SECUREMAIL GATEWAY SYSTEM REQUIREMENTS

The SecureMail Gateway is designed to be scalable, supporting both small to large enterprise installations organizations needing Policy-based email filtering. This means that while the server can run on fairly low-end server hardware, it can also scale up to high-end clusters for high availability, mission critical deployments.

It is recommended that the Gateway be installed on its own server. This can be either a physical server or a virtual one, as long as it meets the requirements specified below.

Operating System Requirements

The Gateway requires one of the following operating systems:

- Microsoft Windows Server 2012/2012 R2 with SP2
- Microsoft Windows Server 2008/2008 R2 with SP2
- Microsoft Windows Server 2003/2003 R2 with SP2
- Microsoft .NET Framework 4.0
  - » The full .NET Framework 4.0 is required, not the Client version. The correct version can be found at http://www.microsoft.com/en-us/download/details.aspx?id=17718.

NOTE: While it is possible to install the SecureMail Gateway software on a 32-bit operating system this is not a recommended configuration.

Database Requirements (Optional)

While previous versions of the Gateway (called the Policy Engine or Policy Manager) required a database to maintain configuration data, the current version of the Gateway can be installed and run without a database.

If the SMGW will be using a database, one of the following must be available:

- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008/2008 R2, Any edition
- Microsoft SQL Server 2005, Any edition
- Microsoft SQL Express

SQL Server Express Editions are capable of supporting reasonably large organizations as a dedicated database for the Gateway, but it will not support high availability environments. To install the Gateway in a HA environment with a database, the Standard or Enterprise editions of SQL Server must be used.

IFilters

The Gateway utilizes IFilter plugins that are used by the Windows Indexing Service to be able to read the contents of file attachments sent through email. By utilizing these filters the Gateway is able

200 Park Avenue, Suite 302 Florham Park, NJ 07932 Tel: 973.455.1245 www.datamotion.com

to scan not only the email message but any attachments for matches to the filtering rules that have been configured on the server.

At a minimum, it is recommended that the following IFilters be installed on the Gateway server:

- Adobe PDF iFilter 11 (note that this is for 64-bit only, to install the 32-bit iFilter, install Adobe Acrobat Reader 11)
- Microsoft Office 2010 Filter Packs (note that this includes all previous versions of Office filters)
- Microsoft Office 2010 Filter Packs SP2 (note that the above filter pack needs to be installed first)

IFilters can be installed at any time and are automatically made available by the operating system.

ANTIVIRUS CONFIGURATION REQUIREMENTS

DataMotion recommends that antivirus software not be installed on the server where the Gateway is installed, but that messages should be scanned directly on the mail server (i.e. the Exchange server) or on the client computer.

In environments where antivirus software must be installed on the Gateway server, the mail drop folders should be added to the exclusion list in the antivirus. These folders are used during the process of sending messages and anything in here is immediately deleted after it has been processed.

The following path is an example of the location that should be excluded on Windows Server 2008/2012/2012R2:

```
C:\ProgramData\DataMotion\Gateway\SMGSvc1
```

The following path is an example of the location that should be excluded on Windows Server 2003:

```
C:\Documents and Settings\All Users\Application
Data\DataMotion\Gateway\SMGSvc1
```

This example assumes the default installation path is used. If multiple Gateway virtual servers are installed, there may be multiple `SMGSvcX` folders (where X is a number), and all must be excluded from scanning.

HARDWARE REQUIREMENTS

While software is fairly fixed in terms of requirements, hardware is entirely different. The level of hardware required is highly dependent on the load placed on the server, with a higher load requiring better hardware. The levels listed here provide a guide to the amount of use that can be done successfully on the listed amount of hardware.

The number of users listed as able to be supported by a configuration assumes an average user sends approximately 100 messages a day and that 40% of those messages are to external users (meaning the message would be filtered by the Gateway).

200 Park Avenue, Suite 302 Florham Park, NJ 07932 Tel: 973.455.1245 www.datamotion.com

NOTE: The Gateway can be installed on a 32-bit system and may be suitable for small environments, but it is recommended to use 64-bit systems whenever possible.

Virtualization

The SecureMail Gateway is fully compatible with any hypervisor that supports the required operating systems. The hardware listed below should be considered guidelines for both physical and virtual systems as the resources necessary to support the number of users shown.

Basic Hardware Requirements – Approximately 1,000 average users

- 64-bit Dual Core processor, ~3GHz speed
- 2GB of RAM
- 100GB of disk space

Recommended Hardware Requirements – Approximately 5,000 users

- 64-bit Quad Core processor
- 4GB of RAM
- 200GB of disk space

High Performance Hardware Requirements – Approximately 10,000 users

- Dual 64-bit Quad Core processor
- 8GB of RAM
- 200GB of disk space

High Availability

High availability environments are supported in one of two ways: Microsoft Clustering or through a Virtual Machine.

Contact DataMotion support for specific high availability configurations, including clustering.

200 Park Avenue, Suite 302 Florham Park, NJ 07932 Tel: 973.455.1245 www.datamotion.com