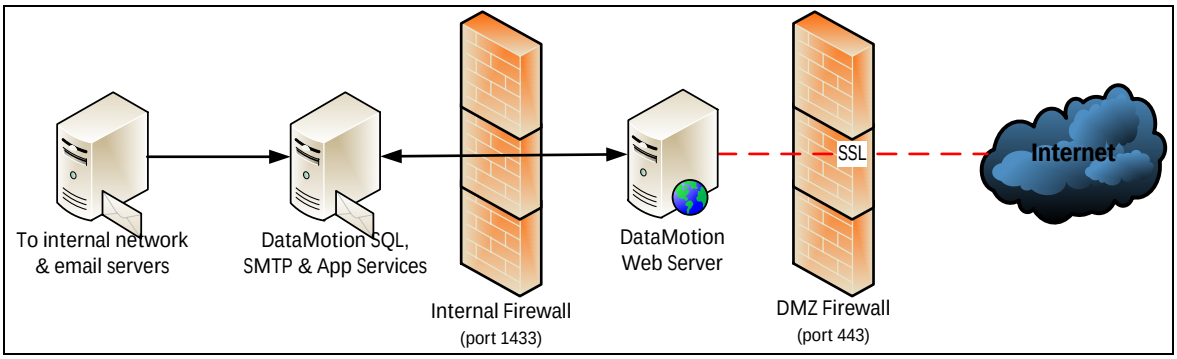
A one server solution provides secure email for corporate departments and for businesses, law firms, healthcare service providers, etc. It clicks into your network and works with your existing email server to provide secure email to any Internet recipient.

- Requires no end-user training or additional IT support
- Installed in your network or co-location facility
- Works with your existing email server, such as Microsoft Exchange, HCL Domino or Micro Focus GroupWise.
- Scales to hundreds of users with no significant administrative overhead
- Enables two-way secure messaging between your employees and customers
- Seamlessly integrates with your existing web site design
- Provides all the security features of the DataMotion service

TWO SERVER SOLUTION

A two-server solution typically divides DataMotion Server into a Web server that resides in the DMZ, and a database server placed behind the internal firewall as shown in *Figure A-2*. In this scenario, the SMTP service can run either on the Web or on the database server, depending on your preferences. The primary advantages of this approach are better performance and the placement of sensitive data behind the internal firewall.

Figure A-2 – DataMotion Server Configuration (Two Server)

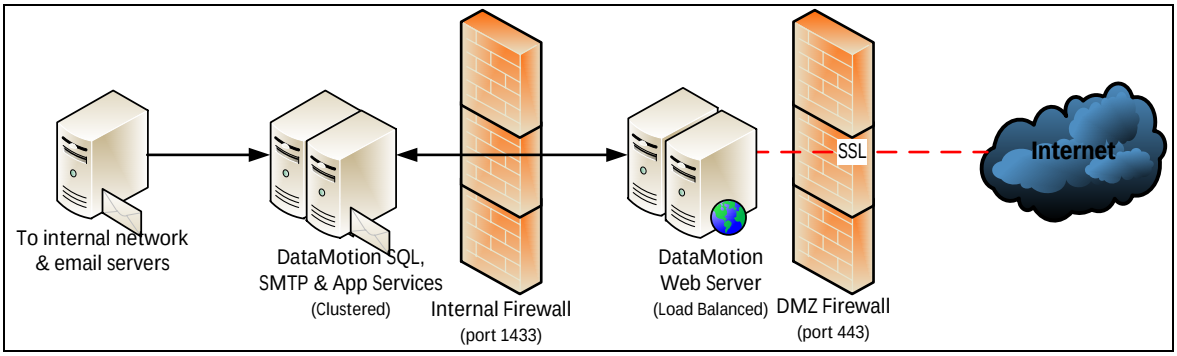


NOTE: SMTP will relay outbound email waiting notices via your email server or can send it directly if run on the DataMotion Web server with DMZ Port 25 open.

FAULT TOLERANT SOLUTION

You can also create a fault-tolerant solution that allows for the addition of two or more load-balanced Web servers, as shown in ***Figure A-3***. You can accomplish this using standard Microsoft operating system methods (e.g. Windows Server with Network Load Balancing), or by a third-party hardware load balancer. Through similar means, you can cluster the internal database and the application services server using standard Microsoft server techniques (e. g. Windows Server 2012 R2, SQL Server 2012 R2 Enterprise, or later). For a high-volume, high-traffic environment, a 3rd server running the application cluster can be implemented. (Note: clustering architecture is beyond the scope of this document.) A fault tolerant design provides increased system performance and eliminates many single-point-of-failure issues. Fault tolerant configurations are used by many enterprises to provide mission critical secure messaging to their employees, vendors, partners, and customers.

Figure A-3 – Fault tolerant DataMotion Server configuration

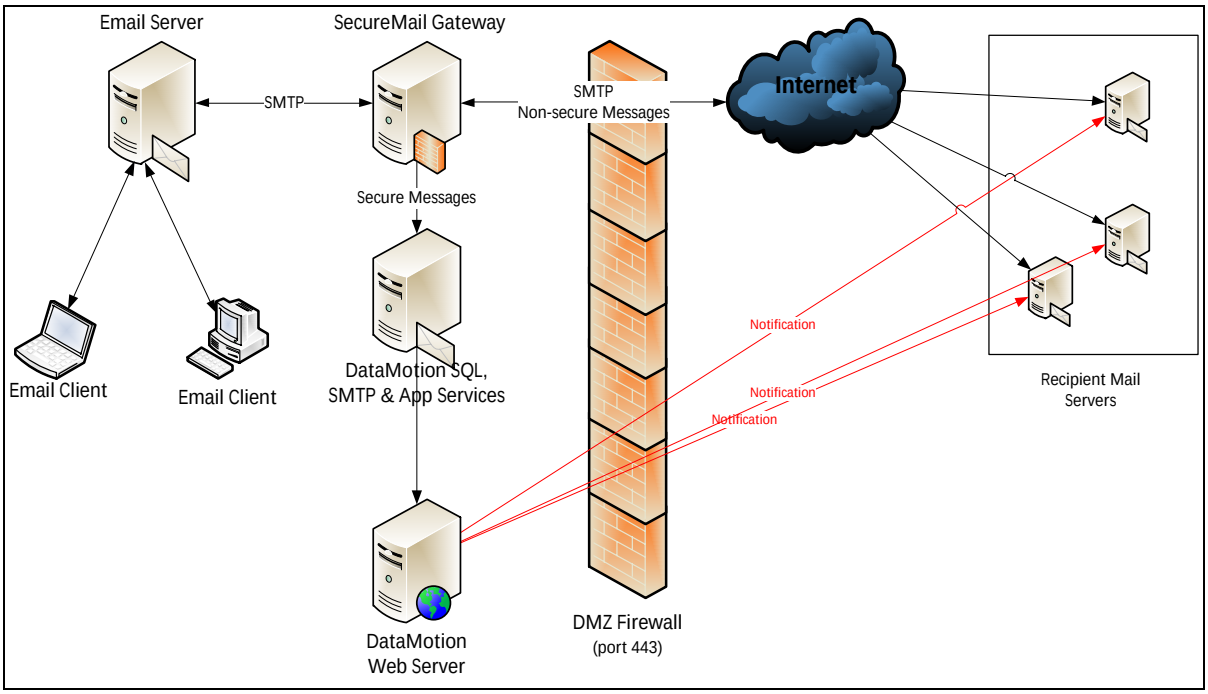


NOTE: SMTP will relay outbound email waiting notices via your email server, or it can send it directly if run on the DataMotion Web server with DMZ port 25 open.

CONTENT FILTER INTEGRATION

You can configure all DataMotion Server configurations with popular content filters. *Figure A-4* depicts one such integration scenario, in which filtered messages are sent securely based on specific message content. In this scenario, the content filter relays messages to be sent securely to the internal DataMotion Server system or writes these messages to a directory that DataMotion Server is set to monitor. The benefit of the content filter architecture is that it is transparent to internal end users. Users send messages from their email client as usual, and the server-side content filter decides which messages to send securely. You can also combine this scenario with our Send Secure email client toolbar button to provide user-selected and system-selected secure messaging.

Figure A-4 – DataMotion Server Configuration with a Content Filter



APPENDIX A – SERVER PREREQUISITE LIST

Regardless of whether you choose one, two, or more servers for your DataMotion Server configuration, you must follow this basic list of prerequisites to prepare the server(s) before you can install the DataMotion Server software:

PREREQUISITES

DataMotion's SecureMail Gateway and Secure Messaging Software have the following Operating System requirements:

- Microsoft Windows Server (multiple options supported):
  - Microsoft Windows Server 2012 R2 64-bit
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
- Application Server Role with .NET Framework 3.5.1 installed
- Web Server (IIS) Role with IIS, ASP.NET and ASP installed
- Microsoft .NET Framework 4.8

One of the following databases must be available:

- Microsoft SQL Server 2012 Standard or Enterprise
- Microsoft SQL Server 2014 Standard or Enterprise
- Microsoft SQL Server 2016 Standard or Enterprise
- Microsoft SQL Server 2019 Standard or Enterprise

NOTE: A "per processor" license (as opposed to Client Access Licensing) is required because the Secure Messaging Software Web server will be using SQL Server.

The DataMotion Server needs the following network configurations:

- Determine the Fully Qualified Domain Name (FQDN) you will use for connections to the Web interface. This is usually a sub-domain of your primary domain. For example, if your domain is company.com, your DataMotion Server Web domain could be securemail.company.com.

  NOTE: Ensure the FQDN you choose is accessible from outside the firewall for Web portal access from the Internet.

- External Ports: Web Server to Internet

- Required: 443 (HTTPS / SSL)
- Optional: 80 (HTTP) – Used only for redirect to SSL
- 25 (SMTP) –Used for sending outbound email notices directly.

NOTE: You can route email to another SMTP gateway for Internet delivery.

- 53 (DNS) – Used for resolving addresses against a public DNS server.

NOTE: You can also point DNS to an internal server.

- Internal Ports: Web Server to Database (if multi-server configuration is chosen)
  - Required: 1433 (SQL) – Used for SQL connection between Web Server and SQL

The DataMotion Server needs to have an SSL certificate for securing web access:

- Generate an SSL certificate request for the FQDN you chose above (for example, securemail.company.com), and apply for an SSL Web server certificate through a public certificate authority (such as DigiCert, etc).

NOTE: It's best to obtain a certificate as early as possible in the installation process, as this procedure may sometimes be delayed by the certificate authority. Also, when you purchase an SSL certificate, you may choose either the standard certificate or the enhanced certificate, based on your own requirements.

- When you receive the certificate from the certificate authority, apply the new certificate to the virtual Web you created for the DataMotion Server Web installation.
- Test that HTTP and HTTPS/SSL access is established to the virtual Web via your Web browser. Perform this test both inside and outside of your firewall.
  - To test HTTP access from your browser, open the URL http://{url}.com. ({url} is whatever your domain for the web portal is).
  - To test HTTPS/SSL, open the URL https://{url}.com ({url} is whatever your domain for the web portal is).

Although no page will be displayed yet, a connection should be available.

APPENDIX B – HARDWARE REQUIREMENTS

The following hardware suggestion is for a high-availability, mission critical deployment. There are no brand requirements for either the processors or the servers themselves:

DATABASE SERVERS

- Two Clustered Microsoft SQL 2014, 2016, or 2019 Database Servers.
- Microsoft Windows Server (multiple options):
  - 2012 R2
  - 2016
  - 2019
- Dual Quad-Core Processors
- 8 Gigabytes of RAM
- 72 GB of hard-drive space (minimum)
- Extendable External Storage Array with 512 gigabytes of storage

SECUREMAIL GATEWAY SERVERS

- Two Load Balanced (or Round Robin DNS) SecureMail Gateway Servers
- Microsoft Windows Server 2012 R2 or later
- Dual Quad-Core Processors
- 4 Gigabytes of RAM
- 72 GB of hard-drive space (minimum)

WEB SERVERS

- Two Load Balanced IIS Web Servers
- Microsoft Windows Server 2012 R2 or later
- Dual Quad-Core Processors
- 4 Gigabytes of RAM
- 72 GB of hard-drive space (minimum)

APPENDIX C – CHECKLIST

DATAMOTION SOFTWARE PRE-INSTALL CHECKLIST

Operating System and Database

- Microsoft .NET Framework 4.0
- Windows Server 2012 R2 or later for load balancing or clustering
- A Per Processor SQL Server 2012 or later
- A Network Engineer, Firewall Engineer, and SQL DBA

Web Tier Configuration

- IIS 7.5 (or later) with ASP.NET and Active Server Pages
- A host header value with your DataMotion URL and IP address should be configured under the default IIS website
- An SSL Certificate for your DataMotion URL. We recommend that you request and apply the Certificate right from your web server.
- The Documents tab under your default virtual server should list `l.aspx` and `default.aspx`.
- Any ISAPI filters should be disabled.
- If you plan to use Active Directory to authenticate your internal users, please configure you web server with a 2nd IP address.
- If you do not plan on using the DataMotion SecureMail Gateway as your email gateway, then Microsoft SMTP should be installed and configured with your domain.
- The SME utilizes the following ports.
- External: Web Server to Internet
  - Required: 443 (HTTPS / SSL).
  - Optional: 80 (HTTP) – Used only for redirect to SSL.
  - 25 (SMTP) – Used for sending outbound email notices directly.
  - NOTE: email can be routed to another SMTP gateway for internet delivery.
  - 53 (DNS) – Used to resolve addresses against a public DNS server.
  - NOTE: you can also point DNS to an internal server.
- Internal: Web Server to Database (if multi-server configuration is chosen)
- Required: 1433 or whichever port SQL is bound to – Used for SQL connection between Web Server and SQL Database Tier Configuration.

SQL Tier

- Install the SQL Server management console and ensure that case insensitive collation is used, which is typically the default.
- SQL Management Console for administration.
- SA level credentials for installing the DataMotion database tier.
- If the SQL Server is to be used exclusively for DataMotion. Please enable cross-database ownership chaining at the server level. If not, we will enable it only for the DataMotion databases after the database tier has been installed.
- Port 1433 or whichever port SQL is bound to must be open for the IP address of the SQL Server.
- If internal security policies forbid you from running binaries on the SQL Server, we will provide instructions on installing the databases via an SQL script.

SECUREMAIL GATEWAY

The SecureMail Gateway can be installed with or without the DataMotion Server. We will discuss requirements for both configurations.

SecureMail Gateway with DataMotion SaaS

In this configuration, the SecureMail Gateway will scan outbound email for privacy rules, and route sensitive messages to the DataMotion SaaS for secure delivery to the recipient.

- The SecureMail Gateway has to be installed on a server with Microsoft SMTP disabled or un-installed. No other application on the server should utilize port 25.
- We will need your public IP for our ACL. We will provide you with ours for configuration on your SecureMail Gateway.
- The SecureMail Gateway requires Windows Server 2012 R2 or later with .NET Framework 4.0 or later.
- A list of IP addresses of servers which will access and relay via the SecureMail Gateway.
- Location of the SecureMail Gateway in your email stream. Depending on your needs, there are various options. It can sit between your internal email server and your edge gateway, or it can be your edge email gateway. If it's the latter, the SecureMail Gateway will need a public 'A' record and a public PTR record.
- If you want to receive secure messages in plain text format, you will need a Certificate for a TLS connection. You can elect to buy your own, or we will issue one.

SecureMail Gateway with Premise-based DataMotion Server

In this configuration, the SecureMail Gateway will scan outbound email for privacy rules, deliver sensitive messages to your DataMotion Server, and deliver messages generated by DataMotion Server to the recipient or your existing email gateway.

- The SecureMail Gateway has to be installed on a server with Microsoft SMTP disabled on un-installed. No other application on the server should utilize port 25.
- The SecureMail Gateway requires Windows Server 2012 R2 (or later) with .NET Framework 4.0 or later.
- A list of IP addresses of servers which will access and relay via the SecureMail Gateway.
- Location of the SecureMail Gateway in your email stream. Depending on your needs, there are various options. It can sit between your internal email server and your edge gateway, or it can be your edge email gateway. If it's the latter, the SecureMail Gateway will need a public 'A' record and a public PTR record.
- The SecureMail Gateway can be installed on either the web or database server of your DataMotion Server. If the SecureMail Gateway is to only send notifications and process rules internally, then it can be installed on your database server, or another server in your internal network. If the SecureMail Gateway is to receive incoming TLS messages from business partners, then it will have to be installed on the DataMotion Server Web Tier or another server in your DMZ.

If you have any further questions or concerns, please do not hesitate to contact your Account Representative or Technical Support.

* * *

This represents the end of the *DataMotion SecureMail On-Premise Planning Guide*.