

SecurityGateway for Email Servers Installation Guide

Step 1 - Install SecurityGateway

- Download the SecurityGateway installer file from **www.altn.com**. Select **Downloads | SecurityGateway for Email Servers**. Click **Download Now** button, click your **language** selection, fill out the form, click **Continue**, and click **Save File**. The installer will now download. [Figure 1-1]
- Double-click the **SecurityGateway installer** on your Windows desktop to begin the installation. Then click **Next** on the Welcome screen.
- Select your **Country** and **Language** in the drop-down menus, **check the box** indicating that you have read and agree to the terms listed above, then click on **Next**.
- Select a destination directory for the installer to copy files to, then click **Next**. [Figure 1-2]
- Select your preferred installation type: [Figure 1-3]
 - Select the first option to install a fully functional trial of SecurityGateway.
 - Select the second option if you have already purchased a license key for SecurityGateway.
- On the following Customer Information screens, enter your country, address, and other requested information. *If installing a trial, then 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.
- 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

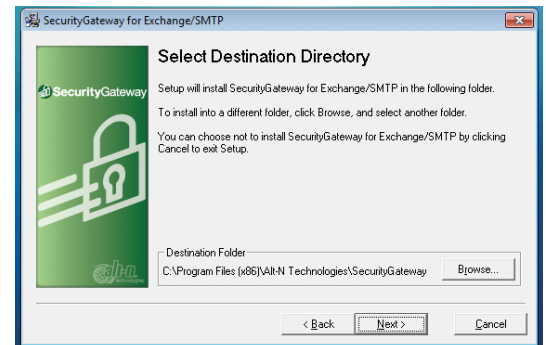


Figure 1-2

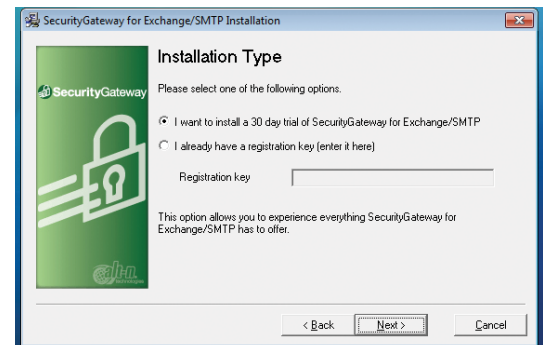


Figure 1-3

Step 2 - Your Domain Name

Enter the **Domain Name** used in your email address (e.g. example.com).

[Figure 1-4]



Note: If SecurityGateway will protect multiple domains, enter the first domain here. The remaining domains can be configured via the web interface once installation is complete.

Step 3 - Choose a Verification Source

Choose the type of User Verification Source SecurityGateway will use to confirm the validity of users and local email addresses. [Figure 1-4]



Note: This may be changed later, and there may 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 Five User Verification Source Types are:

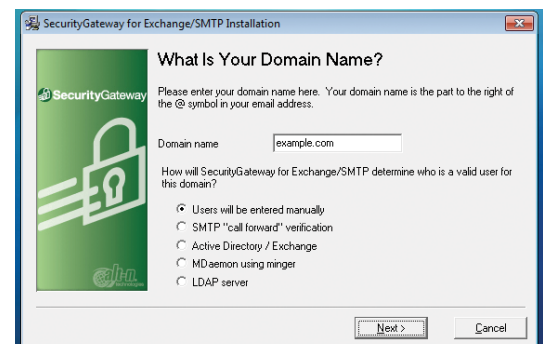


Figure 1-4

- 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. ActiveDirectory / 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 ActiveDirectory, 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.

Step 4 - Email Server Details

- A. Description** – This field will auto-populate with the domain information you entered on the previous screen. You can customize this data as needed.

[Figure 2-1]

- B. 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 during the install.

- C. Port** – Set the port that SecurityGateway will use to send mail to the server (the default is 25).

- D. Requires SMTP Authentication** – Finally, if you would like SecurityGateway to authenticate with the domain mail server when sending emails, those credentials can be entered here during the installation.

- E.** Click the **Next** button to continue when finished.

Additional Information – Preparing for Install

- A. The domain name used in the email address** – This is the first domain you intend to have SecurityGateway protect.

1. This domain’s MX record needs to point to SecurityGateway’s IP address or SecurityGateway’s domain name (ensure this isn’t the email server SecurityGateway is protecting).

2. **Note:** If the name used in the email address points to the domain name of SecurityGateway, that domain name will need an A record pointing to the IP address of SecurityGateway.

- B. The domain name of the email server**

SecurityGateway is protecting – This domain name needs an A record that points to the email server SecurityGateway is protecting.

- C. The domain name of the SecurityGateway server**

– Make sure this domain’s A record points to the SecurityGateway server. Leave this domain name as the top-level domain.

Let’s say these domains exist with these DNS records, where 10.0.0.1 is the web server:

example.com	mail.example.com
A = 10.0.0.1	A = 10.0.0.2
MX = mail.example.com	

Setting up SecurityGateway for this existing domain, example.com, and there is a new computer with SecurityGateway at the IP 10.0.0.3. The domain example.com’s MX record needs updating and sg.example.com needs to be created. The DNS records would then be:

example.com	mail.example.com
A = 10.0.0.1	A = 10.0.0.2
MX = sg.example.com	
	sg.example.com
	A = 10.0.0.3

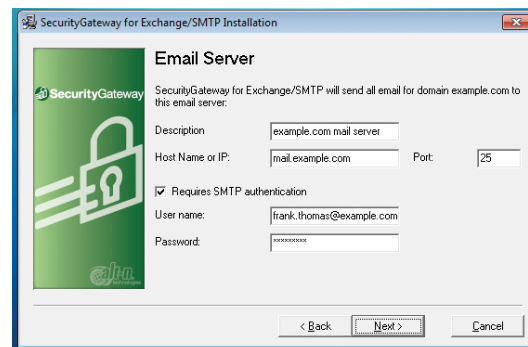


Figure 2-1

Step 4 - 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 3-1]

A. 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”).

B. 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:
 ` ~ ! @ # \$ % ^ & * () _ - + = { } [] \ | ; : ‘ ‘ < > , . ? /

C. 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.

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

Figure 3-1

Figure 3-2

Step 5 - SMTP Port Configuration

SMTP Ports – For most installations these won’t need to be altered.

[Figure 3-2]

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.

Click the **Next** button to continue.

Figure 3-3

Step 6 - HTTP User Interface

HTTP Host Name – This field will auto-populate with the domain information you entered on a previous screen. [Figure 3-3]



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.

The default listening port of the interface is 4000 and the SSL listening 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.

Click the **Next** button to continue.

Step 7 - Finishing Setup

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

Step 8 - Login

Open SecurityGateway and log in. [Figure 4-2]

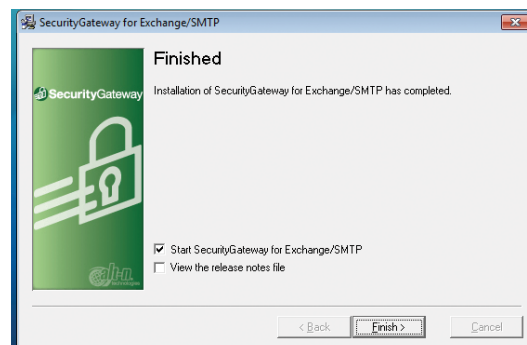


Figure 4-1



Figure 4-2