SecurityGateway

SecurityGateway Installation Guide

Pre-Deployment Preparation

Before deploying SecurityGateway, the following DNS records must be updated in order to route email and web (HTTP) traffic to the appropriate IP addresses.

1. **The MX record of the domain SecurityGateway will be protecting**
   - This domain's MX record must point to the IP address or domain/host name of the server SecurityGateway is installed on (not the email server SecurityGateway is protecting).

     Note: *If the domain name used for your email points to the domain name of SecurityGateway, then that domain name will need an A record pointing to the IP address of the SecurityGateway server.*
2. **The domain name of the email server SecurityGateway is protecting**
   - This domain will need an A record that points to the IP address of the email server SecurityGateway is protecting.
3. **The domain name of the SecurityGateway server**
   - This domain's A record must point to the IP address of the SecurityGateway server. Leave this domain name as the top-level domain.

Example: The following domains exist with these DNS records, where 10.0.0.1 is the web server for example.com:

example.com
A = 10.0.0.1
MX = mail.example.com

mail.example.com
A = 10.0.0.2

In the above example, web traffic is routed to 10.0.0.1 via the A record, and inbound email traffic is routed to mail.example.com via the MX record. The above A record lists the IP address that connections to mail.example.com should be routed to (10.0.0.2).

When setting up SecurityGateway for this existing domain, example.com, on a new computer with an IP address of 10.0.0.3, the MX record for the domain example.com will need to be updated, and an A record for the SecurityGateway server (sg.example.com) will need to be created. The DNS records would then be:

example.com
A = 10.0.0.1

MX = sg.example.com

mail.example.com
A = 10.0.0.2

sg.example.com
A = 10.0.0.3

In the above example, web traffic for example.com is still routed to the existing web server at 10.0.0.1, but the MX record has been updated to route inbound mail to the new SecurityGateway server via the new MX record (sg.example.com). A new A record for sg.example.com that points to the IP address of the SecurityGateway server (10.0.0.3) was created.

Installation & Setup Instructions

Step 1 - Install SecurityGateway

1. Download the SecurityGateway installer from www.mdaemon.com. Select **Downloads | SecurityGateway for Email Servers**. Click the **Download Now** button, click on your **language selection**, and then click on **Save File**. [Figure 1-1]
2. Double-click the **SecurityGateway installer** on your Windows desktop to begin the installation, and then click **Next** to continue.
3. Click on **I Agree** to indicate that you have read and agree to the terms listed above.
4. Select a destination directory for the installer to copy files to, then click **Next**. [Figure 1-2]
5. On the **Select Database** screen, select the first option if you would like SecurityGateway to create and use an embedded Firebird database (default option), or select the second option to use an external database, and then enter the database server details.
6. Select your preferred installation type: [Figure 1-3]
   A. Select the first option to install a fully functional free trial of SecurityGateway.
   B. Select the second option if you have already purchased a license for SecurityGateway, and enter your registration key in the box below. Click **Next** to continue. If you selected the Free Trial option, click **Next** on the *Trial SecurityGateway for Email Servers free for 30 days* screen.
7. On the following Customer Information screens, enter your name, company, country, and email address. *If you are installing the free trial, be sure to enter a valid email address. Your trial key will be sent to this address, and must be entered before proceeding to the next step.* Click **Next** to continue.
8. Enter the trail key that was emailed to you from the previous step, and then click **Next** to continue.
9. On the **Ready to Install** screen, click **Next** to continue with the installation process. The SecurityGateway files will be copied to the destination directory.

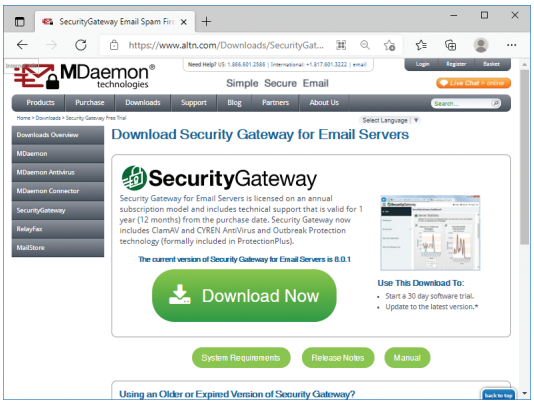

Figure 1-1

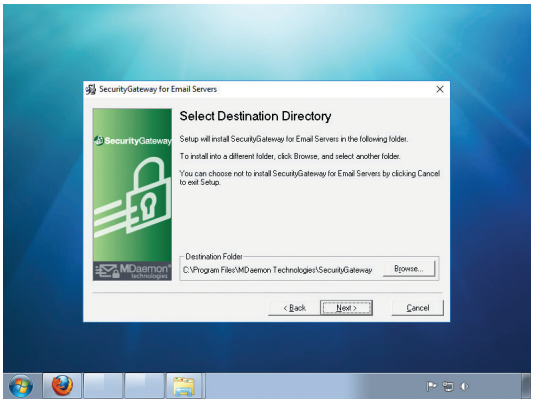

Figure 1-2

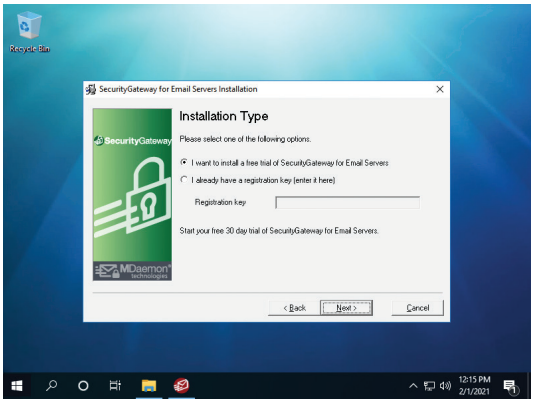

Figure 1-3

Step 2 - Enter your Domain Name

1. Enter the **Domain Name** that SecurityGateway will be protecting *(e.g. example.com)*.
   [Figure 2-1]

   Note*: If SecurityGateway will protect multiple domains, enter the first domain here. The remaining domains can be added later.*

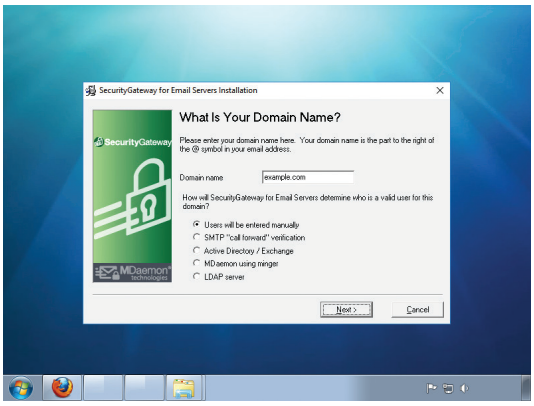

Figure 2-1

Step 3 - Choose a User Verification Source

1. Choose the type of User Verification Source SecurityGateway will use to confirm the validity of users and local email addresses. [Figure 2-1]

   Note: *This can be changed later, and there can be multiple selections. This is only the initial setting. After you have selected your initial user verification source, click the Next button to continue.*

The Six User Verification Source Types Are:

1. **Users will be entered manually** - The administrator(s) will enter each user/address manually to set them up in SecurityGateway.
2. **SMTP "call forward" verification** - This verification source uses an SMTP session to determine whether email addresses exist on the mail server. If they do, they're automatically added to the database and the mail is accepted.

   Note: *When using SMTP "call" forward, at this time aliases will also count as users, so administrators should be aware of this when choosing a license size.*

3. **Active Directory / Exchange** - SecurityGateway will query the AD/Exchange server to confirm the validity of any unknown email addresses. If they're found, they're automatically added and the full user list is pruned for any changes.

   Note: *When using Active Directory, any aliases will be recognized as such and will not be counted as a "user" in terms of licensing.*

4. **MDaemon using Minger** - SecurityGateway will check with MDaemon's own Minger server to confirm the validity of any unknown email addresses.

   Note: *When using this verification method, any aliases will be recognized as such and will not be counted as a "user" in terms of licensing.*

5. **LDAP server** - SecurityGateway will query an LDAP database to confirm the validity of unknown local addresses.

   Note: *LDAP (Lightweight Directory Access Protocol) is the Internet protocol for directories and is found in a variety of applications, including some mail servers.*

   As with SMTP verification, at this time aliases will also count as users, so administrators should be aware of this when choosing a license size.

6. **Office 365** - SecurityGateway will query the Office 365 Azure Active Directory server to confirm the validity of any unknown email addresses. If they're found, they're automatically added and the full user list is pruned for any changes.

   Note: *To allow SecurityGateway to access the Office 365 tenant, the Office 365 plan requires Exchange Online. Please make sure the Office 365 plan includes this feature.*

Step 4 - Email Server Details

1. **Description** - This field will auto-populate with the domain information you entered on the previous screen. You can customize this data as needed. [Figure 3-1]
2. **Host Name or IP** – This field will auto-populate with the domain information you entered on the previous screen.

   Note: *If you have a specific port that you wish to use for your internal mail, it can be specified here.*

3. **Port** - Set the port that SecurityGateway will use when connecting to the mail server to send email (the default is 25).
4. **Requires SMTP Authentication** - Finally, if you would like SecurityGateway to authenticate with the domain mail server when sending email, those credentials can be entered here during the installation.
5. Click the **Next** button to continue when finished.

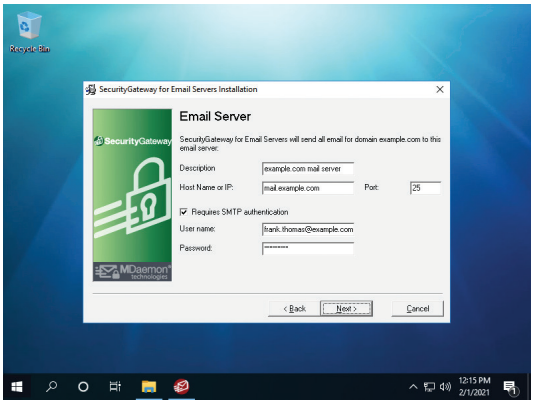

Figure 3-1

Step 5 - Administrator Account Setup

Set Up Administrator Account (Local user) - This account is a global administrator account with access to all of SecurityGateway's settings. Additional accounts and administrators can be added after the installation. [Figure 3-2]

1. Enter the user's **Full name** *(e.g. Frank Thomas)*.

   Note: *The mailbox name is the part of the email address to the left of the '@' sign (e.g. if the email address is frank.thomas@example.com, the mailbox name would simply be "frank.thomas").*

2. **Set the user's password** - It is suggested that you choose a "strong" password, consisting of eight or more characters including capital and lower case letters, numbers, and special characters not defined as letters or numerals: ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /
3. **Set Up Administrator Account (External)** - An administrator can be external to the SecurityGateway domains. Simply choose the external user option and instead of defining the administrator's mailbox, enter the full, external email address. This will be their username when logging in to SecurityGateway.
4. Click the **Next** button to continue.

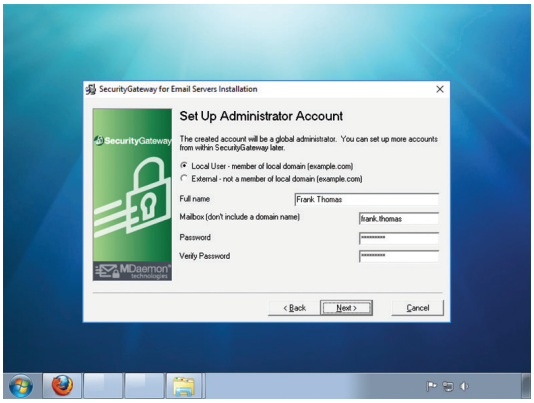

Figure 3-2

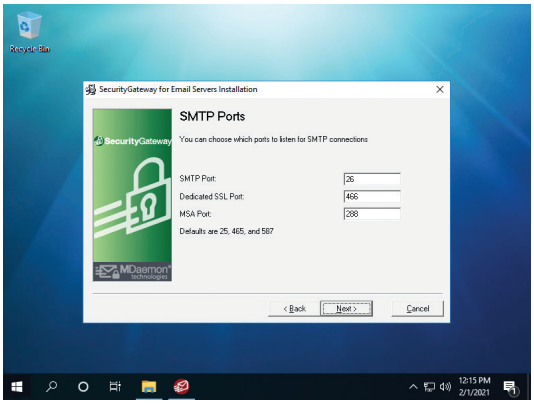

Figure 3-3

Step 6 - SMTP Port Configuration

1. **SMTP Ports** - For most installations these won't need to be altered. [Figure 3-3]

   The ports should be left as their defaults, unless there are special circumstances such as, for example, a custom setup for mail on the internal network, or when a router is redirecting ports.

2. Click the **Next** button to continue.

Step 7 - HTTP User Interface

1. **HTTP Host Name** - This field will auto-populate with the domain information you entered on a previous screen. [Figure 4-1]

   Note: *If you leave the domain name as the top-level only (e.g. example.com), it may resolve to the Web server and not to SecurityGateway.*

2. The default port used to access the SecurityGateway interface is 4000 and the SSL port is 4443.

   These settings are important as they are used for configuring SecurityGateway's web interface. This host name and these ports will be used in login links created by SecurityGateway for the various notification messages and quarantine summaries sent to users.

3. Click the **Next** button to continue.

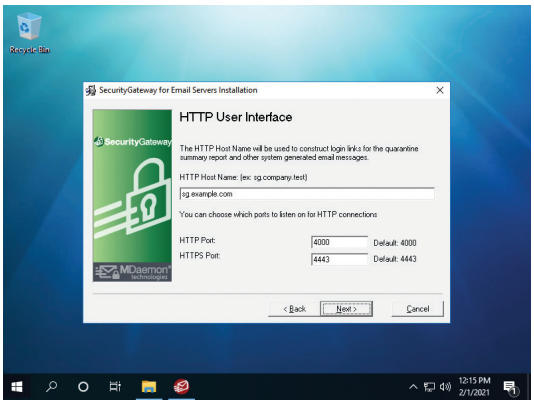

Figure 4-1

Step 8 - Finishing Setup

1. Check the first box to start SecurityGateway.
2. Check the second box to view the release notes.
3. Click **Finish** to complete the installation. [Figure 4-2]

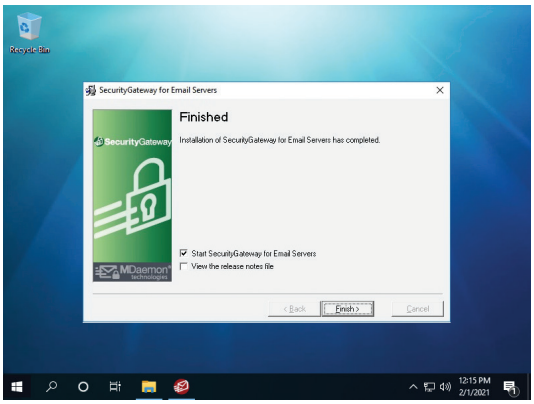

Figure 4-2

Step 9 - Login

Open SecurityGateway and log in. [Figure 4-3]

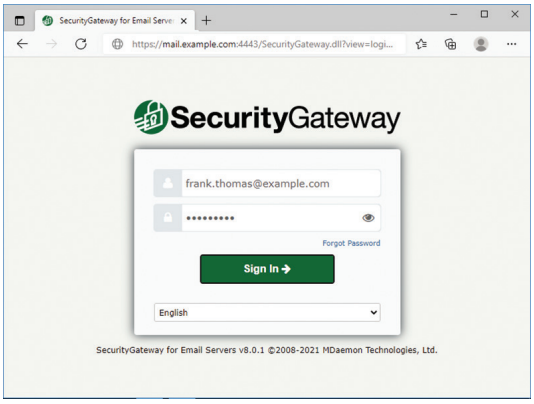

Figure 4-3

Appendix: Firewall/Router Configuration

For SecurityGateway to be able to communicate with external networks, your firewall must be configured to allow communication over the following ports:

25 (SMTP - Non-SSL)
465 (SMTP - SSL)
4000 (HTTP - Non-SSL)
4443 (HTTPS - SSL)
587 (MSA - Inbound)
110 (POP - Non-SSL)
995 (POP - SSL)
53 (DNS)
389 (LDAP User Verification)
4069 (MDaemon User Verification via Minger)

MDaemon® technologies