alt-n technologies

Trusted Messaging Solutions

SecurityGateway
For Exchange/SMTP Servers

Quick Start Guide

Contents

Step 1 — Download Install Files

Ensure you've downloaded the latest versions of both SecurityGateway and the ProtectionPlus plug-in from:

Double-click the SecurityGateway installer to begin the installation.

Once you've launched the installer, this will bring up the splash screen.

Step 2 – Welcome Screen

At the welcome screen, click "Next" to continue.

![SecurityGateway For Exchange/SMTP Servers]

Step 3 – License Agreement

At the License Agreement, please read the terms and click "I Agree" button to continue.

Step 4 – Installation Location

Select a destination directory for the installer to copy files into.

Click the "Next" button to continue.

By default, SecurityGateway installs into the \Program Files\ directory for Windows Vista compliance, but any directory location can be specified.

Step 5 – Registration Information

Enter your registration information.

Click the "Next" button to continue.

Leaving the registration key blank creates a 30-day trial key as with all of Alt-N's products.

Step 6 – Begin Installation

Click the "Next" button to continue with the installation process.
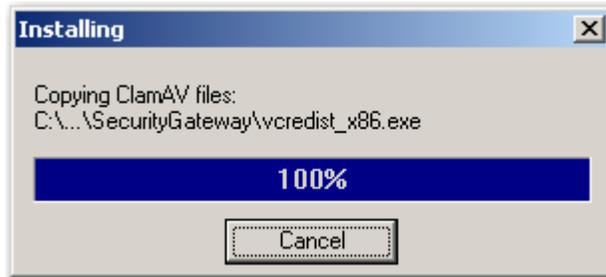
The files are copied to the destination directory.
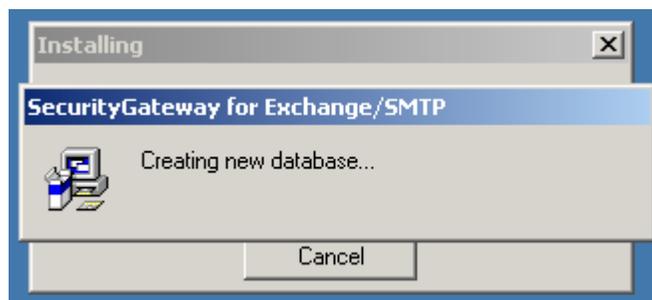
The database is then created.

Step 7 – Your Domain Name
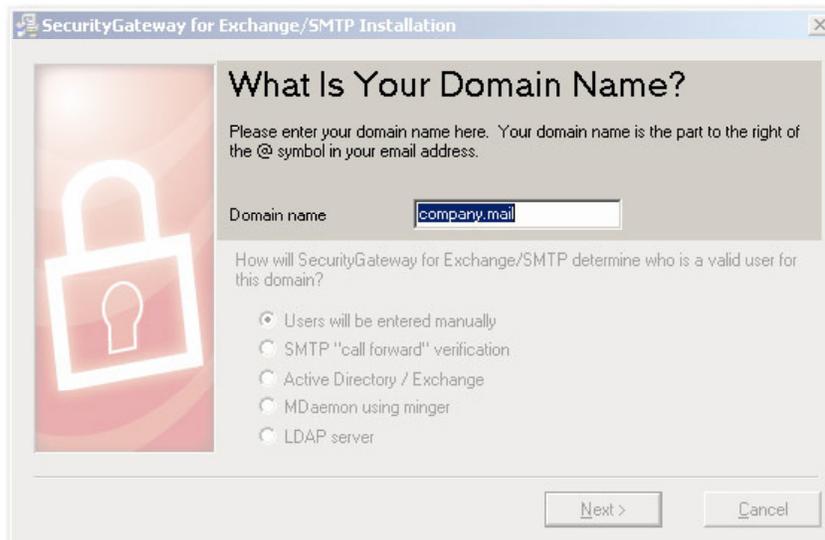
Enter the domain name used in your email address (e.g. example.com).

If there are multiple domain names to be setup in SecurityGateway, enter the first one here, and during the setup the others can be configured once installation is complete.

Step 8 – Choosing a Verification Source
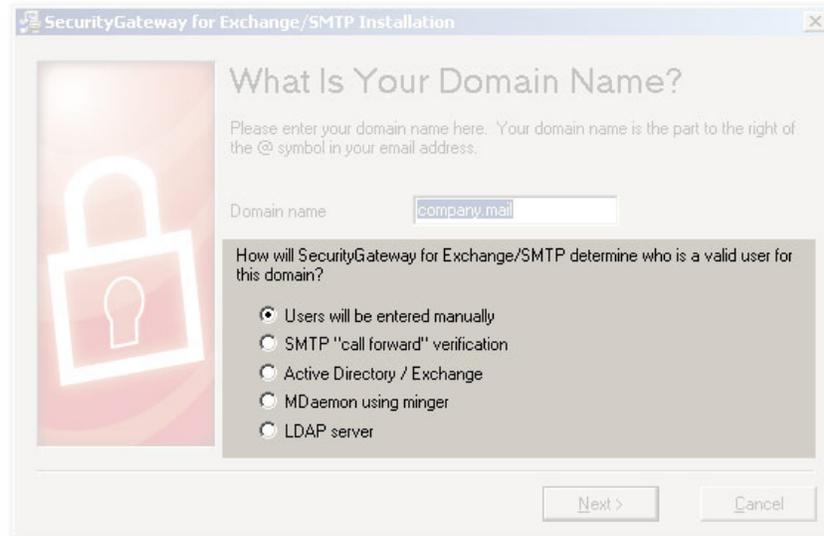
Choose the type of User Verification Source SecurityGateway will use to confirm the validity of users and local email addresses.

⚠️ *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:

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 accepted.

⚠️ *When using this verification method, 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 pruned for any changes.

⚠️ *When using this verification method, 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.

> *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.

> *LDAP (Lightweight Directory Access Protocol) is the Internet protocol for directories and found in a range 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 9 – Email Server Details
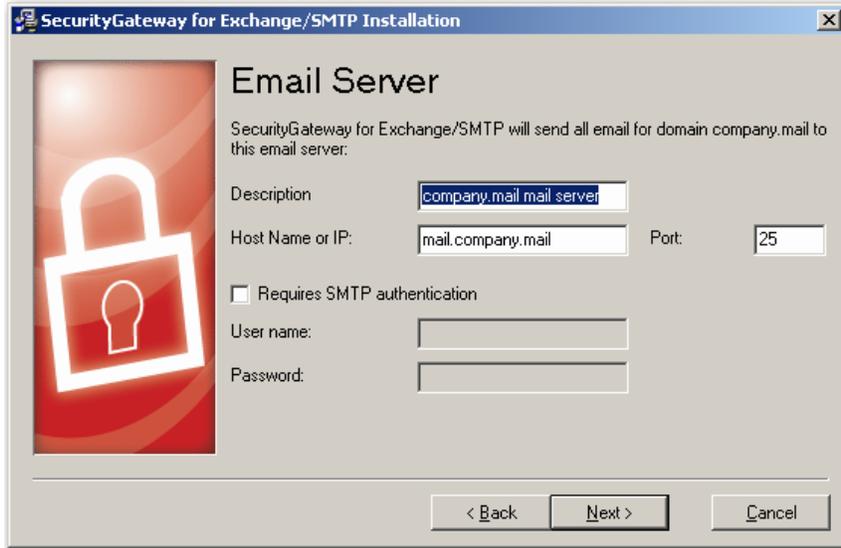
Description — This field will auto-populate with the domain information you entered at the previous screen.

Host Name or IP — This field will auto-populate with the domain information you entered at the previous screen.

Port — Set the port that SecurityGateway will use to send mail to the server (the default is 25).

> *If you have a specific port setup for your internal mail, it can be accommodated here during the install.*

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

Click the "Next" button to continue when finished.

Step 10 – 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 set up after the installation.

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

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').

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

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.

Click the "Next" button to continue.

Step 11 – SMTP Port Configuration
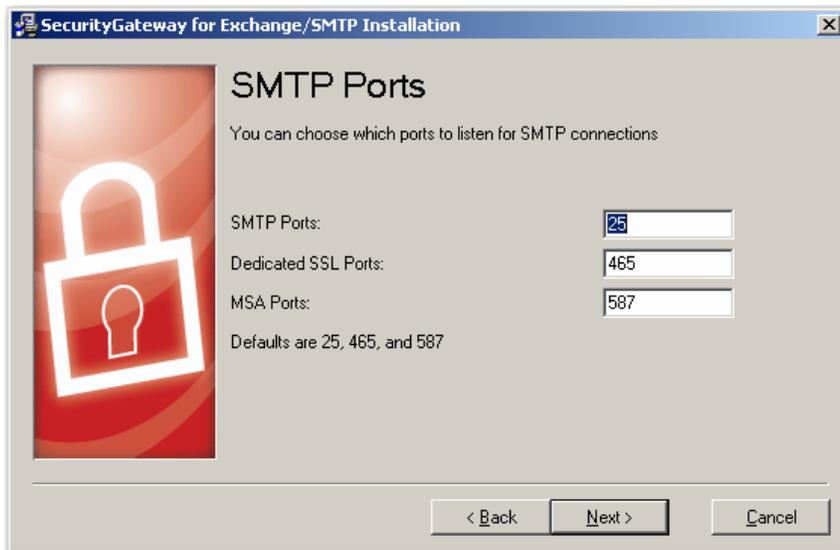
SMTP Ports — For most installations these won't need to be altered.

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

Click the "Next" button to continue.

Step 12 – HTTP User Interface
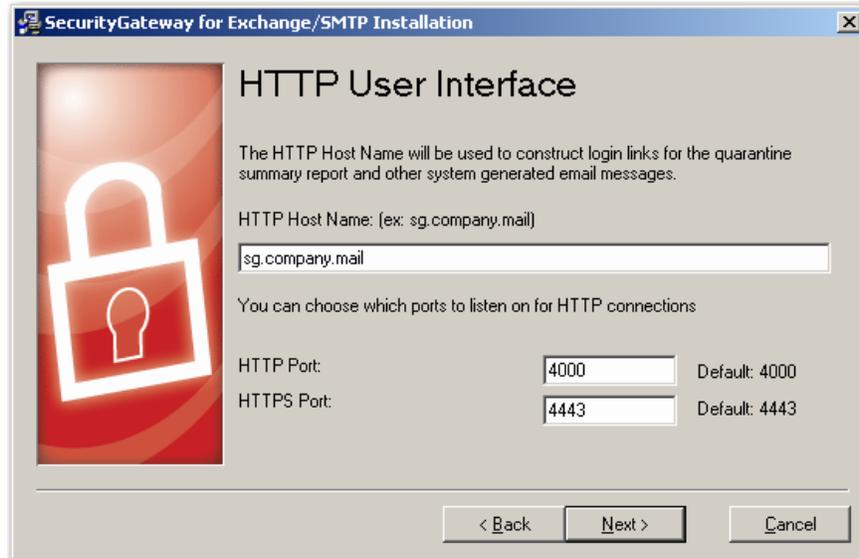
HTTP Host Name — This field will auto-populate with the domain information you entered at the previous screen.

> ⚠️ *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.*

HTTP Port — For most installations these won't need to be altered.

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 13 – Final Steps
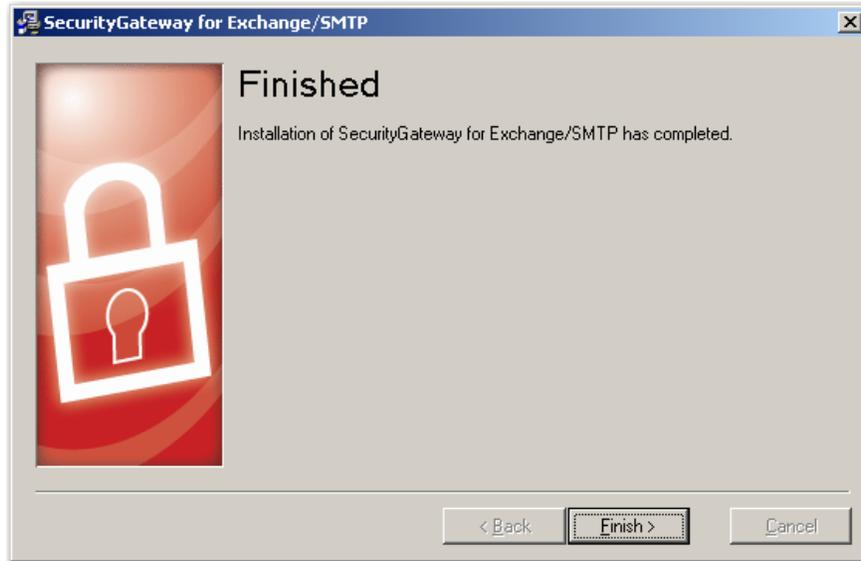
Your set-up is now complete.

Click "Finish" to complete the installation.

The installer starts the SecurityGateway service.

Step 14 – Log in
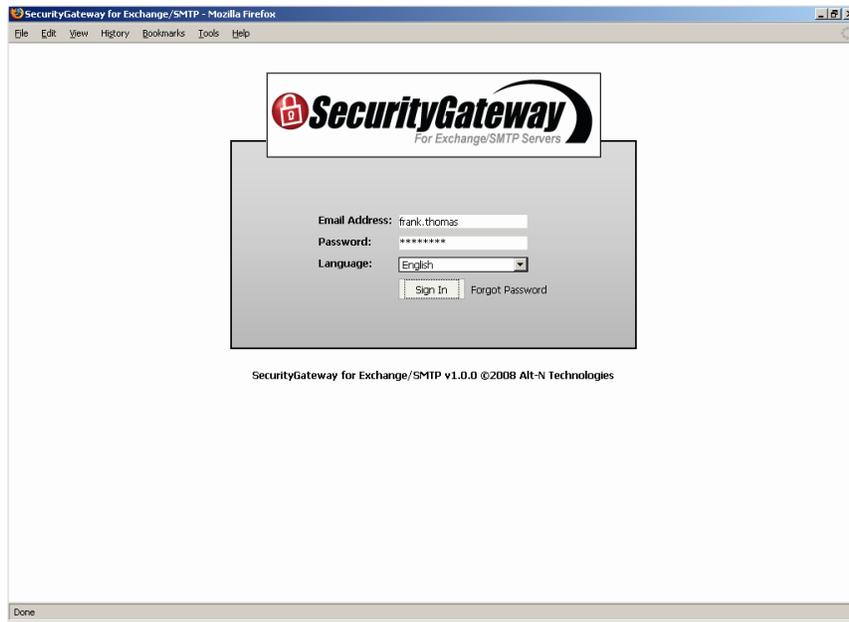
The SecurityGateway log in page opens.

You're now able to log in using the credentials of the global administrator you've just created during installation.

Quick Start Guide

Install Complete - Dashboard View
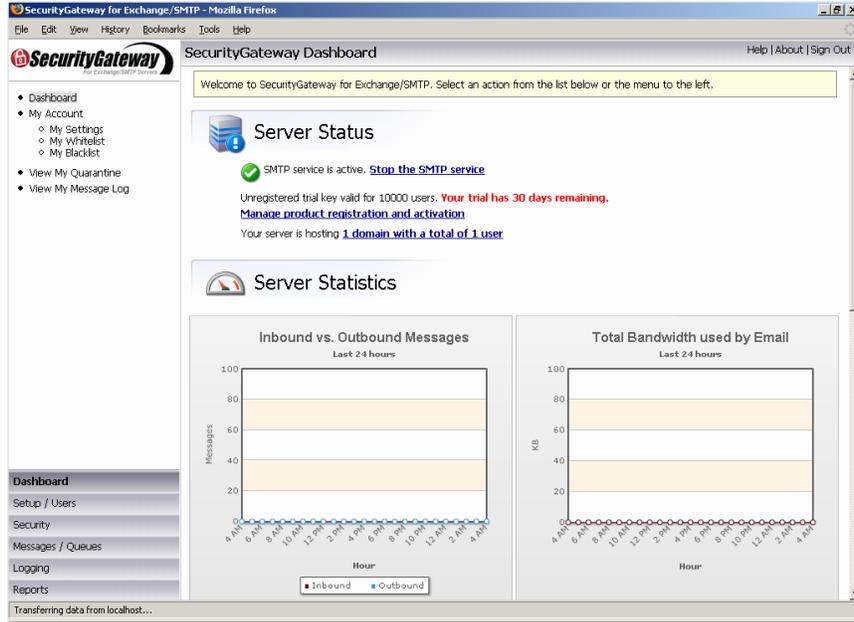
Congratulations, your installation is complete and you are ready to start using SecurityGateway!

Additional Information – Preparing for Install

1. The domain name used in the email address — This is the first domain you intend to have SecurityGateway protect.

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).

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.

2. 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.

3. The domain name of the SecurityGateway server — Make it's A record points to the SecurityGateway server. Leaving the domain name as the top-level domain name may point to the web server and not to SecurityGateway.

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

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

mail.example.com
A = 10.0.0.2

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
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