

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 and 3.5 is installed (This is already installed upon Windows 2008 server editions)

Hardware Requirements

CPU – Pentium class processor 1 GHz or faster
HD - 150Mb of available hard disk space
RAM – 120Mb of available ram

Optional for integrated user management

Connection to a Directory server (MS Active Directory, Novell e-Dir, Sun Directory Server and Open LDAP) is required. A service account with read all and write access to the TelexNumber attributes.

Note

For Active Directory configurations see section 5.2 of this guide for step by step instructions of using Microsoft's ADSI Edit tool if you do not wish to use a domain admin account.

Network Connectivity

- Security server needs read/write access to your Directory Server via LDAP (port 389) or LDAPS (port 636)

Note

LDAPS is required for SecurPassword and Integrated Desktop Management.

- If the Web SMS Gateway is being used to send SMS messages, the Security Server needs https access to the Internet (port 443)
- The IIS Agent needs https connectivity between the IIS server you are protecting and the security server(s) (port 80)
- The VPN or other Radius based client requires to have access to the security server's radius service (port 1645 or 1812)

It is recommended that two security servers should be installed for each IIS agent or each RADIUS client that is being authenticated.

Each security server should be configured to connect to a primary and secondary Directory server's (LDAP). This approach prevents any 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)

SecurEnvoy Ltd

1210 Parkview, Arlington Business Park, Theale, Reading. RG7 4TY
Tel: 0845 2600010 Fax: 0845 260014 www.SecurEnvoy.com

1.1 SecurMail 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 and 3.5 is installed (This is already installed upon Windows 2008 server editions)

Hardware Requirements

CPU – Pentium class processor 1 GHz or faster

HD – 500GB of available hard disk space (dependant on number of Store mode emails that are to be kept)

RAM – 120Mb of available ram

Optional for integrated user management

Connection to a Directory server (MS Active Directory, Novell e-Dir, Sun Directory Server and Open LDAP) is required. 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)