SecurEnvoy Security Server Installation Guide

SecurEnvoy Global HQ
The Square | Basing View | Basingstoke | Hampshire | RG21 4EB
Tel: 0845 2600010 Fax: 0845 260014 www.SecurEnvoy.com

Version 8.1

SecurEnvoy Security Server

Installation Guide v8.1

© 2017 SecurEnvoy

The SecurEnvoy Security Server is the main central component of the SecurEnvoy suite of products. It has direct integration into a LDAP directory server (Microsoft Active Directory, Novell e-Dir, Sun One Directory Server and Linux Open LDAP Directory Server) for access to user information. SecurEnvoy Security Server controls and manages the authentication and sending of SMS passcodes and Emails. This must be installed for SecurAccess, SecurICE, SecurPassword and SecurMail.

© 2017 SecurEnvoy All Rights Reserved

Foreword

SecurEnvoy is the trusted global leader of tokenless two-factor authentication. As the pioneers of mobile phone based tokenless authentication; SecurEnvoy leads the way with ground-breaking solutions that others aspire to.
Our innovative approach to the tokenless market demonstrates that thousands of users are benefitting from our solutions all over the world.

With users deployed across five continents, our customers benefit from a significantly reduced time to deploy and a zero footprint approach means there is no remote software deployment and administrators enjoy our comprehensive management tools allowing them to rapidly deploy up to 100,000 users per hour.

Our design philosophy is based on re-using existing customer technology investments such as Microsoft Active Directory, simplifying the end user authentication experience while enhancing the overall security.

With no hardware token manufacturing, distribution and maintenance costs as users can make use of existing mobile phone or Email technology, the return on investment (ROI) is so much more acceptable to businesses and organizations. A zero carbon footprint is also very beneficial for environmentally responsible purchasers. We are truly providing solutions that have zero impact on our environment.

SecurEnvoy distributes through the channel, providing customers the value added benefits of working with local partners. We have established a technical and sales infrastructure that supports most languages and cultures around the world.

The business was officially incorporated in 2003 after preliminary, coding and testing in our labs. Over a decade has passed since our initial incorporation and we are very proud of our happy customer base across the five continents and with regional support for them.

Business levels have more than doubled year on year due to our subscription sales model that is an acceptable route that allows our clients to budget more effectively. This model includes local support and annual subscriptions.

Founded by Andrew Kemshall and Stephen Watts, the two founders work relentlessly to achieve business growth worldwide. This massive growth has been possible through the quality of people and the experience within the company both from sales and technical expansion.

SecurEnvoy continues to shape the way millions of people plan their authentication requirements and purchasing decisions.

© 2017 SecurEnvoy All Rights Reserved

Contents

Document History **5**

Securenvoy server topology **6**
Internal Server (no external facing web portal) 6
Internal Server with web resources published via a Reverse Proxy (SSL VPN etc.) 7

Pre requisites **8**

1.0 Installation **9**
New Installation of SecurEnvoy Security Server 9

2.0 Advanced Configuration Wizard **12**
LDAP Tab 12
eMail Tab 13
IIS URLS Tab 14
SMS/Voice Gateway Tab (Multi-Gateway Support) 14
Web SMS Gateway 15
RADIUS Tab 19

3.0 Security Server Admin GUI **20**

4.0 Upgrading **21**

5.0 Migrate SecurEnvoy to additional server **23**

6.0 Additional Information **25**
SecurEnvoy services 25
Active Directory Security 26

7.0 LDAP (other) Security **32**

8.0 Notes **33**

© 2017 SecurEnvoy All Rights Reserved

DOCUMENT HISTORY

SecurEnvoy Installation Guide v8.1

Publisher
SecurEnvoy Publishing

Managing Editor
SecurEnvoy Training Department

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

Cover Designer
SecurEnvoy Marketing

Revision	
V1.0 AK PU	10/05/2008
V1.1 AK PU	21/12/2008
V1.2 PU	07/07/2009
V1.3 PU	03/11/2009
V1.4 PU	18/01/2010
V1.5 AS	10/01/2011
V1.6 PU	11/05/2011
V1.7 PU	29/06/2011
V1.8 PU	20/04/2012
V1.9 SM	08/05/2013
V2.0 TD	15/01/2014
V8.1 RDS	29/01/2017
V8.11 RDS	13/03/2017

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Document Version 8.1 Printed: Mar 2017 in United Kingdom.

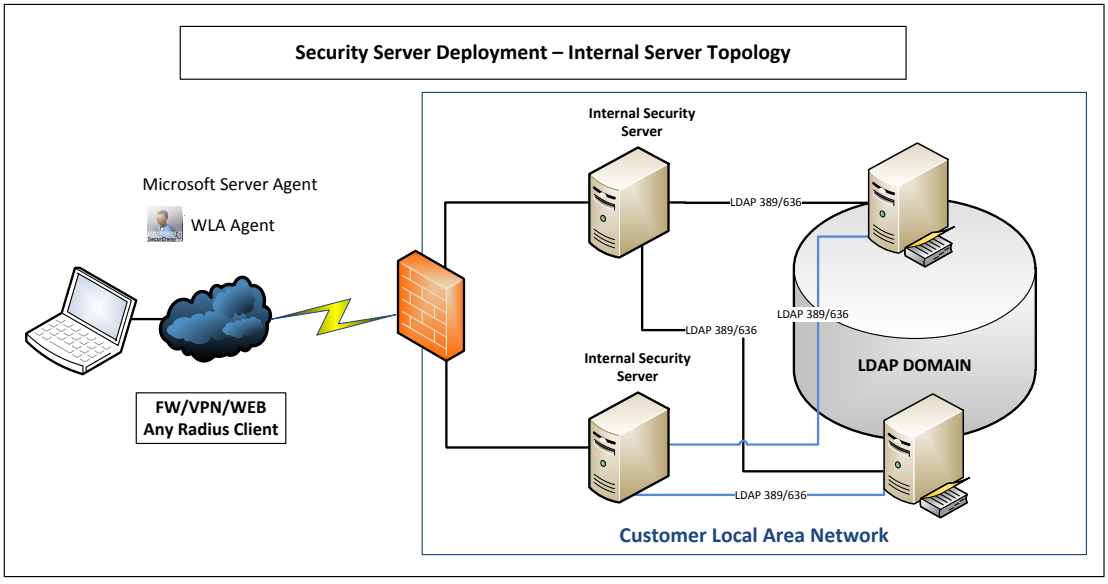
© 2017 SecurEnvoy All Rights Reserved

SECURENVOY SERVER TOPOLOGY

Version 8.1 of SecurEnvoy Security Server introduces some exciting new features into the two-factor authentication (2FA) arena, including push notification technology and Near Field Communication (NFC). Push notifications work by sending a message to the notification centre or status bar of a users' smartphone. NFC allows a customer to authenticate contactlessly using their smartphone. These new features are dependent on the architectural topology of the SecurEnvoy Server implementation. This section of the guide has been created to provide some guidelines for selecting the correct topology to deliver all required features of each organization's SecurEnvoy Security Server solution.

> **Note**
>
> *It is important that this decision is made in advance of installing the product.*

Internal Server (no external facing web portal)



Advantages of this topology

No external Internet facing portals. Therefore no hardening of servers is required and the risk of attack to these portals is limited to internal users only.
Note: SecurEnvoy's Manage My Token portal requires two-factor authentication.

© 2017 SecurEnvoy All Rights Reserved

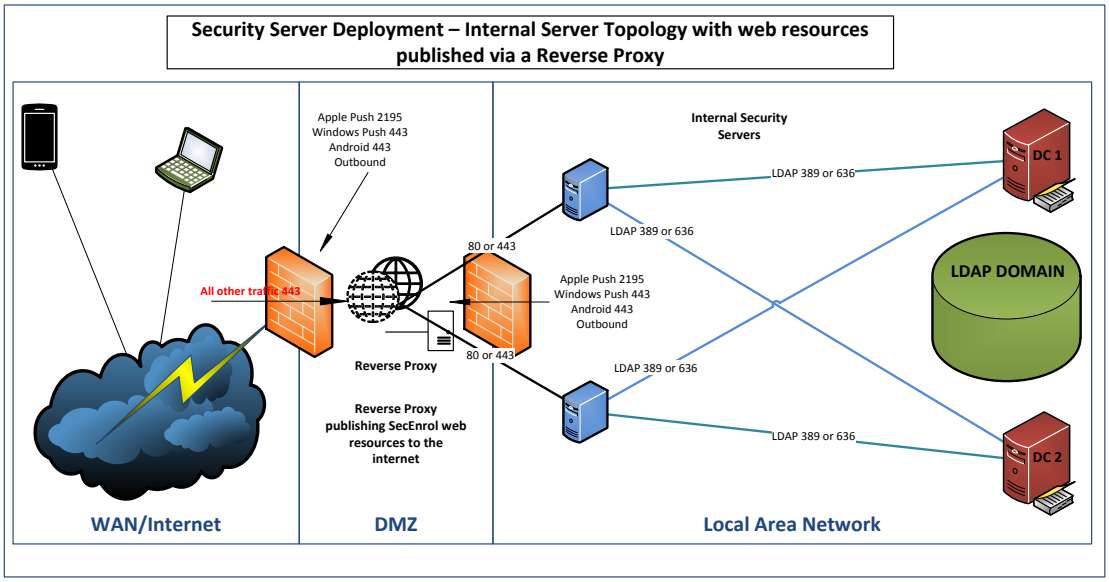
Disadvantages of this topology

The following token types are not supported:

- Oneswipe online push
- Oneswipe offline NFC

In addition, a user will need to be on the internal local area network (LAN), or connected over VPN, to manage changes to their token types on the Manage My Token portal.

Internal Server with web resources published via a Reverse Proxy (SSL VPN etc.)



The Manage My Token portal located in IIS default website (SecEnrol) must be published to the Internet via a reverse proxy or load balancer appliance.

Advantages of this topology

All token types are supported including oneswipe push and NFC.
Users are able to manage their tokens externally from any Internet location.

Disadvantages of this topology

Manage My Token portal must be published to the Internet.
The risk of attack to this and other portals is exposed to external users.

© 2017 SecurEnvoy All Rights Reserved

PRE REQUISITES

Software Requirements

- Windows 2008 (R2) / Windows 2012 (R2)
- IIS installed with default settings (Site ID1 "Default Web Site")
- Microsoft .NET 2 and .Net 3.5 installed.
- Active Internet Connection

Hardware Requirements

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

Network Connectivity

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

For integrated user management (Optional)

For integration user management, a connection to an existing LDAP Directory server (MS Active Directory, Novell e-Dir, Sun Directory Server and Open LDAP) is required, with a service account with read all and write access to the TelexNumber attributes.

Technical Note

A service account must exist within each configured Domain for all SecurEnvoy server(s)
For Active Directory configurations see section 7 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.
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).
- If Apple push is being used then it will need access to port 2195 (outbound) to allow communication to the Apple gateway (gateway.push.apple.com). The APNs servers use load balancing, so devices won't always connect to the same public IP address for notifications. It's best to allow access to these ports on the entire 17.0.0.0/8 address block, which is assigned to Apple. Windows and Android push gateways use port 443 (HTTPS). All 3 gateways come inbound on HTTPS (443)
- The IIS Agent (pre 5.4) needs http connectivity between the IIS server you are protecting and the Security Server(s) (port 80).
- The VPN, IIS Agent (5.4 and later), or other Radius based clients require access to the Security Server's radius service (default UDP port 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 (LDAP). This approach prevents any single point of failure.

Technical Note

For Operating Systems not using English language
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).

© 2017 SecurEnvoy All Rights Reserved

1.0 INSTALLATION

New Installation of SecurEnvoy Security Server

The following steps will describe how to install the SecurEnvoy Security Server and will guide the user through a new installation using the Advanced Configuration Wizard. Please make sure that you have the correct License key from your purchase of the SecurEnvoy Security Server or from your Trial/Demo License, which is received via Email after downloading a 30-day trial from www.securenvoy.com/trial.aspx. If you have not received a license key from your reseller, please contact them to obtain it.

1. Locate the SecurEnvoy Security Server software and execute the setup file.

Technical Note
Microsoft .NET 3.5 must be-installed

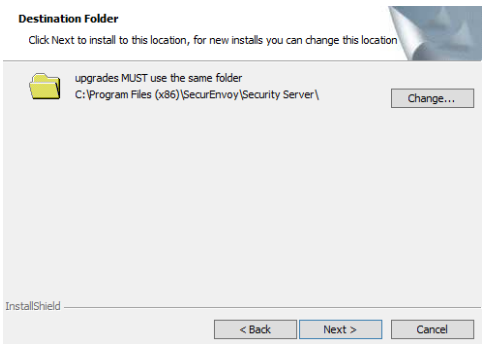
2. When the setup is executing, it will check to see if Microsoft .Net Framework 3.5 is installed.
   If it is not installed it will download and install the Microsoft Dot Net Framework.

3. Click "I agree" to Microsoft's license terms, and then click the install button to carry out the .Net installation.

4. When the .Net installation is compete, click OK to continue.

5. Click to accept the license terms for SecurEnvoy, then click Next to continue.

6. Accept the default destination path for installation or enter a new path where SecurEnvoy Security server should be installed. Click Next.

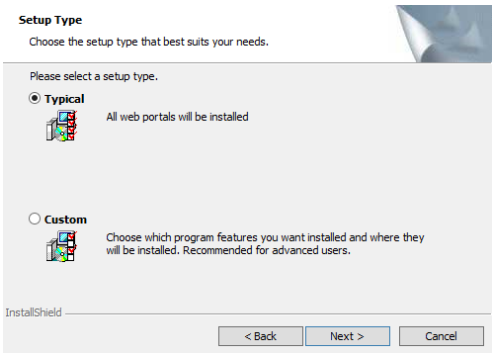


© 2017 SecurEnvoy All Rights Reserved

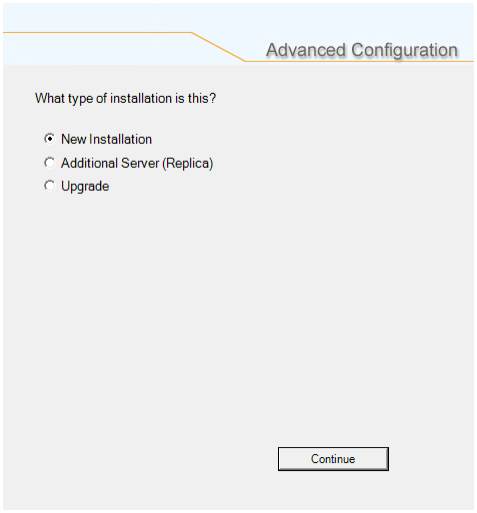
7.

A Setup Type screen will be shown. Select Typical and click on Next to continue.

A summary screen will be displayed, click on Install to continue.



8.



The user should now select the type of installation required. Select New Installation and click Continue. The 2 remaining installation types Additional Server and Upgrade are covered later in this guide see Section 4 Select New Installation and click Continue.

⚠ Important Note – Customer Encryption Key ⚠

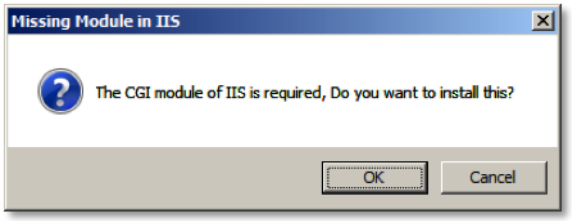
A customer encryption key is created that is unique to this installation and domain. The customer encryption key is created using AES 256 bit encryption technology and will encrypt any user data such as private telephone numbers and the types of token selected, that are stored within the SecurEnvoy Security Server. It is essential that the key created and saved in the file config.db is not deleted or overwritten with a second new installation, otherwise it will not be possible to decrypt the user data stored within the SecurEnvoy Security Server.

For disaster recovery and all future upgrades or server replication a backup of Config.db and server.ini MUST be made.

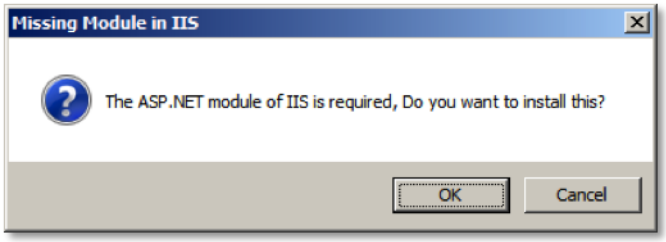
32 bit installations dir :\program Files\SecurEnvoy\Security Server
64 bit installations dir :\program Files (x86)\SecurEnvoy\Security Server

© 2017 SecurEnvoy All Rights Reserved

9. Installation of Missing CGI Module in IIS. The following warning is displayed, if the server does not have the CGI Module of IIS installed. Select OK for the SecurEnvoy Installation process to install the missing IIS Module.



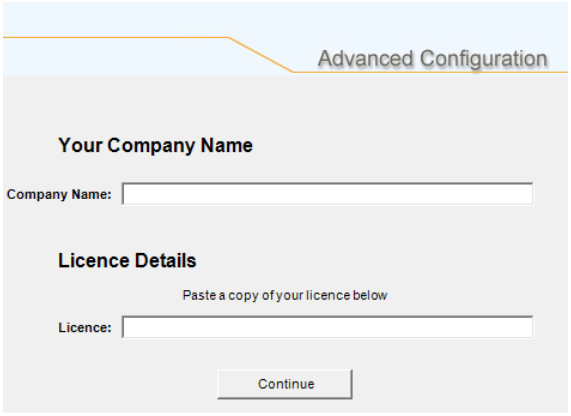
10. Installation of Missing ASP.NET Module in IIS. The following warning is displayed, if the server does not have the ASP.NET Module of IIS installed. Select OK for the SecurEnvoy Installation process to install the missing IIS Module.



11. Complete the installation with Organizational details and enter the license key.

Technical Note

Your Company Name will be used in all SecurAccess/ SecurPassword passcode messages sent to mobile phones. Click Continue.

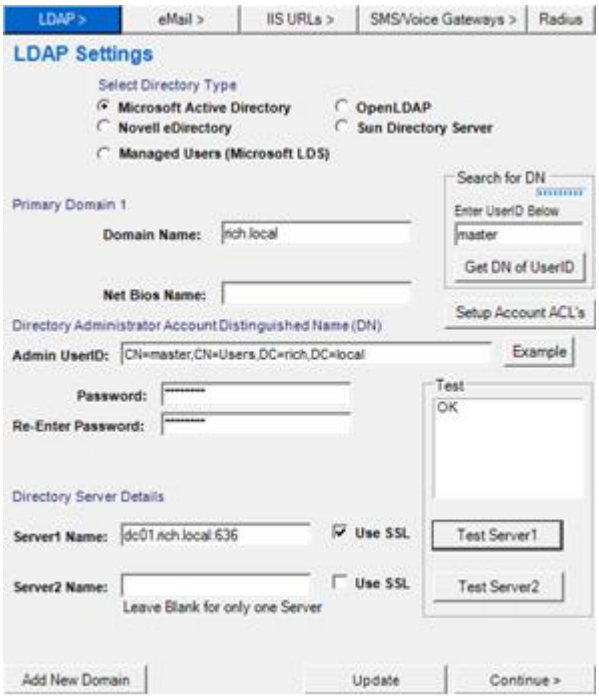


© 2017 SecurEnvoy All Rights Reserved

2.0 ADVANCED CONFIGURATION WIZARD

Any new installation of the SecurEnvoy Security Server will require the user to step through each tab within the wizard. This is essential, so that the installation can be finalized and the required batch services can be installed and started, which can only happen once the user has clicked Continue on each tab. It is not possible to exit the Wizard until the user has clicked continue on each tab, a warning will be shown on screen if the user attempts to exit the window.

LDAP Tab



Select Directory Type - First step is to select the Directory Type, either "MS Active Directory, Novell e-Directory, SecurEnvoy Managed Users – MS ADAM, OpenLDAP – Linux, Sun Directory server".

Primary Domain 1 - The *Domain Name* is the domain where the active directory resides and user information is stored and retrieved.

Directory Administrator Account Distinguished Name - Use the Tab key to step into the *Search for DN* section and into the field *Enter UserID*. Type the name of the account that will run the SecurEnvoy server. Click *Get DN of UserID* this will automatically populate the DN account details providing you are currently logged on as a domain administrator of this domain. If correct enter the password for the User ID account.

Using the button *Example* will provide a real example of the administrator DN directly from Active Directory.

Directory Server Details - Finally enter the names of your Directory servers. If certificates have been deployed upon your directory servers, LDAPS (port 636) can be utilised by enabling the "Use SSL" check box, note that LDAPS generally requires the server name to be fully qualified.

Test – after completing the required details, the connection can be tested by clicking Test Server 1 or Test Server 2. If OK is returned then click Continue. If OK is not returned, errors should be rectified before proceeding.

> **Note**
>
> *If Use SSL is selected, the server name MUST be the same name as set in the common name of the Directory's server certificate.*

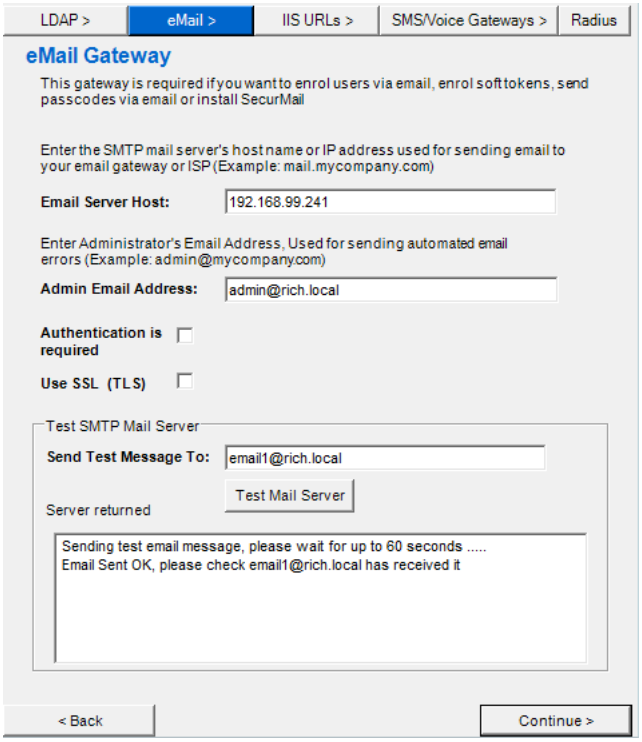
© 2017 SecurEnvoy All Rights Reserved

If you wish to add an additional domain, click the "Add New Domain" button and enter the LDAP Settings for each new domain. The web server is the machine that the security server software was installed upon, this does not require changing.

The domain name is the additional domain where user information will be stored and retrieved. The Net Bios Name is optional and only needs setting if UserID logons use Net Bios Domain names for example "SECURENVOY\john smith".

Once the above information has been entered and a successful test established, click Continue. A warning will be displayed in the Wizard that confirms that the batch services are being installed.

eMail Tab



If using SecurMail, sending passcodes via eMail, or require enrolment emails to be sent. Enter details of the SMTP server that should be used for the sending of emails and the associated email account you wish to use.

There are two further options, for SMTP servers that require authentication, enable the checkbox and enter account details.
To support SMTP server that utilise TLS, enable the checkbox.

A test email can then be competed in the "Send Test Message To" box.

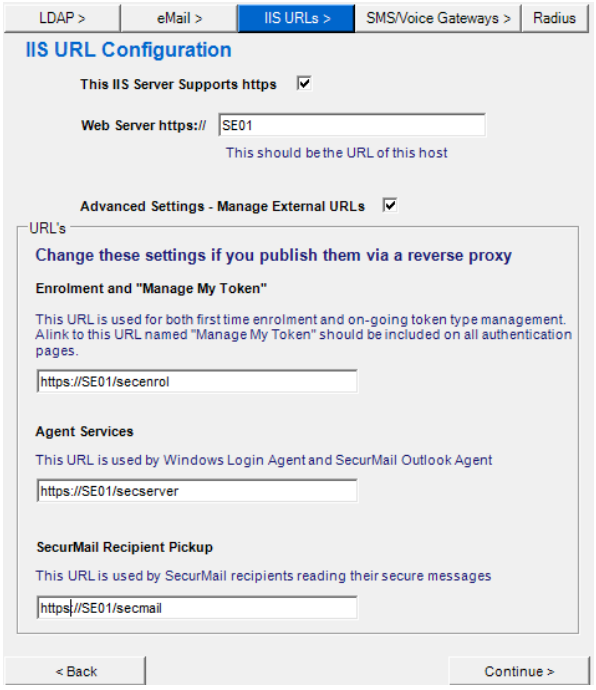
Note

Please ensure that your SMTP server has been setup to allow relaying from the SecurEnvoy server.

Click Save and Continue

© 2017 SecurEnvoy All Rights Reserved

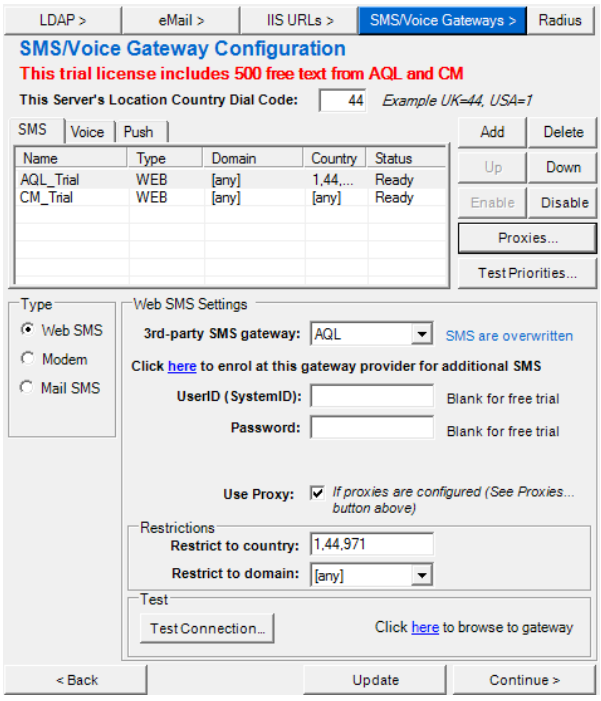
IIS URLS Tab



The URL configuration can be viewed and maintained from this tab. If the server supports HTTPS, then this can be selected, this setting will be inherited in the URL values that are displayed when selecting Manage My URLs. These URL values are included in system generated Emails sent to users. For example user enrolment Email.

Click Save and Continue

SMS/Voice Gateway Tab (Multi-Gateway Support)



Multiple gateways can now be setup and maintained via this Tab. It is possible to setup as many gateways as required to meet the needs of the organisation. SecurEnvoy can support various gateway types from WebSMS or Voice through to Serial or TCP IP Modems.

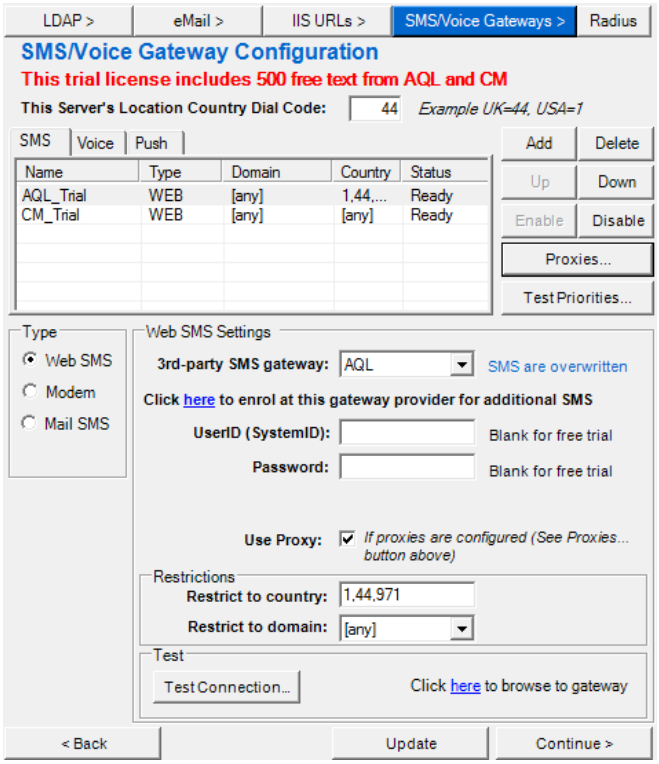
The gateways can also be setup in priority order and can also be disabled as required very easily from with this wizard. The priority ordering of the gateways in controlled using the "Up" and "Down" buttons.

The gateways can be restricted per country, to allow the user more control as to which service is used in certain countries. This is used to overcome difficulties sending SMS into countries that might not support advanced SMS features such as flash message and sms overwrite.

Once the priority ordering is completed, it is possible to test the priorities.

© 2017 SecurEnvoy All Rights Reserved

Web SMS Gateway



Select Add to install a Windows service that communicates with a Web based SMS gateway. The default web service is from AQL - see www.AQL.com

Trial licenses have a built in AQL account, therefore no username or password is required.

Otherwise an account is required with the selected Web SMS provider. Enter UserID and Password account information (provided by your Web SMS provider) and enter proxy information if required.

Once completed, click the Test gateway button output should show that the "SMS Gateway responded OK".

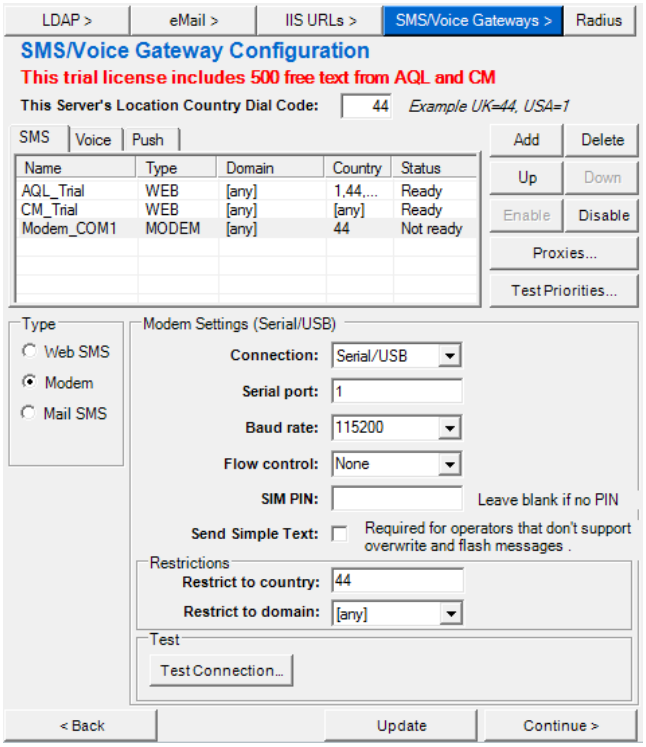
Restrict to Country / Domain
Enter dialing codes for countries that should be served by this modem. If the modem is also to be restricted to serve a certain domain, this can be selected from the radio button dropdown.

If errors are shown, click the link to manually check a web connection can be initiated. If the web browser connection is OK, a "Fail Auth" should be returned. *(This is because no account information was sent, but it proves the SMS Gateway server can be reached and a response received.)*

SsecurEnvoy can connect to many Web based SMS providers. A new template may be required – Security Server Administration Guide *for more details*.

© 2017 SecurEnvoy All Rights Reserved

- **Modem**



Select "Add" to install a Windows service that communicates with an SMS modem. The SMS modem is a serial GSM device attached directly to the security server's serial interface. This option allows a corporation to use its own SIM chip from their Telco and take advantage of any free or group SMS call rates.

To setup the Phone Gateway, make sure the device is connected and powered on.

The following are configurable options:

Send Simple text
When enabled, allows a SMS to be sent in simple mode. Use this if the Telco operator does not support message overwrite (PDU mode).

Select Connection Type
Either Serial/USB or TCP/IP

Enter serial port
Comm port the GSM modem is connected.

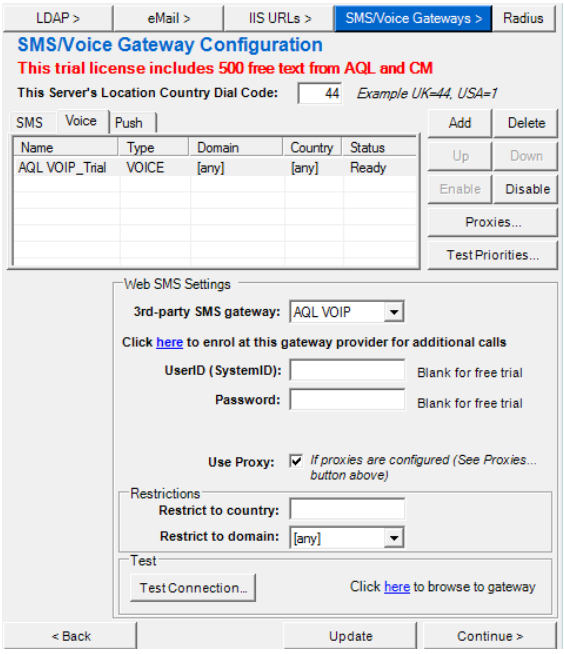
Baud rate
Select the appropriate baud rate.

Restrict to Country / Domain
Enter dialling codes for countries that should be served by this modem. If the modem is also to be restricted to serve a certain domain, this can be selected from the radio button dropdown.

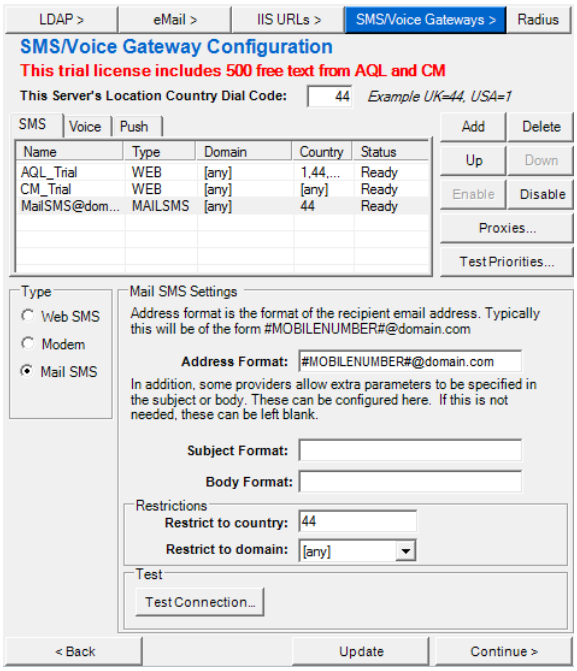
When complete, click the OK button to test. The test will carry out an ATI and signal strength test. Version information will be shown as well as signal strength information. Signal strength is measured from 0-31. An acceptable figure is 16 or above.

© 2017 SecurEnvoy All Rights Reserved

- **Voice**



- **Mail SMS**



A Voice gateway is setup in much the same way as for Web SMS. Select "Add" to install a Windows service that communicates with a Web based Voice gateway. The default web service is from AQL - see www.AQL.com

Trial licenses have a built in AQL account, therefore no username or password is required.

Otherwise an account is required with the selected Web Voice provider. Enter UserID and Password account information (provided by your Web Voice provider) and enter proxy information, if required.

Once completed, click the Test gateway button, output should show that the "Gateway responded OK".

Restrict to Country / Domain
Enter dialing codes for countries that should be served by this modem. If the modem is also requires restricting to serve a certain domain, this can be selected from the radio button dropdown.

To provide a facility to send a sms via an SMTP server, a gateway can be setup and included in the prioritised list of gateways.

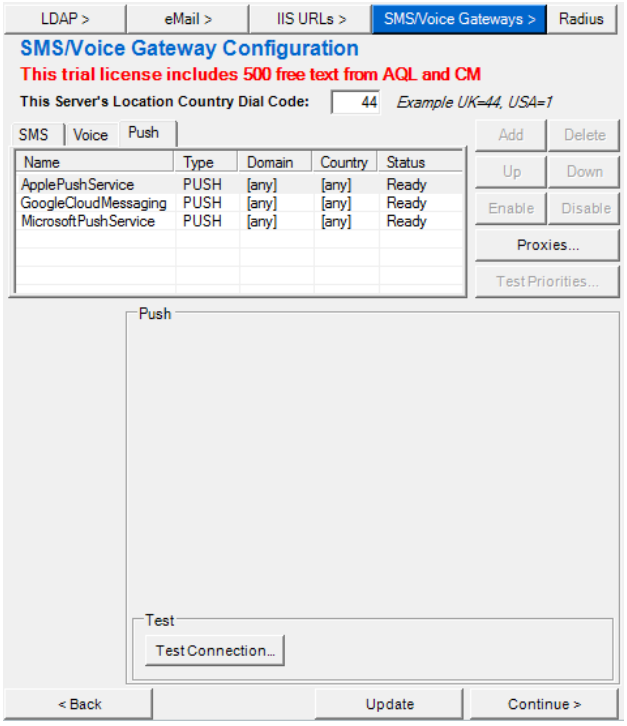
Select "Add" and complete the Address format which should be
#MOBILENUMBER#@atyourprovider.com

If the Telco provider allows user modifications to Subject and Body formats, please set these.

Restrict to Country / Domain
Enter dialing codes for countries that should be served by this modem. If the modem is also to be restricted to serve a certain domain, this can be selected from the radio button dropdown.

© 2017 SecurEnvoy All Rights Reserved

- **Push**



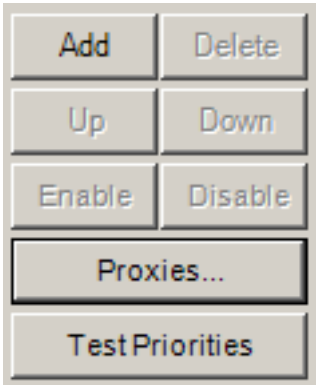
The below three push notification gateway services connections can be tested from the "Push" Tab by selecting "Test Connection"

- ApplePushService
- GoogleCloudMessaging
- MicrosoftPushService

The test connection will return a status and a Trace can be displayed if required.

- **Using a Proxy for Web Services**

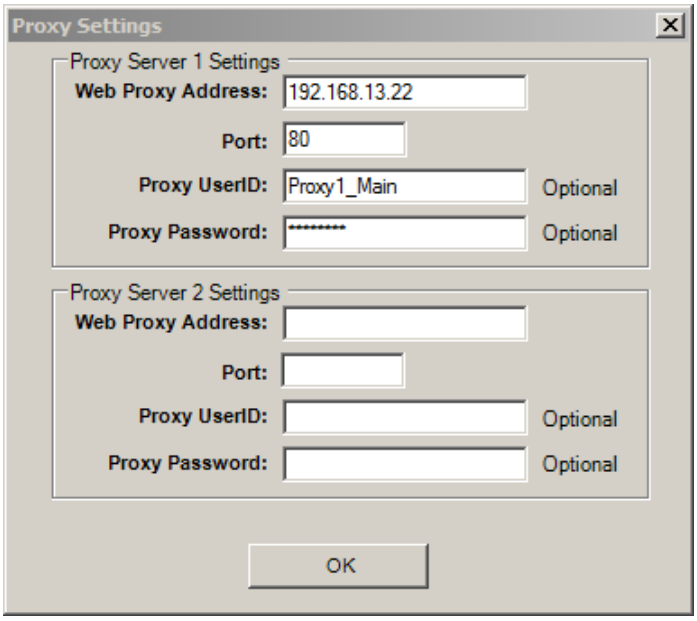
If the organisation requires the use of a Proxy Server, this must be setup using the Proxies button: -



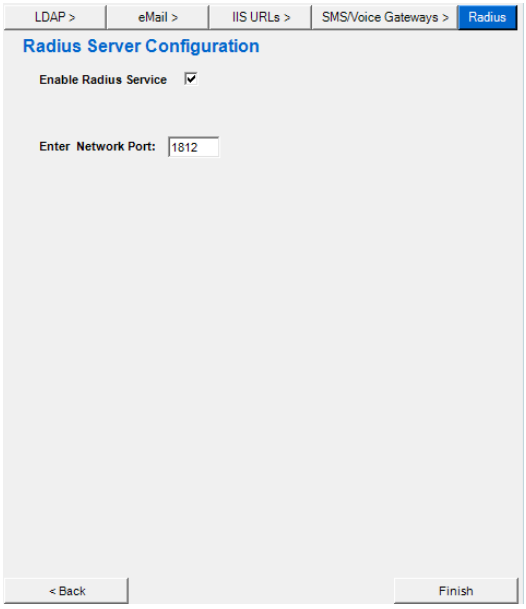
Select Proxies to open a new window, which will allow the user to save any proxy server properties.

© 2017 SecurEnvoy All Rights Reserved

Once the properties for the proxy server have been saved, the user can select to use the Proxy when setting up the individual gateways for web services such as Web SMS or Voice.



> **Note**
>
> *SecurEnvoy supports proxy servers - enable the checkboxes for each gateway required and populate proxy settings.*



RADIUS Tab

SecurEnvoy by default will use Radius Port 1812. If this port is already in use, the user can change this setting. Once update is selected, the radius batch service is started.

© 2017 SecurEnvoy All Rights Reserved

Important

For new installations it is important to be aware that the Advanced Configuration Wizard will not be allowed to close, until all tabs have been updated. This is to ensure the batch services all start as required, with the correct information.

3.0 SECURITY SERVER ADMIN GUI

Select Start → Programs → SecurEnvoy → Local Security Server Administration. This will execute the Web based Admin GUI.

The following screen will be displayed, for more information on managing and configuration please see the SecurEnvoy Administration and Configuration Guide.



© 2017 SecurEnvoy All Rights Reserved

4.0 UPGRADING

Prior to Upgrade
Before upgrading the SecurEnvoy Security Server software, please make a copy of the following: -

- config.db
- configpre54.db
- local.ini
- server.ini

These are all located on the file system in the following locations:

For 32 bit installations install dir\Program Files\SecurEnvoy\Security Server
For 64 bit installations install dir\Program Files(x86)\SecurEnvoy\Security Server

Also export the registry key HKLM\software\SecurEnvoy. Finally, make a backup copy of the DATA directory.

Important

Before commencing an upgrade, it is crucial that a backup is made of the following files; config.db, configpre54.db, local.ini and server.ini. These files will be required for purposes of roll back if the upgrade should fail.

Upgrade Process
Locate the SecurEnvoy Security Server software and execute the setup.exe file.

This will install on top of the existing installation, all server configuration and user's settings will be preserved.

Note

Any bespoke HTML templates that have been created, will require re-creating upon each SecurEnvoy Security Server after the upgrade.

When the setup is executing, it will check to see if Microsoft .Net Framework 3.5 is installed.

If it is not installed it will download and install the Microsoft Dot Net Framework, as with a new installation.

Note

Microsoft .NET 3.5 must be-installed

© 2017 SecurEnvoy All Rights Reserved

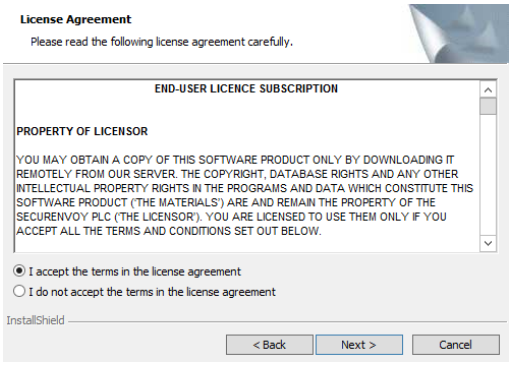
Click "I agree" to Microsoft's license terms, and then click the install button to carryout the .Net installation.

When the .Net installation is compete, click OK to continue.

The setup will then run through the upgrade procedure.

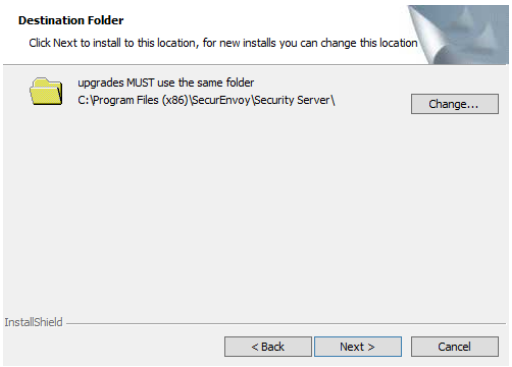
Click Next when prompted.

Click to accept the license terms for SecurEnvoy, then click Next to continue.



Accept the default path for installation upgrade or enter an existing path where SecurEnvoy Security server should be upgraded.

Click Next to continue



Once the installation is complete the Advanced Configuration Wizard will automatically launch and allow the setup of any new parameters.

See **Section 2** for more details.

© 2017 SecurEnvoy All Rights Reserved

5.0 MIGRATE SECURENVOY TO ADDITIONAL SERVER

Important

Before commencing a server migration, it is crucial that a backup is made of the following files; config.db, configpre54.db, local.ini and server.ini. Which can be located:-

For 32 bit installations install dir\Program Files\SecurEnvoy\Security Server
For 64 bit installations install dir\Program Files(x86)\SecurEnvoy\Security Server

The recommended method to migrate a SecurEnvoy installation from one server to another is to conduct a clean install of SecurEnvoy Security server upon the new target machine. When the advanced configuration wizard executes, select "Additional server (Replica)" and follow the screen prompts to use the config.db and server.ini from the existing server.

All global configuration data is stored upon the SecurEnvoy server within the server.ini file and all user data is stored encrypted with the LDAP server/domain. Therefore no user data is affected when adding an "additional SecurEnvoy server".

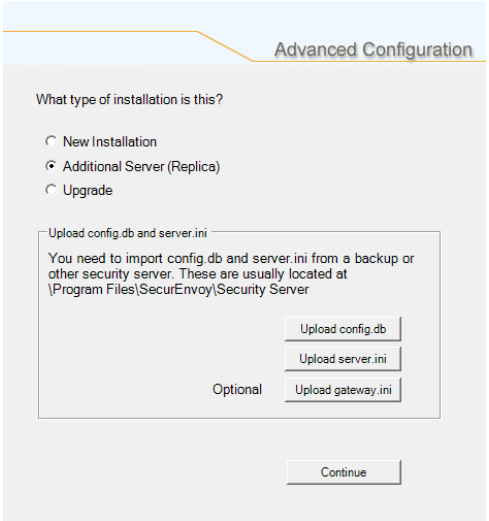
When the new SecurEnvoy server is full operational, the original can then be decommissioned.

Please note that Radius clients, IIS and Windows login agents will require updating so that they communicate with the correct SecurEnvoy server.

Multiple security servers must share the same security encryption key (config.db) so it is essential to backup this file beforehand.

Steps to Install additional security servers

1 Run the Security Server's setup.exe install program on the next required server,



1.1 Select "Additional server"

1.2 Press the "Upload config.db" button and browse to the config.db file on the first security server you installed, default location for this file is for

64 bit installations

C:\Program Files(x86)\SecurEnvoy\SecurityServer\

© 2017 SecurEnvoy All Rights Reserved

1.3 Carry out the same task for the "server.ini" file and optionally for the "gateway.ini" file.

Note

Each SecurEnvoy security server will use a local.ini file and a server.ini file, this has been created to assist deployments where multiple SecurEnvoy servers exist. Any changes made on a server will update server.ini or local.ini. At which point these files must then be copied to the other servers.

The local.ini file stores data regarding local configuration details
The server.ini file stores data that are global configuration details

2 Start the Security Server Admin GUI on the new server and select the menu "config".

Start → All Programs → SecurEnvoy → SecurEnvoy Local Administration

For a default installation the physical path is;

C:|Program Files (x86)|SecurEnvoy|Security Server|LOCALADMIN|localadmin.exe

Match any changes made so that all servers have the same configuration settings.

Additional servers MUST share the same SecurEnvoy administration account for each domain they manage.

The Batch server start times must be set to start at the same time allowing for any local time zone changes.

Multiple batch server processes must run within 10 minutes of each other or multiple day codes may be sent to end users.

Note

Additional servers MUST share the same SecurEnvoy administration account for each domain they manage.

© 2017 SecurEnvoy All Rights Reserved

6.0 ADDITIONAL INFORMATION

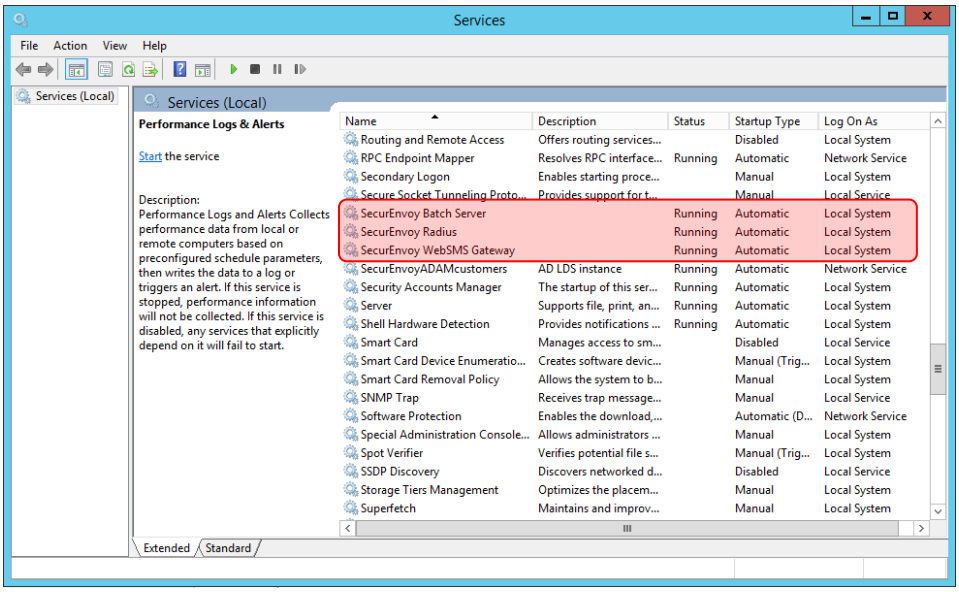
SecurEnvoy services

It is always beneficial after installation to check that all SecurEnvoy services are running. Click on the Windows "Start" button, then "Run" and then type "services.msc" and press "OK"

The following screen will be displayed. All SecurEnvoy services start with "SecurEnvoy" so can that they can be indexed and searched upon. Check installed SecurEnvoy options have started.

Default options are:

SecurEnvoy Batch Server
SecurEnvoy Radius
SecurEnvoy WebSMS Gateway



© 2017 SecurEnvoy All Rights Reserved

Active Directory Security

The LDAP Admin service account used by SecurEnvoy for SecurAccess and SecurPassword requires Active Directory permissions as follows –

- Read All User Attributes (Default Permission for all users)
- Write Access To "PrimaryTelexNumber" also referred to as "Telex Number"
- Write Access To "Telex Number Other"

Optionally, to allow user Mobile and Email address attributes to be updated from the SecurEnvoy admin GUI :–

- Write Access To Mobile Number (Optional)
- Write Access To E-Mail Address (Optional)

For SecurPassword and Integrated Desktop Logon :–

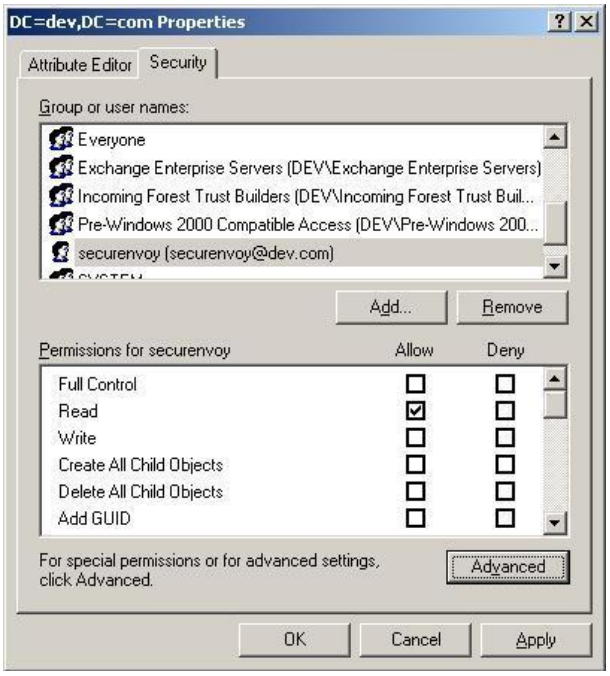
- User Object: "Reset Password"
- User Object: "Change Password"

Important

Do NOT use "Active Directory Users and Computers", you MUST use "ADSI Edit" or these edits will fail

Example: Admin User "SecurEnvoy" setup with ADSI Edit

For Windows 2008 Server



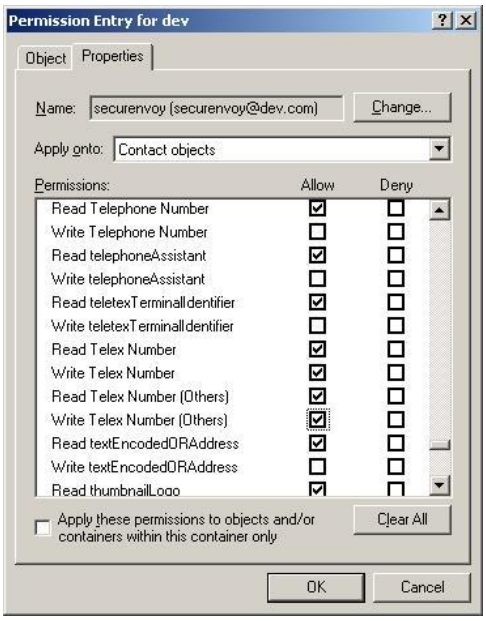
1. Create a user called "securenvoy" in the normal way and set "Password never expires" as this is a system account.

2. Right Click the top directory for example if your domain is called dev.com then right click "DC=dev,DC=com" and select Properties.

3. Select the "Security" tab and press the "Add" button to add the user securenvoy that you created in the first step.

4. Press the "Advanced" button.

© 2017 SecurEnvoy All Rights Reserved



5. Re-select the user in the Permission entries list.
6. Press the "Edit…" button and select the "Properties" tab.

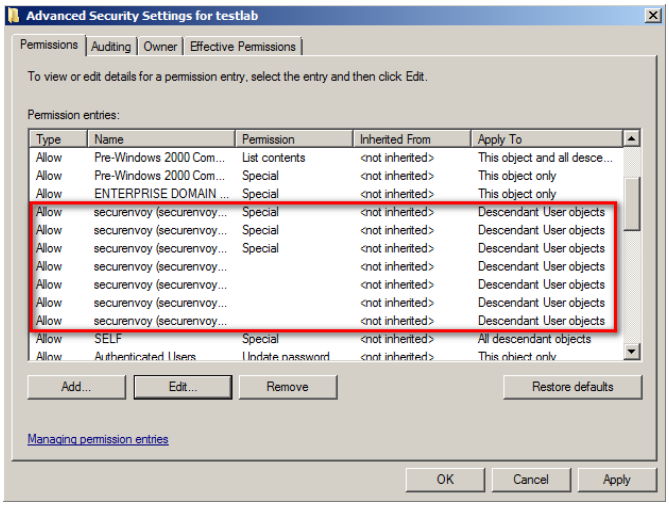
7. In the "Apply onto" field select "Descendant Contact objects"
    a. Tick Allow Write Telex Number
    b. Tick Allow Write Telex Number (Others)
    c. Tick Allow Write Mobile Number
    d. Tick Allow Write E-Mail

8. Change the "Apply onto" field from "Contact objects" to "User objects**"**. All the selected attributes will be carried over to "User objects".

9. Select the "Object" tab.

10. Select "Descendant User objects".

11. Tick Reset Password and Change Password (Both required only for SecurPassword or Integrated Desktop)

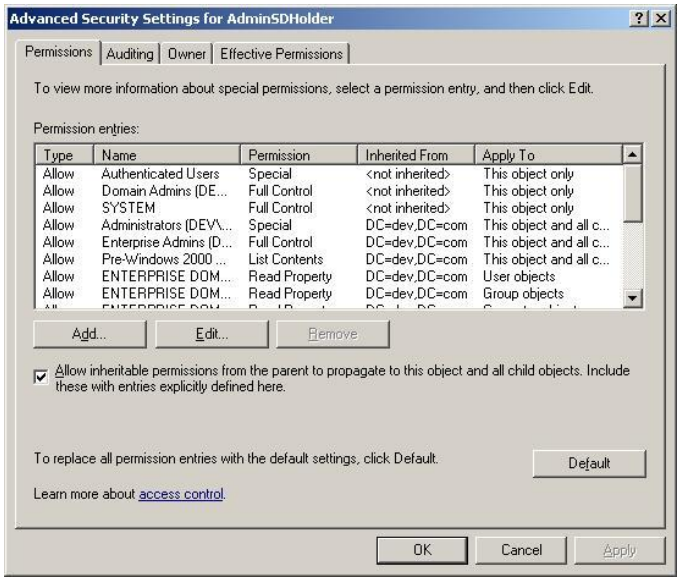


12. Press "OK".

13. Press "Apply". The account should now have the six permissions shown (*left*).

© 2017 SecurEnvoy All Rights Reserved

14. Right-click "AdminSDHolder" under the directory CN=system and select "Properties". Select the check box "Allow inheritable permissions". Press "OK". This adds support for users that are members of the following protected groups

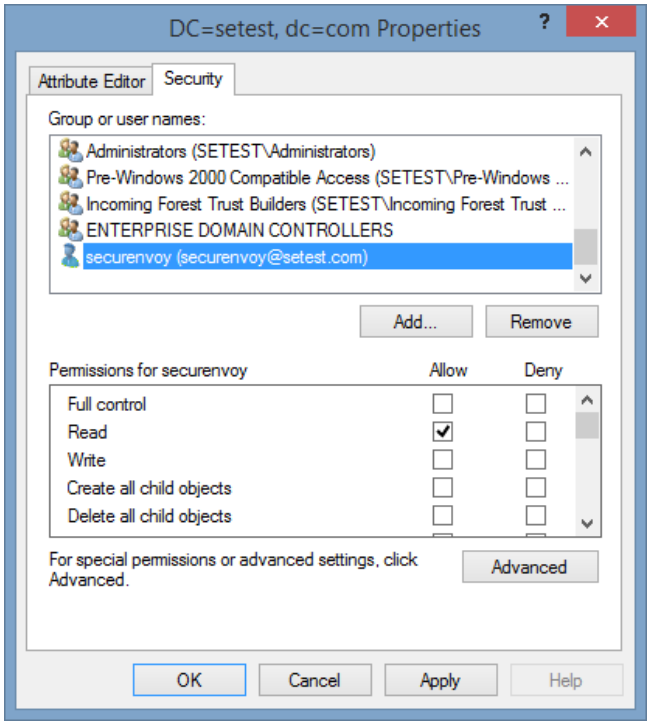


a. **Administrators**
b. **Account Operators**
c. **Server Operators**
d. **Print Operators**
e. **Backup Operators**
f. **Domain Admins**
g. **Schema Admins**
h. **Enterprise Admins**
i. **Cert Publishers**

Note

Write userAccountControl permission, found within Properties>descendant User Objects is also required for password reset

For Windows 2012 Server



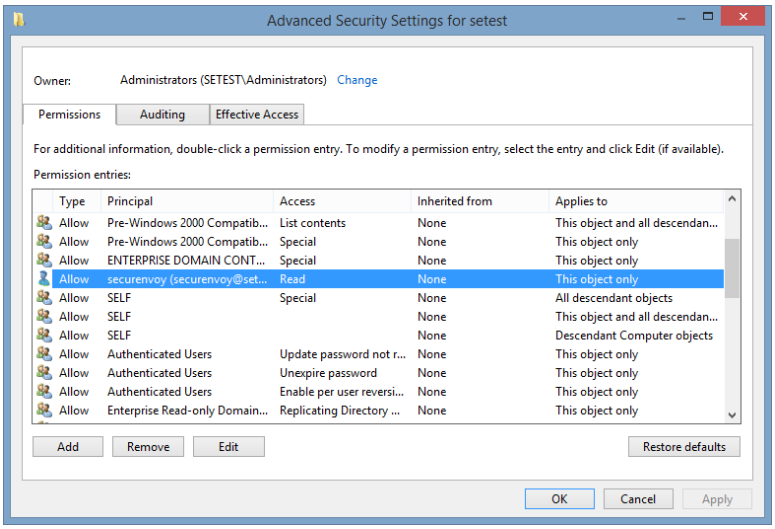
1. Create a user called "securenvoy" in the normal way and set "Password never expires" as this is a system account.

2. Run "ADSI Edit".

3. Right Click the top directory for example if your domain is called dev.com then right click "DC=dev,DC=com" and select Properties.

4. Select the "Security" tab and press the "Add" button to add the user securenvoy that you created in the first step.

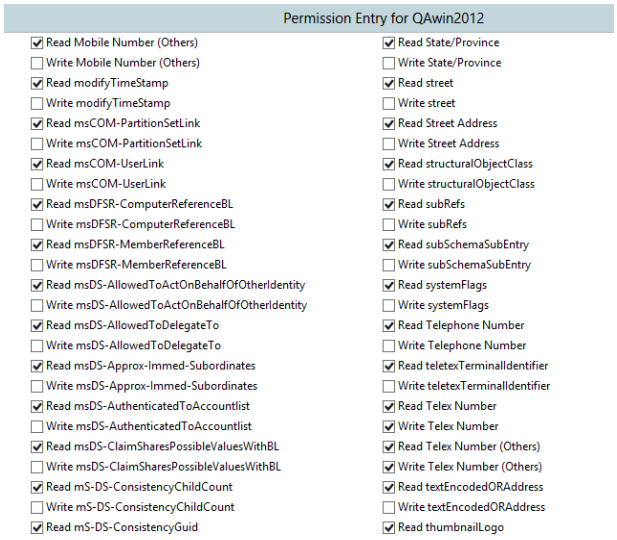
© 2017 SecurEnvoy All Rights Reserved



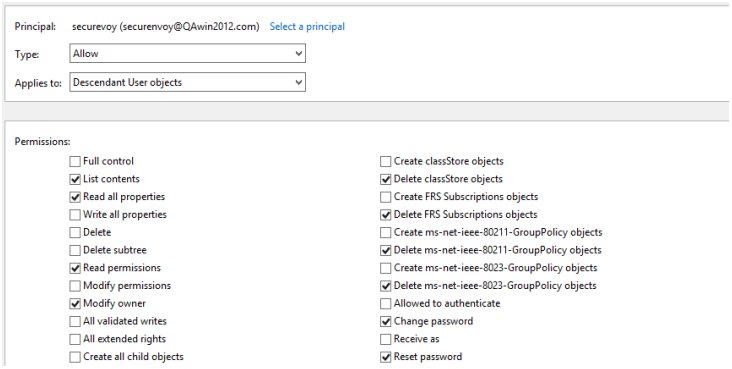
5. Press the "Advanced" button.

6. Re-select the user in the Permission entries list.

7. Press the "Edit…" button and select the "Properties" tab.



8. In the "Applies onto" field select "Descendant User objects"
   - Tick Allow Write Telex Number
   - Tick Allow Write Telex Number (Others)
   - Tick Allow Write Mobile Number
   - Tick Allow Write E-Mail
   - Click "OK"



9. At the 'Advanced Security Settings', click edit. In the "Applies to" field select "Descendant User objects" Tick Reset Password and Change Password (Both required only for SecurPassword or Windows Login Agent)

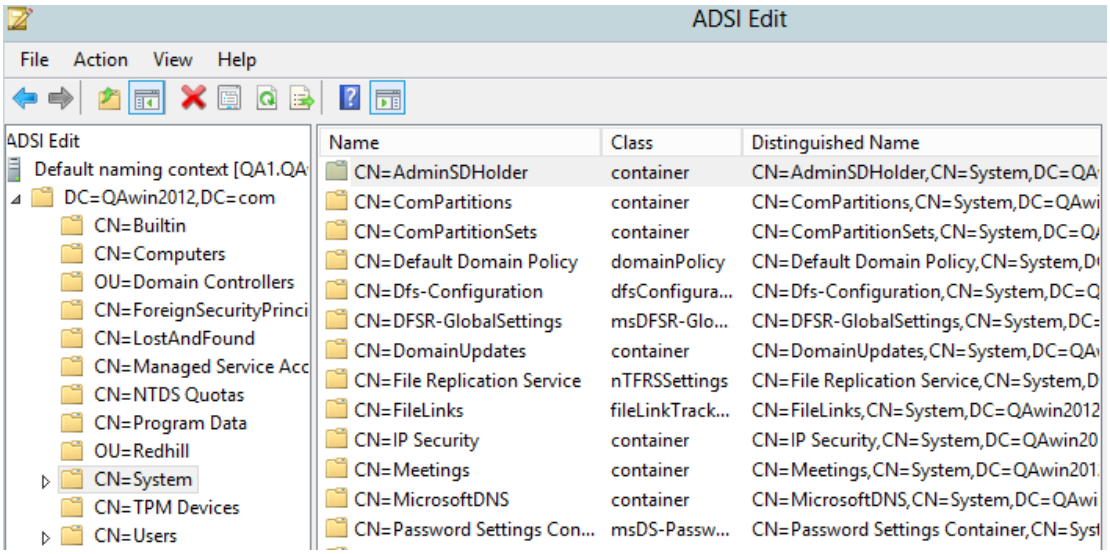
© 2017 SecurEnvoy All Rights Reserved

10. Press "OK".



11. Press "Apply". The account should now have the five entries shown above.

12. Right-click "AdminSDHolder" under the directory CN=system and select "Properties" → Security Tab → Advanced. Select the option "Enable Inheritance". Press "OK". This adds support for users that are members of the following protected groups –
    - Administrators
    - Account Operators
    - Server Operators
    - Print Operators
    - Backup Operators
    - Domain Admins
    - Schema Admins
    - Enterprise Admins
    - Cert Publishers



Note

Additional servers MUST share the same SecurEnvoy administration account for each domain they manage.

© 2017 SecurEnvoy All Rights Reserved

Note

Write userAccountControl permission, found within Properties>descendant User Objects is also required for password reset

To Test, Start the SecurEnvoy Admin GUI and enable a user, enter the mobile number and press "Update User"
You should get the message. "OK, Passcode Sent To Gateway"
"If you get the message "ERR, Error writing to LDAP, General access denied error" then your write permissions are incorrect.

SecurEnvoy Service Permissions Account Wizard

Create a service account within Active Directory Users and computers and set the account so that the password does not expire.

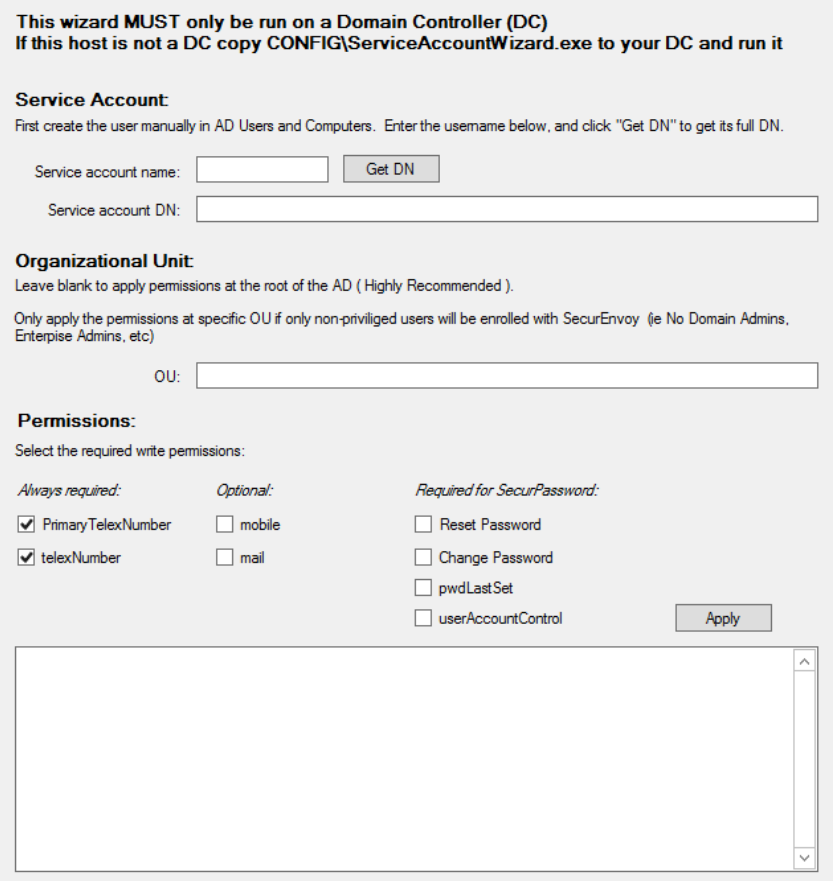
Enter the service account within the Service account name field and click 'Get DN'

It is also possible to set a specific OU, although this should not be required within most environments.

Set the permissions you desire to use:

Primary TelexNumber
telexNumber
mobile
mail
Reset Password
Change Password
pwdLastSet
userAccountControl

Then click 'Apply'



© 2017 SecurEnvoy All Rights Reserved

7.0 LDAP (OTHER) SECURITY

It is required that the LDAP Admin account used by SecurEnvoy for SecurAccess and SecurPassword should have Active Directory permissions as follows:-

Read All User Attributes (Default Permission for all users)
Write Access To Telex Number
Write Access To Mobile Number (Optional)
Write Access To E-Mail Address (Optional)
User Object: "Reset Password" (Only required for SecurPassword or Integrated Desktop Logon)

Note

When installing "SecurEnvoy Managed Users" Microsoft ADAM, only a username is required as SecurEnvoy will automatically create an admin account called "securenvoy". In addition "SecurEnvoy Managed Users" Microsoft ADAM will always use a PIN as the password can be seen in clear text (this is a limitation of Microsoft ADAM).

© 2017 SecurEnvoy All Rights Reserved

8.0 NOTES

© 2017 SecurEnvoy All Rights Reserved