SecurEnvoy

SecurEnvoy Security Server

SecurMail Solutions Guide

SecurMail Solutions Guide

© 2009 SecurEnvoy

Printed: 2009 in United Kingdom

Publisher
SecurEnvoy Publishing

Managing Editor
SecurEnvoy Training Dept

Technical Editors
A Kemshall Technical Director
P Underwood WW Pre – Sales

Cover Designer
SecurEnvoy Marketing

Revision	
v1.1 AK PU	12/11/09

Contents

1.0 Pre requisites....4
2.0 SecurMail Overview....5
3.0 SecurMail Administration....9
3.1 SecurMail Virus Checking Integration....10
3.2 SecurMail Server Security Considerations....12

1.0 Pre requisites

Security Server

Software Requirements

- Windows 2003 x32 and x64 bit SP1 or higher, or Windows 2008 x32 and x64 bit
- IIS Installed
- Microsoft .NET 2.0 is installed (This is already installed upon Windows 2008 server editions)

Software Requirements

CPU – Pentium class processor 1 GHz or faster
HD - 150Mb of available hard disk space for application recommend at least 100GB for email storage.
RAM – 120Mb of available ram

User management

Connection to a Directory server (MS Active Directory, Novell e-Dir, Sun Directory Server and Open LDAP) is required. If no Directory server exists Microsoft ADAM can be used. This is installed and config via SecurEnvoy. A service account with read all and write access to the TelexNumber attributes.

Network Connectivity

- Security server needs read/write access to your Directory Server via LDAP (port 389) or LDAPS (port 636)
- If the Web SMS Gateway is being used to send SMS messages, the Security Server needs https access to the Internet (port 443)
- The Outlook client can be configured to upload all SecurMail messages over http (80) or https (443), if https is being used a trusted certificate is required upon the IIS server that is running as the SecurMail server.

Load Balancing and Redundancy

It is recommended that two SecurMail servers should be installed for redundancy. These servers can either be software or hardware clustered, alternatively the data directory can be installed upon NAS or a SAN device. The data directory path will be the same upon both SecurEnvoy SecurMail servers.

The IIS server needs to be configured so that they are active-active or active passive to each other. Layer 7 switches are one way to load balance across multiple IIS server running SecurMail.

Alternatively install Microsoft network load balancing (NLB) on both servers. Using NLB, the same data is stored on multiple servers, so if one becomes unavailable, the client is redirected to another server with the same information. Please see http://technet.microsoft.com/en-us/library/cc770558.aspx

These approaches prevents a single point of failure

Non English Operating Systems

You must create the following groups prior to installation Administrators with the local administrator account as a member Guests with the IIS User account IUSR_(hostname) as a member (hostname is the name of the local server)

2.0 SecurMail Overview

SecurEnvoy SecurMail Key Points

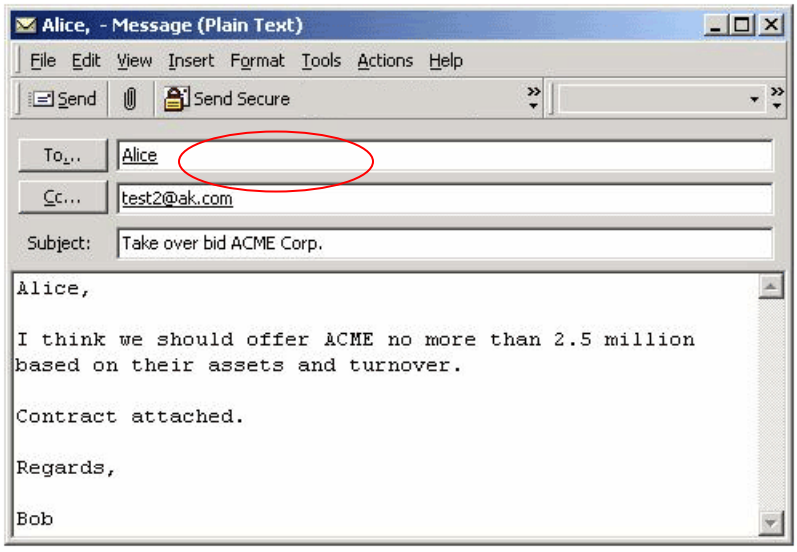
SecurMail uses a patented approach that doesn't suffer from the complexity of traditional digital certificate-based solutions, and doesn't get blocked by email virus checkers that can't decrypt messages. SecurMail is compatible with all recipient email clients so that secured messages and attachments can be sent to any email account, even webmail providers such as Hotmail, Yahoo and Gmail. There isn't a plug-ins required at the receiving end so the recipient does not need to update or download anything extra to be able to read the mail. All they need is internet access, an email account and a mobile phone.

SecurEnvoy SecurMail Solution Overview

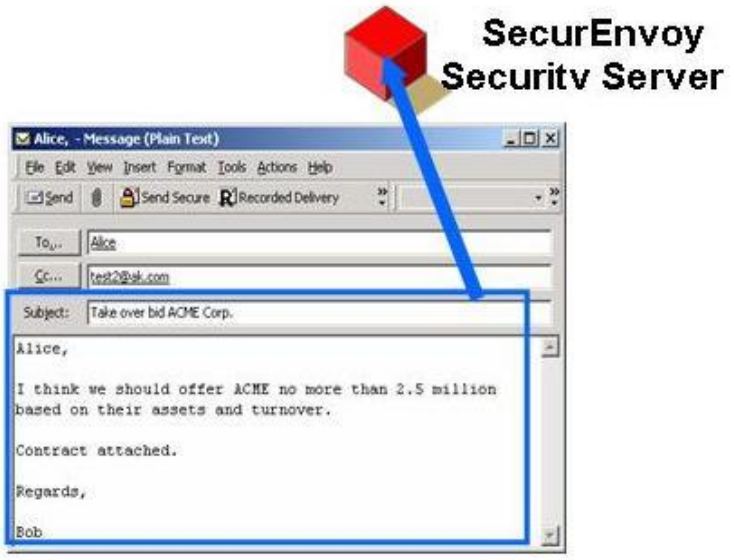
Emails sent from senders Microsoft Outlook program are sent via a web server's https connection to protect the data sent across the Internet. This SecurMail web server will be based within sender's network or hosted upon the Internet. The SecurMail web server then encrypts the email data when it is at rest. At this point a pick up email and SMS message are sent to the recipient.
Two factor authentication of the recipient is achieved, with the first factor being an eight digit code (MailboxID) sent via email and the second factor being a six digit passcode sent via SMS to the recipient's mobile phone, then you have an absolute assurance that the email has only been read by the intended recipient.

The following steps show an employee sending a secure mail.

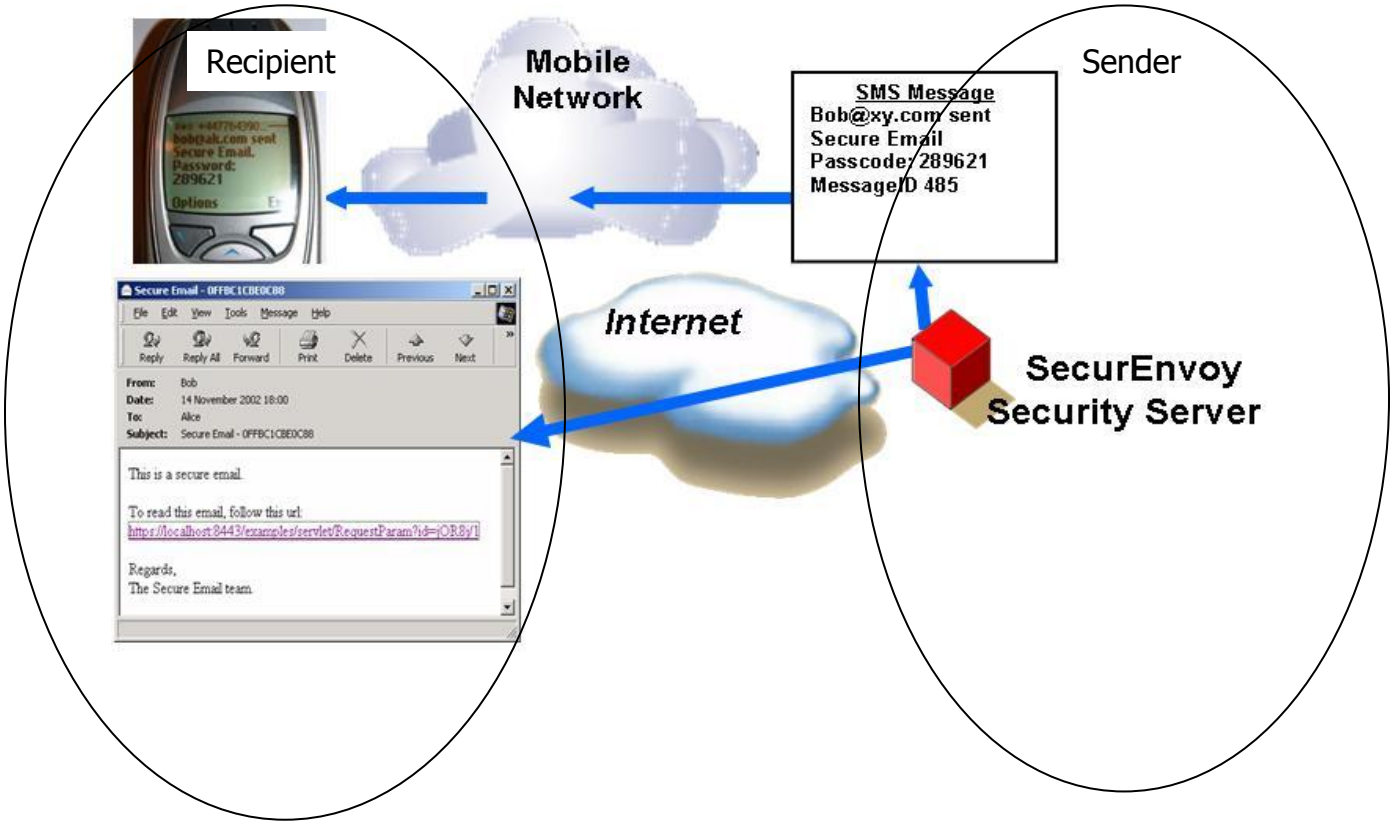
The employee creates an email with any required attachments in the normal way.
When this employee wishes to send the email they simply press the "Send Secure" button.
This new button is created in Outlook when the SecurEnvoy Outlook Agent is installed.
The customers email address and mobile number is found within either the local Outlook Contacts or the Global Address List. If the mobile number of the customer is not known, the employee is prompted to enter a mobile telephone number or a pre-agreed password if no mobile number is available.



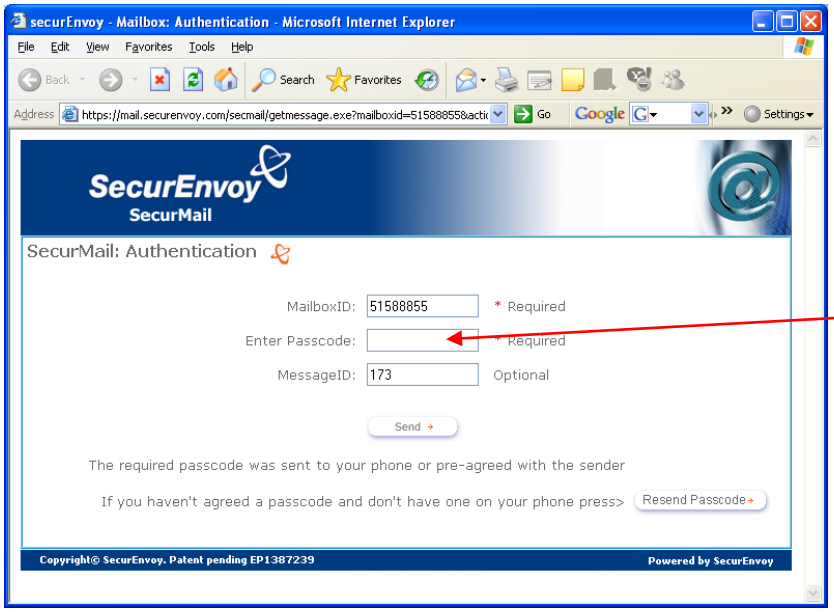
The security sensitive parts of the email, the Subject, Body and any attachments are uploaded to the SecurEnvoy Security Server based in senders environment or hosted datacenter and a clear text copy of the mail is saved in the sent items folder of Outlook which in turn is backed up to the exchange server and passed for archiving.



The SecurEnvoy security server then sends both an email and an SMS text to the customer. The email contains a URL of this message along with the first factor of authentication, the MailboxID. The SMS text message contains the second factor of authentication, the six digit passcode.

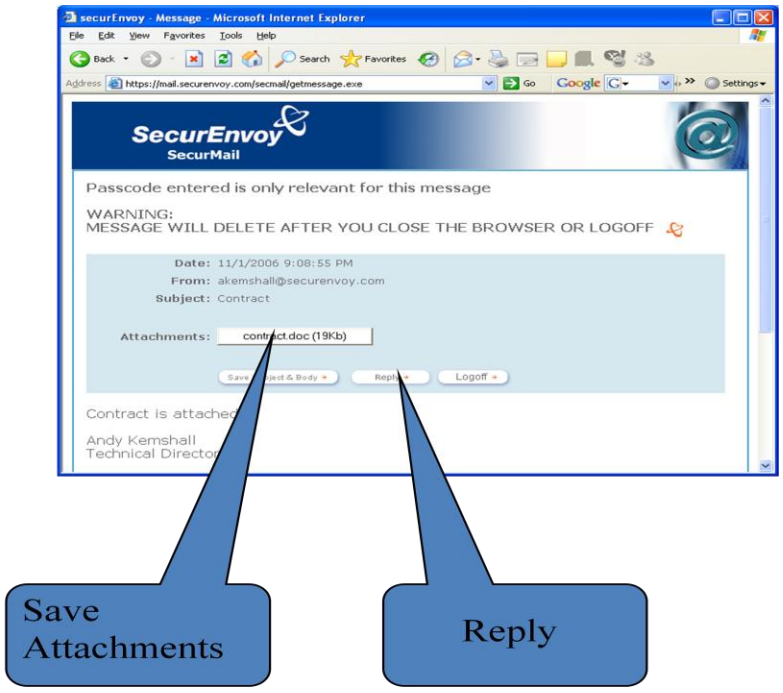


When the customer opens the URL in the email, a secure https session is started between the recipient and the SecurEnvoy security server based at Sender network. The first factor of authentication, the MailboxID (PIN) is then passed within the URL. The customer is prompted for the second factor of authentication, their passcode. The customer reads the onetime passcode from their mobile phone and enters it at the passcode prompt.





If the MailboxID and Passcode are correct, the recipients' message and any attachments are available for viewing and saving locally. While the customer browser is still open and not timed out (configuration setting defaulting to 1 hour) they can select to reply back to the sender. After the customer logs off or kills their browser, this message cannot be accessed again as it is one time message.



If the recipient replies to the sender, the reply and any attachments are sent backup the open SSL connection to the SecurEnvoy security server which in turn converts it to SMTP (email) and forwards to the sender as a regular email message.

SecurMail also has the ability for reply messages to be sent with the same strength as they were sent. i.e. Two Factor authentication.

Note that as the SecurMail web server and existing mail gateway are located within the same private network, there is no outside threat of these reply emails being intercepted.

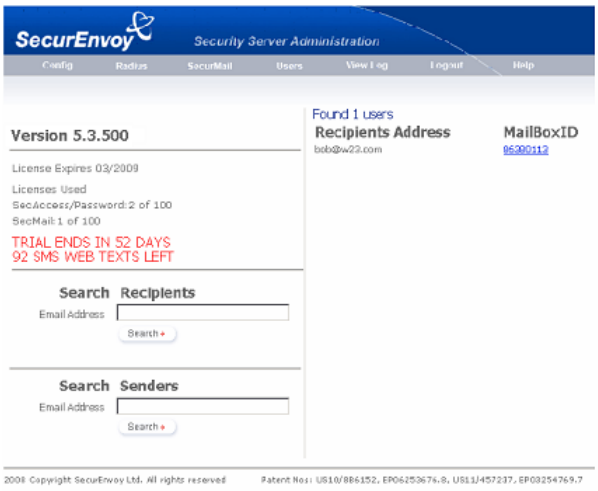
Finally, if the sender selected the recorded delivery option, after the customer has authenticated an email is send out to the employee to notify them.

Once the security server is setup, there is no administration tasks required as the sender is notified of any delivery issues (incorrect mobile number or email address).

Any secret messages that have not been picked up within 30 days (configurable) with be deleted and a warning email message is sent to the sender.

If the recipient completed too many incorrect authentications (configurable 3-10) the message is deleted a warning email message is sent to the sender.

3.0 SecurMail Administration

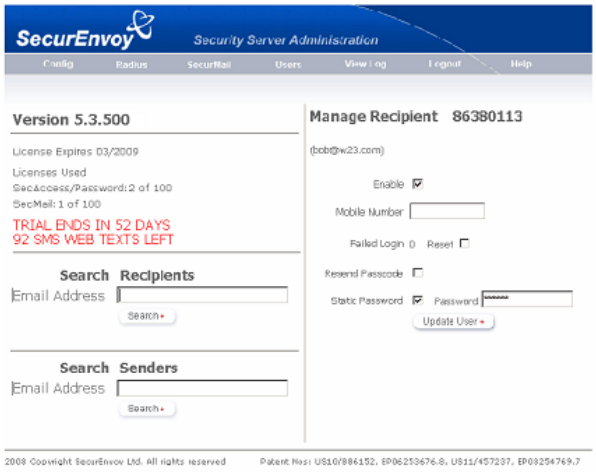


Launch the SecurEnvoy Admin GUI and select the SecMail tab, the following screen is displayed. You can then search for "Senders" or "Recipients"

Searching for "Senders" will display all users who are configured and have sent a SecurMail. Users that are displayed after searching can be deleted and removed from the system.

Searching for "Recipients" will display users who have been sent a SecurMail in "Auto Enrol and Store" mode.

Any search criteria can be used to search upon.



Recipient users that are searched upon will display their associated mailbox. You can then select the mailbox to provide additional management options. See diagram.

The Mailbox can be enabled and disabled

The mobile number can be updated

The Failed login can be reset, as after 10 consecutive bad authentications the mailbox is locked.

The passcode can be resent via SMS

A static password can be applied to the mailbox

3.1 SecurMail Virus Checking Integration

Email send via the "Send Secure" button in Outlook are uploaded to the Security Server and stored in an encrypted state. Virus software deployed on the security server would not be able to check these messages as there are encrypted so any virus checking must be integrated into the security server.

If virus checking is enabled, the message subject, body and any attachments are submitted to a third party virus scanning engine after they are uploaded and before they are encrypted.

If a virus is found a warning message is displayed at the Outlook agent and sending this email is aborted.

SecurMail can integrate with any third party virus software that supports a command line interface and will delete infected files.

The following products have been tested:

Symantec Scan Engine V4.30
Trend Micro Office Scan Corporate Edition 6.5

Integration procedure

Step 1 Install the third party Virus checker on the Security Server

Step 2 Start a command window (cmd)

Step 3 Test the third party's recommend commend line program with a test document and note the response for a clean file.

Step 4 Test the third party program with a test infected file. Note non-harmful test viruses can be downloaded from www.rexswain.com/eicar.html
Check that file is deleted

Step 5 Update setting in server.ini file as detailed below:

Step 6 If disk virus checking is preformed; change the virus checker's configuration to ignore the DATA directory located by default in c:\program files\SecurEnvoy

Step 7 Recipient reply emails. Reply emails are forwarded as is with no checking.
Make sure the MailHost configured in is set such that emails still pass through any email virus checking gateway that you have installed.

The virus settings of SecurMail are location in the server.ini file in:

Install dir\Program Files\SecurEnvoy\Security Server\

SecurMail settings are located in the Secmail Settings

Virus_Checking	Can be set to True or False If set to True will run the program Virus_Command with arguments Virus_Command_Args after the Outlook agent has uploaded the message body or attachments. Default: False
Virus_Command	The full path to the third party virus checking program
Virus_Command_Args	The arguments required to pass to the checking program defended in Virus_Command. Note that $FILENAME$ must be used in place of the test document you checked
Virus_Return	The return message displayed if execution worked and no viruses are found

Example 1

Integration with Symantec's Scan Engine V4.30

Virus_Command=C:\Program Files\Symantec\Scan Engine\savsecls\savsecls.exe

Virus_Command_Args=-verbose $FILENAME$

Virus_Return= 0

Example 2

Integration with Trend Micro's Office Scan Corporate Edition 6.5 with the virus definition file lpt$vpn.335

Virus_Command=C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Engine\vscanwin32.com

Virus_Command_Args=
/D /NM /NB /C /P="C:\Program Files\Trend Micro\OfficeScan\PCCSRV\lpt$vpn.335" $FILENAME$

Virus_Return=1 files have been checked

3.2 SecurMail Server Security Considerations

Virtual Directory Security

IIS Virtual Directory Secmail

The server should be hardened according to Microsoft's recommendations Once installed only one virtual directory requires being published externally, this is Secmail. This can be controlled via IIS properties, a firewall or reverse proxy server.

It is recommended that any other SecurEnvoy virtual directory is not exposed to the Internet, unless especially required.

Microsoft IIS Server

It is recommended that a dedicated instance of SecurEnvoy SecMail security server be installed for being public facing on the Internet ideally within the DMZ environment. A reverse proxy such as Microsoft ISA 2006 or various vendor SSL VPN are capable of providing this functionality.

For SecurMail access, it is strongly recommended that a trusted public web server certificate is installed in the IIS server.

The only Virtual directory that should be accessible from the internet is the "secmail" as this is the only one needed by the recipients. All other virtual directories should be set to be accessible from the internal network.

Recipients must access the secmail directory over https. Therefore the server (or the reverse proxy in that case) must use a public trusted certificate.

It is considered more secure to use the reverse proxy method, because there is only a single point of access and you share the certificate with other content using the reverse proxy.

Microsoft Windows 2003 Security resource
http://technet.microsoft.com/en-us/library/cc163140.aspx

Microsoft Windows 2008 Security resource
http://technet.microsoft.com/en-us/library/cc514539.aspx