SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

SecurEnvoy Security Server 9.3

Installation Guide

SecurEnvoy Security Server 9.3

Contents

1.1 Solution Summary

This document walks you through an installation of the SecurEnvoy Security Server product within your environment quickly and easily.

1.2 Getting Started

The purpose of this document is to outline the general steps for the installation and validation of the SecurEnvoy Security Server Two-factor Authentication Solution within your environment quickly and easily.

The SecurEnvoy Two-Factor Authentication Solution has many features and options. We will not be covering all features and options in this guide. The intent of this guide is to provide instruction for the initial implementation and allow customers to explore additional features as they see fit.
Advanced configuration features are not covered here. If you are looking for advanced configuration instructions, please refer to the Help section in the SecurEnvoy Admin Console.
At the end of this guide you will have a fully functional environment.

1.2.1 Things You Will Need

This document will assume that the reader is a network and systems administrator with administrative level access to the systems required for this implementation, listed below. If you do not currently have this level of access to the environment, you should obtain it before you continue.
To properly implement SecurEnvoy SecurAccess you will need the following;

- A single Microsoft Windows 2008 R2, 2012 R2 or 2016 Server, either physical or virtual.
- Administrative Access to your Microsoft Active Directory.
- Download the SecurEnvoy SecurAccess product latest version.

Download is available here: https://www.securenvoy.com/products/securaccess/key-features.shtm

Microsoft Windows 2008 R2, 2012 R2 or Windows 2016
Here are some basic items to cover about the server you chose to use.

- Your server can be physical or virtual.
- Your selection of which server version you choose does not impact the implementation.
- Please assure that your server is fully patched as a best practice.
- There is no requirement for the SecurEnvoy Security server to be a member of the Active Directory.

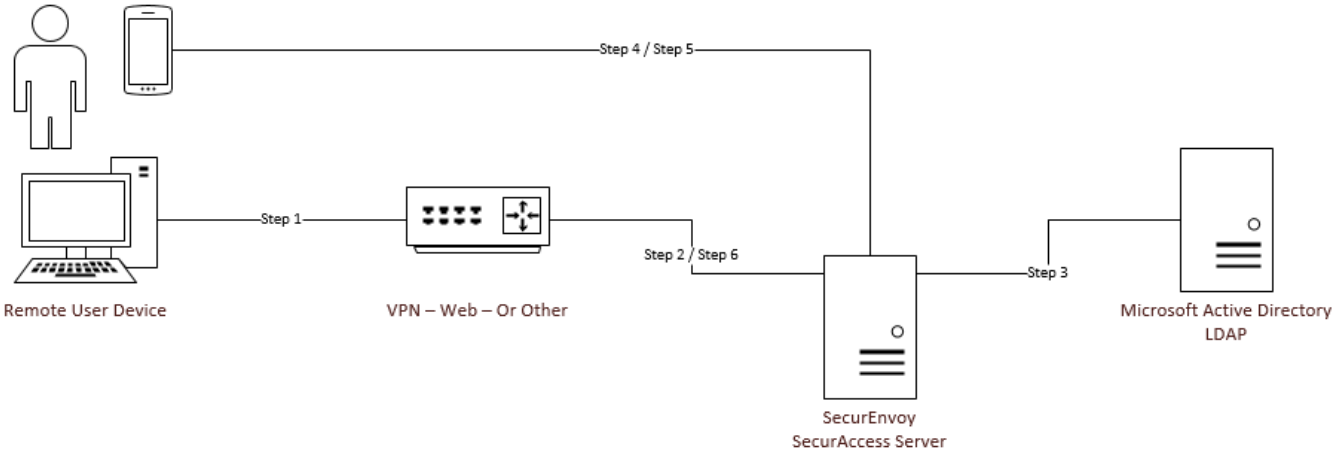
Examples;

- Microsoft Windows 2012 R2 Virtual Guest on VMware ESX and is a member of the Active Directory.
- Microsoft Windows 2008 R2 Physical Server in a workgroup.

Either of the above examples will work.

1.2.2 Authentication Processing Topology

SecurEnvoy SecurAccess will integrate with any solution that can use RADIUS, such as; A10, Amazon Web Services, F5, IBM, Microsoft, Oracle, SalesForce, VMware, Barracuda, Check Point, Cisco, Citrix, Juniper, Palo Alto, SonicWall, Sophos, WatchGuard, Linux and many others.
In the below simplified diagram, we are showing a VPN, using RADIUS with SecurEnvoy SecurAccess Two Factor Authentication and a Microsoft Active Directory.



Step 1: The user on a device (internal or external) makes a request for authentication to a VPN, Web Site or some other application which uses RADIUS authentication.

Step 2: A RADIUS authentication package is delivered to the SecurEnvoy SecurAccess Server for processing.

Step 3: LDAP Credentials are validated against the Microsoft Active Directory.

Step 4: Using information from the Active Directory user account, an Approve / Decline message is delivered to
the users' mobile device.

Step 5: The user approves the authentication by acknowledging the message. This causes the SecurEnvoy Phone App to send Secure Passcodes to the SecurEnvoy Server.

Step 6: The SecurEnvoy Server returns a 'Good to Go' message to the VPN.

It's important to note that there are many options and methods for delivering the second factor authentication. In our example and for the purposes of this quick start guide, we're keeping it as simple as possible.

As you explore the product and its features, you'll find the many options available and we encourage you to try ones that you would want to work with in your environment.

1.3 Pre-requisites

1.3.1 Software Requirements

- Windows 2008 (R2) / Windows 2012 (R2) / Windows 2016
- IIS installed with default settings (Site ID 1 "Default Web Site")
- Microsoft .NET 4.5 installed for SecurEnvoy 9.3.x and later. Microsoft .NET 2 and .Net 3.5 installed for SecurEnvoy 8.1.x and earlier.
- Active Internet Connection

1.3.2 Hardware Requirements

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

1.3.3 For integrated user management

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

- Read All User Attributes (Default Permission for all users)
- Write Access to Telex Number
- Write Access to Telex Number (other)
- Write Access to Mobile Number (Optional)
- Write Access to E-Mail Address (Optional)

Please refer to Configure Your Service Account

1.3.4 SMS Requirement

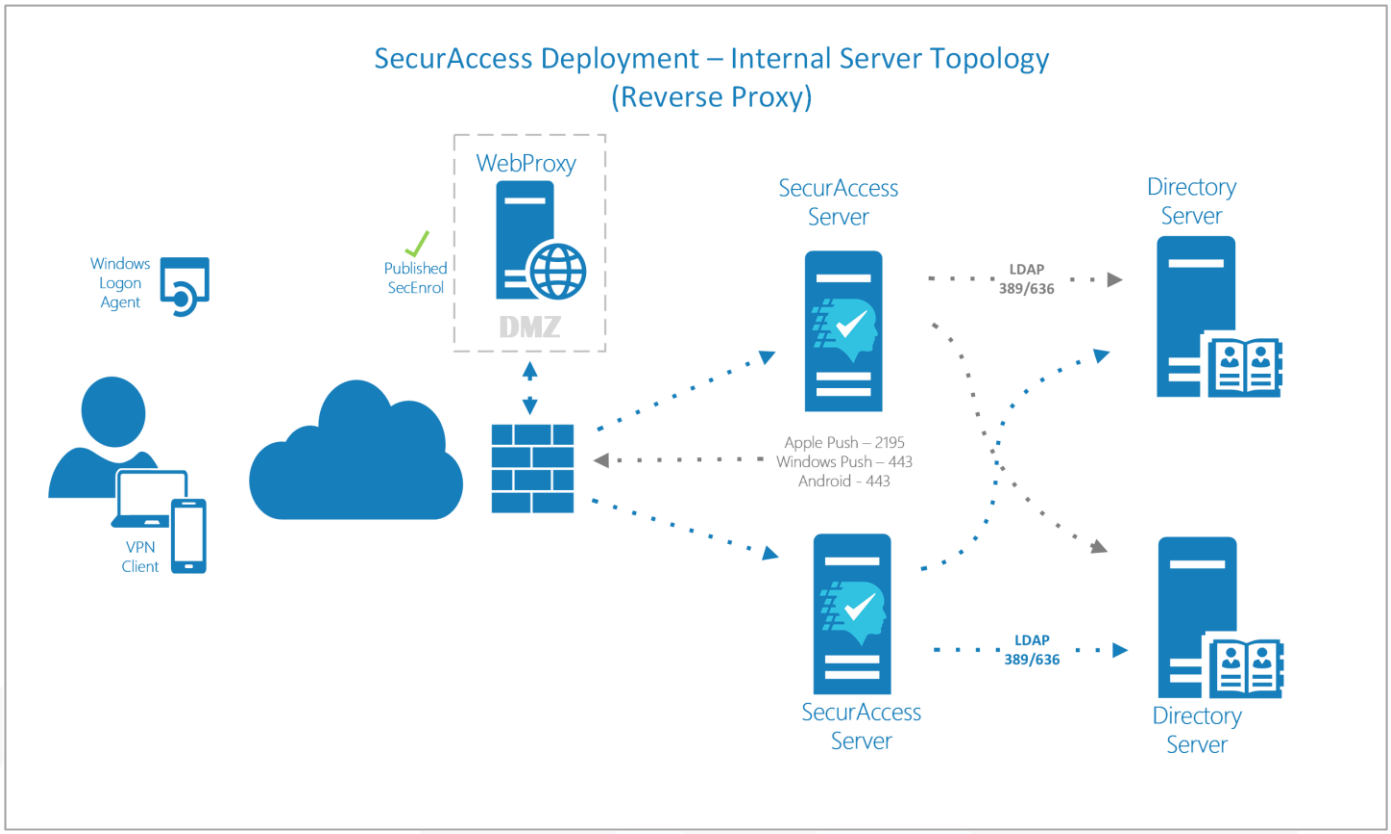
If you are upgrading from a trial license to a live license, please ensure you have an SMS gateway in place if you wish to use this authentication method going live, as live licenses DO NOT include any free SMS messages. For Additional Information on SMS Gateways see:

http://www.securenvoy.com/support/SMSgateway.htm

1.3.5 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. Push notifications work by sending a message to the notification centre or status bar of a users[1] smartphone. This new feature is dependent on the architectural topology of the SecurEnvoy Server implementation.

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

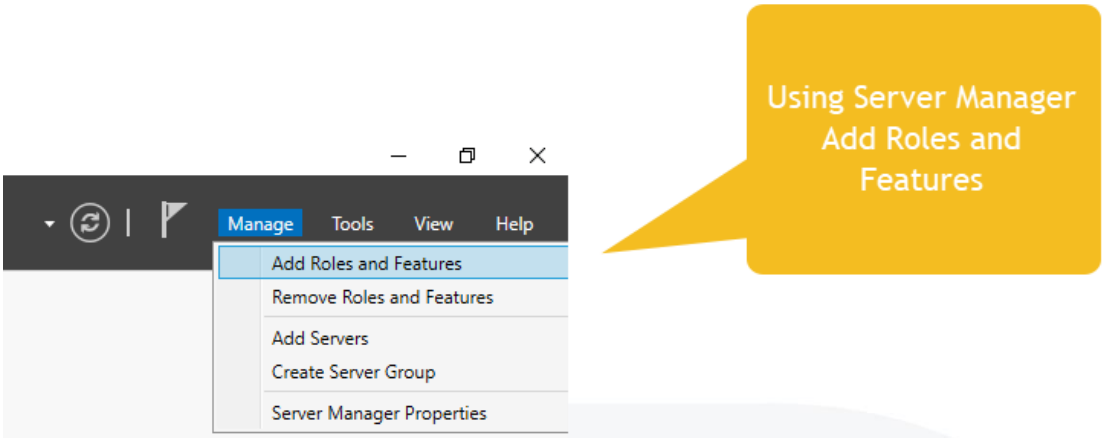
- All token types are supported including oneswipe push and NFC.
- Users are able to manage their tokens externally from any Internet location.

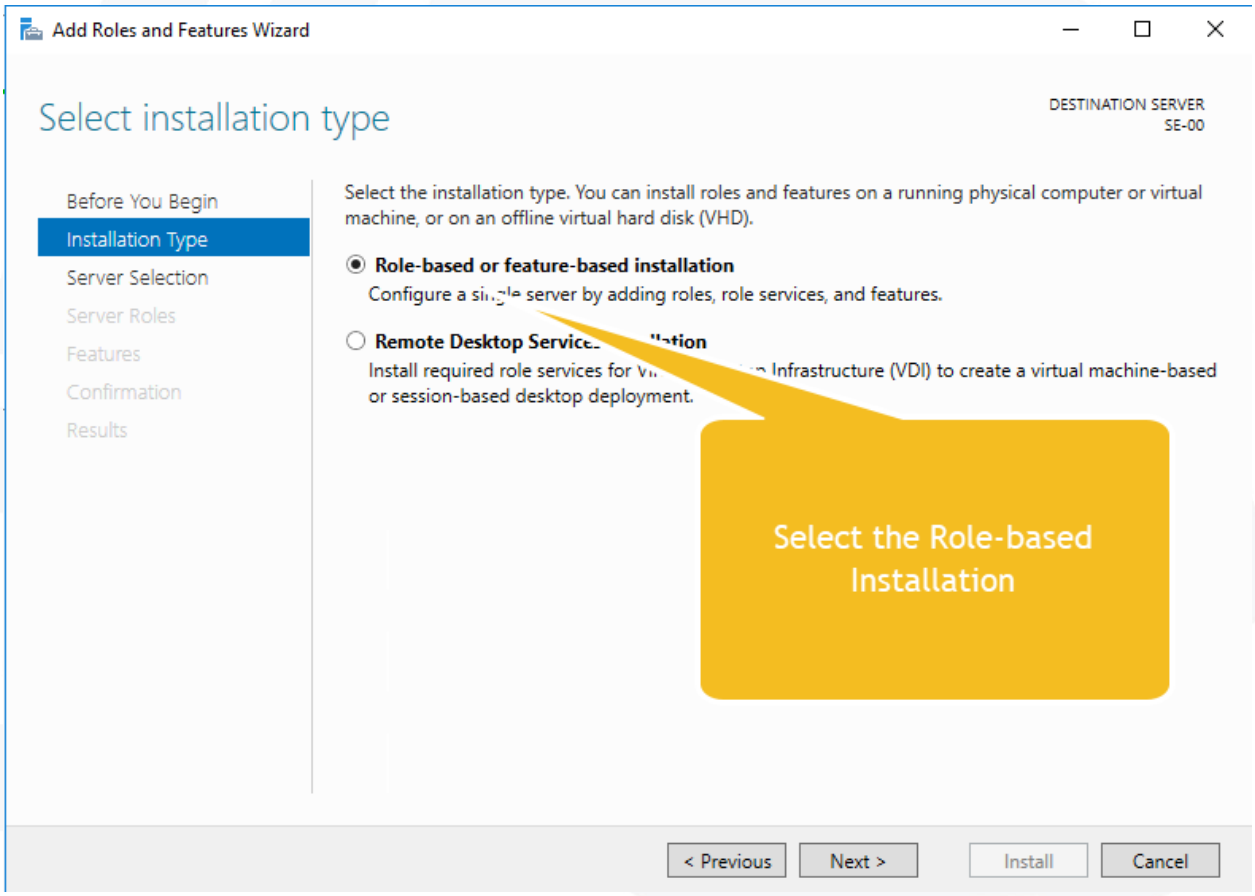
Disadvantages of this topology

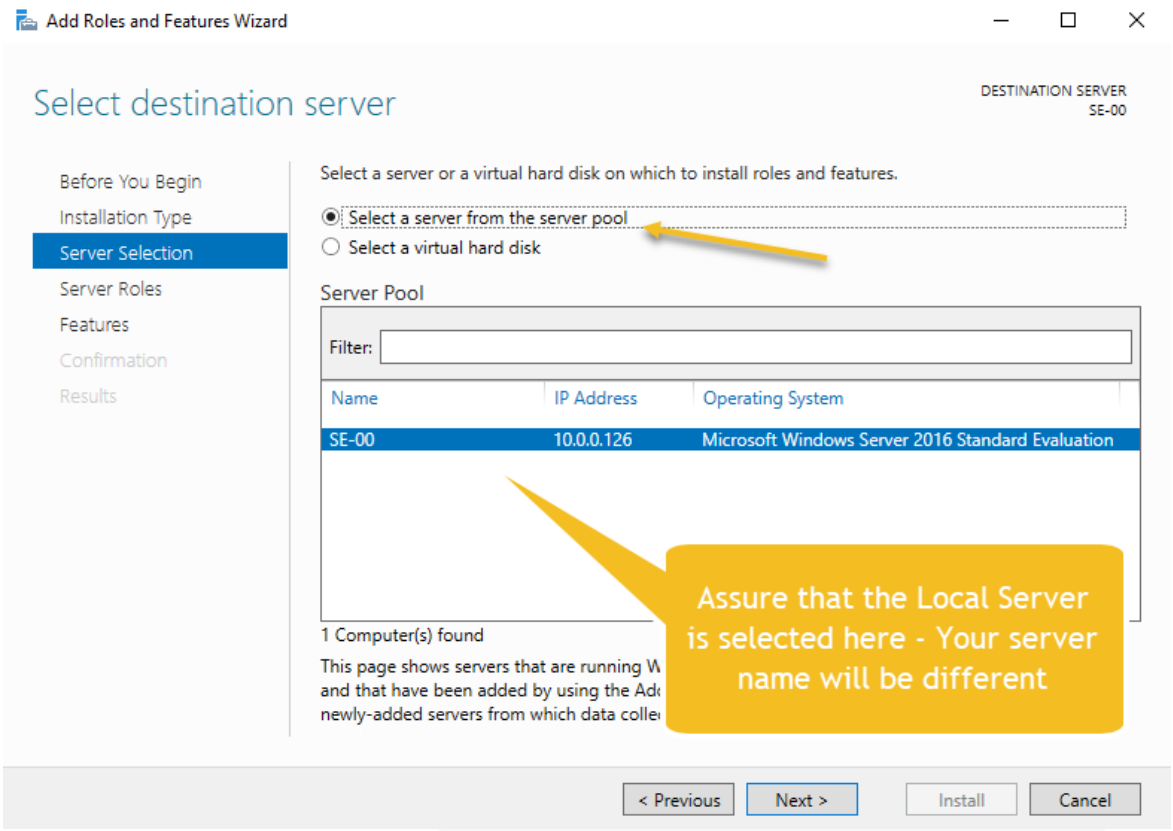
- Manage My Token portal must be published to the Internet

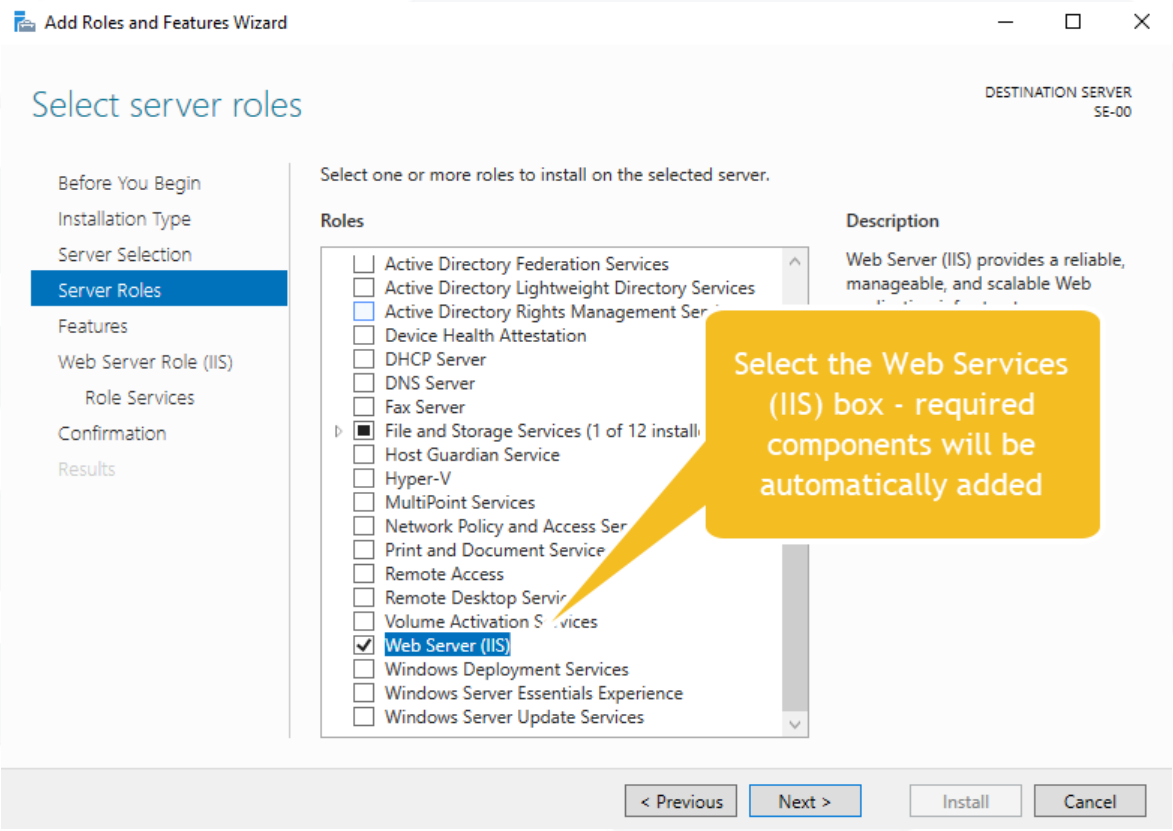
1.4 Installation of Microsoft IIS Web Services

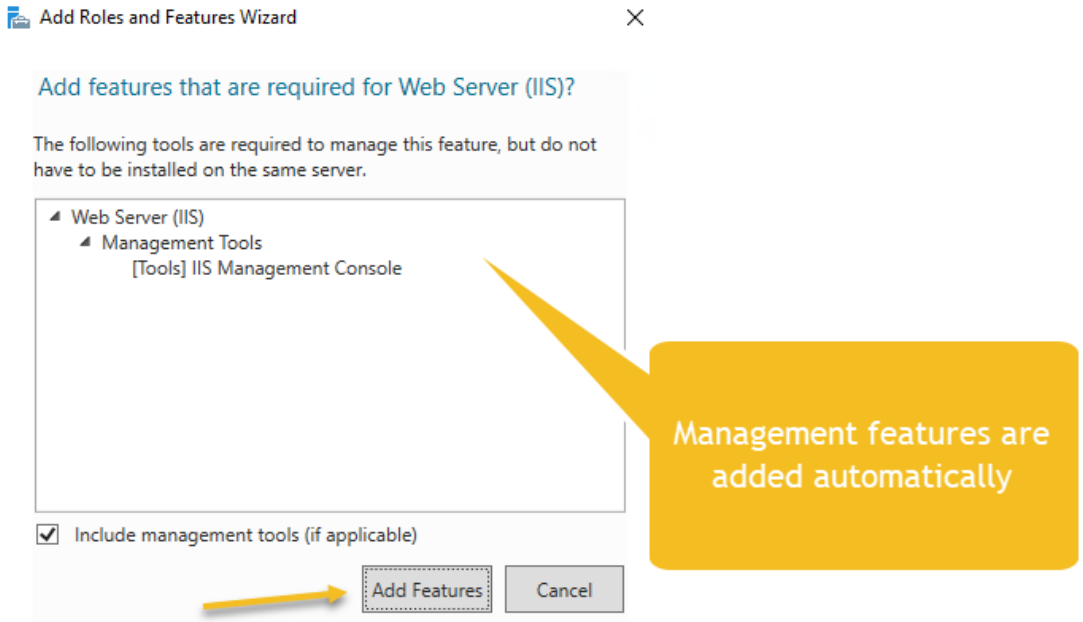
The SecurEnvoy SecurAccess Two Factor Authentication Solution uses http and https for communication. This allows you to use the solution both internally and externally easily.
We will begin the implementation with the web components that are required for the SecurAccess. Microsoft IIS Web Services.

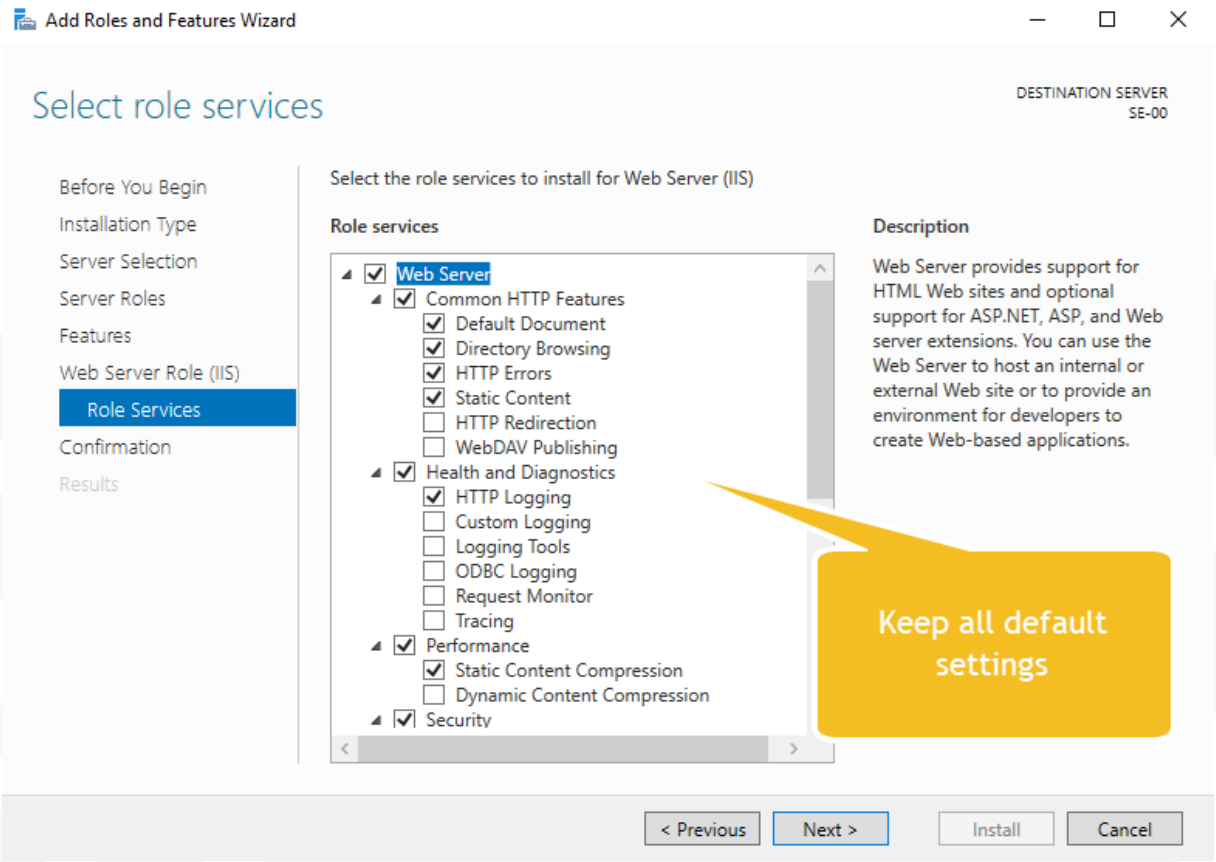


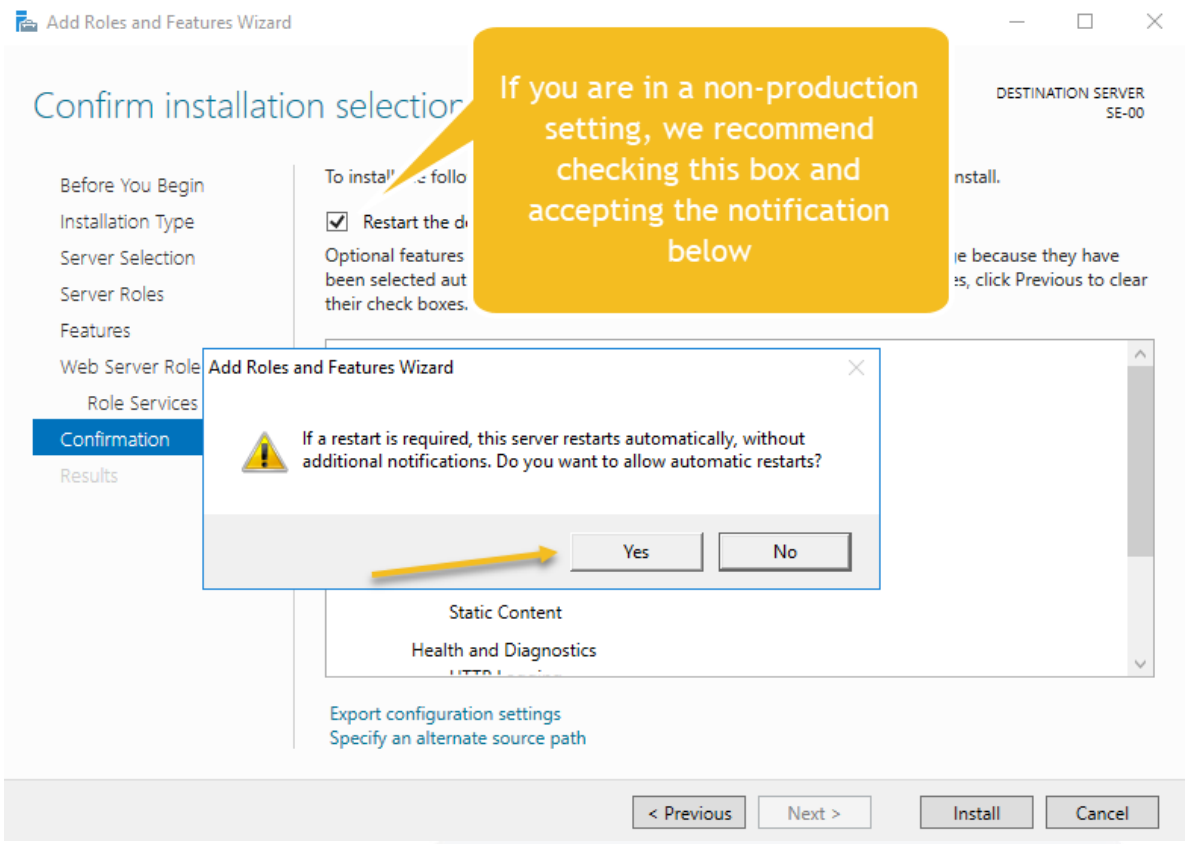


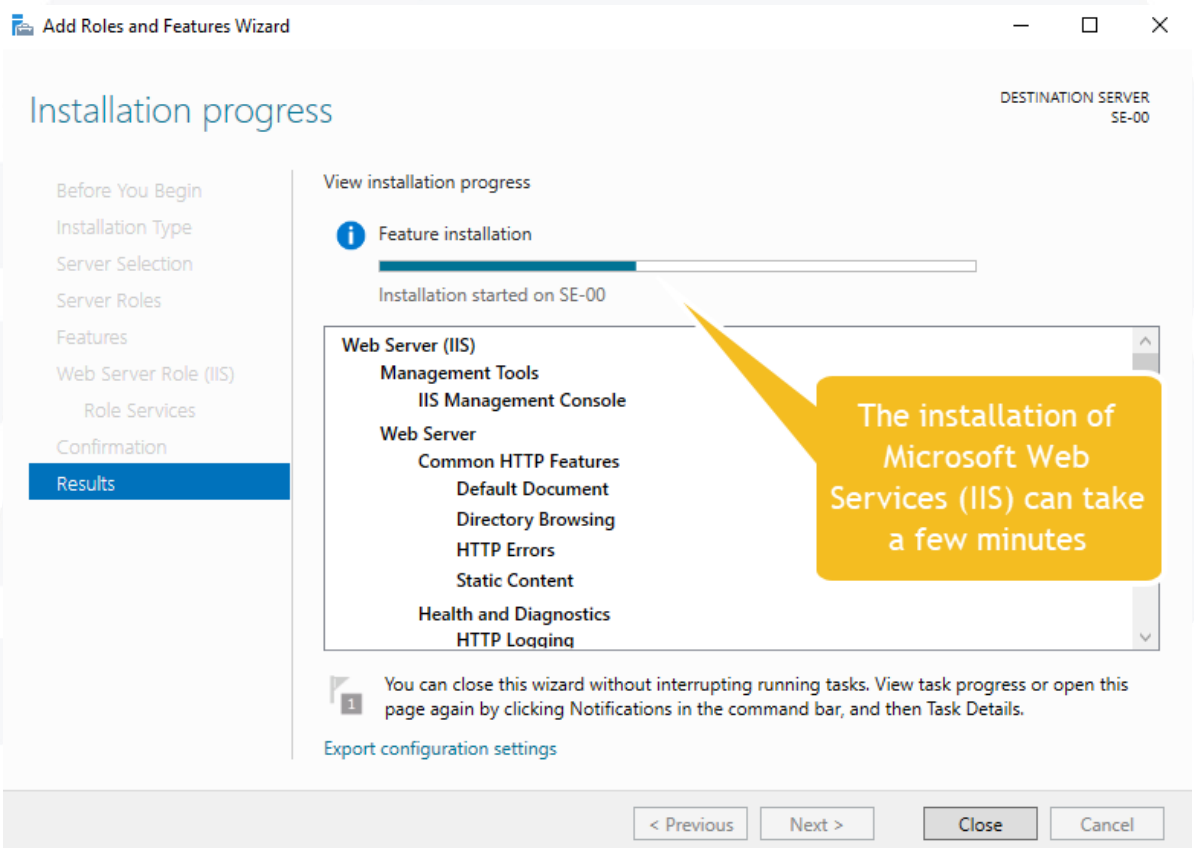

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
SE-00
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
SE-00
10.0.0.126
Microsoft Windows Server 2016 Standard Evaluation
1 Computer(s) found
This page shows servers that are running W
and that have been added by using the Ad
newly-added servers from which data colle
Assure that the Local Server is selected here - Your server name will be different
< Previous
Next >
Install
Cancel

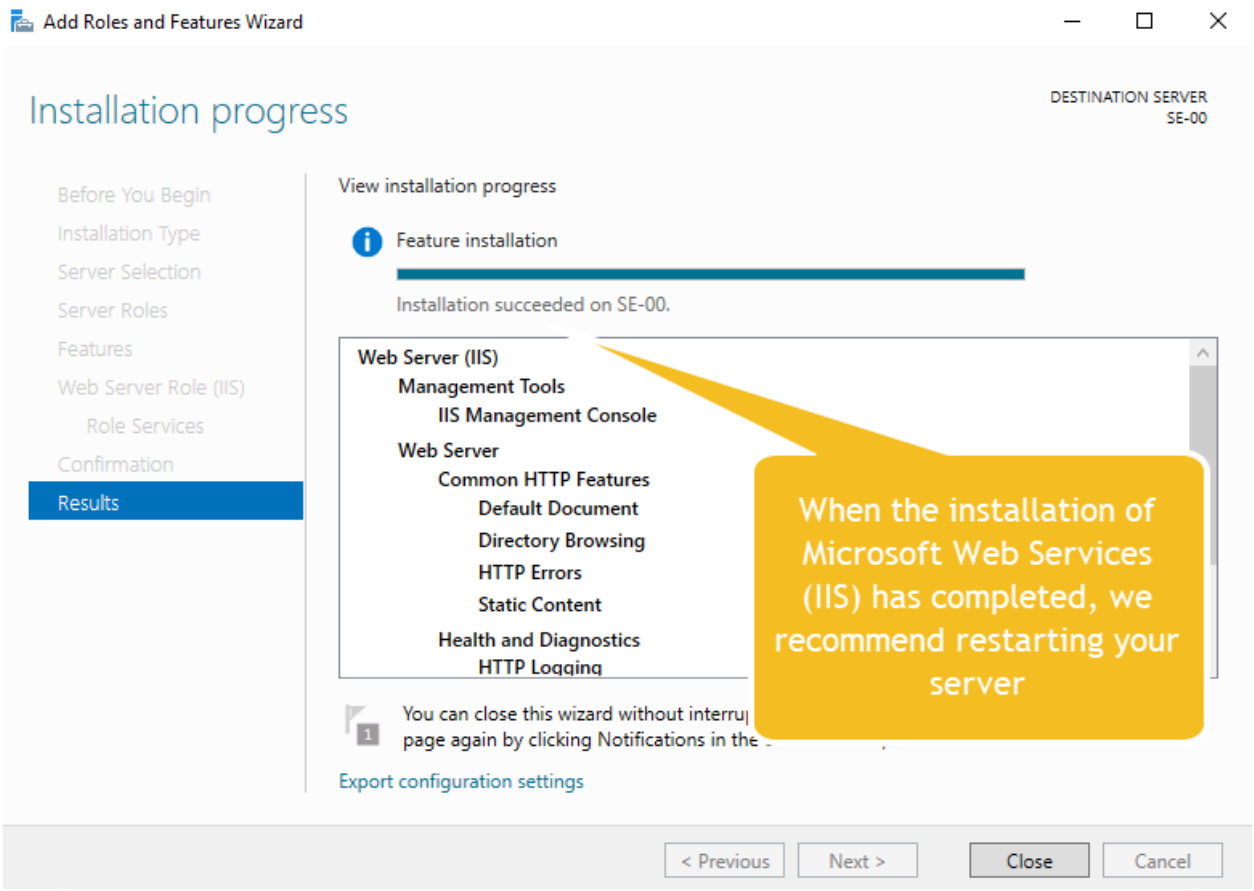

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
SE-00
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Description
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Ser
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 install
Host Guardian Service
Hyper-V
MultiPoint Services
Network Policy and Access Ser
Print and Document Service
Remote Access
Remote Desktop Servic
Volume Activation S vices
Web Server (IIS)
Windows Deployment Services
Windows Server Essentials Experience
Windows Server Update Services
Web Server (IIS) provides a reliable, manageable, and scalable Web
Select the Web Services (IIS) box - required components will be automatically added
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
Management features are added automatically


Add Roles and Features Wizard
Select role services
DESTINATION SERVER
SE-00
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Description
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
Keep all default settings
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Confirm installation selection
DESTINATION SERVER
SE-00
If you are in a non-production setting, we recommend checking this box and accepting the notification below
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role
Role Services
Confirmation
Results
Restart the d
Optional features
been selected aut
their check boxes.
Add Roles and Features Wizard
If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?
Yes
No
Static Content
Health and Diagnostics
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
SE-00
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation started on SE-00
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
The installation of Microsoft Web Services (IIS) can take a few minutes
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel


Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
SE-00
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation succeeded on SE-00.
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
When the installation of Microsoft Web Services (IIS) has completed, we recommend restarting your server
Export configuration settings
< Previous
Next >
Close
Cancel

1.5 Installing & Configuring SecurEnvoy SecurAccess

Available SecurEnvoy Web Portals That Can Be Installed

- **Admin Portal** – This provides the SecurEnvoy Security Server Admin console. It is not recommended to publish this to the Internet unless you are a cloud provider.

- **Manage my Token Portal** - This may be required for initial enrolment and for ongoing management of token types, such as migrating to a new phone. See above details.

- **Lost Token Emergency Access Portal** – This allows end users to request a temporary code whilst disabling their lost device via this self-service portal. Note: This portal is not protected with 2FA and relies on a combination of pin/password and answers to predefined secret questions. Typically, customers would not publish this to the Internet and would rely on a manual helpdesk process or the user being connected to the internal LAN.

- **SecurPassword Portal** – This is part of the SecurPassword product and is only required if this function is being utilized. Allows end users to reset their Microsoft AD (or other LDAP) password and requires 2FA for access.

- **SecurMail Sender Portal** - This is part of the SecurMail product and is only required if this function is being utilized. It allows a sender to create secure 2FA emails to recipients. Installing this portal will also add an additional IIS web service called SecUpload2, which is used to upload SecurMail file attachments. These are optional and only required to be published to the Internet if your senders need to create emails externally.

- **SecurMail Recipient Portal** - This is part of the SecurMail product and is only required if this function is being utilized. This portal must be published to the Internet or recipients will not be able to retrieve their secure messages. This portal uses 2FA.

- **SecServer Portal** – This portal is required for SecurAccess if you wish to use Windows Logon Agent externally on the Internet, for instance for logging in on a remote laptop. This is not required if you are not using Windows Logon Agent or only use the agent to protect internal servers and desktops. This portal is required for SecurMail if a recipient is connecting from an external SecurEnvoy Outlook Agent that is connecting across the Internet or a SecurMail phone app that is also connecting across the Internet.

- **SecRep** is installed by default on all server instances and is used to automate the replication of the server.ini file between multiple SecurEnvoy servers, if this function is enabled.

CAUTION!

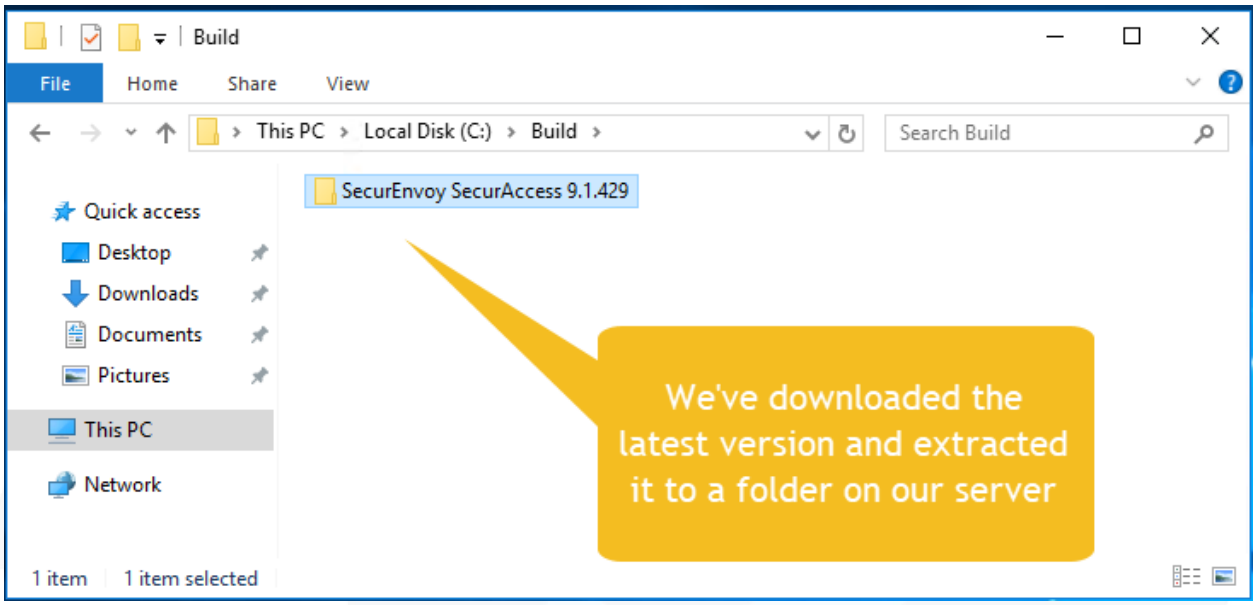
Do not publish SecRep to the Internet, as this will risk exposing configuration settings to external threats.

The following steps are required to configure the SecurEnvoy SecurAccess product for use. Please note that this configuration is for trials and some components, like Secure LDAP and HTTPS are not used in these examples. If you require these for your trial, please reference the SecurEnvoy SecurAccess Administrators Guide that was included in your download.

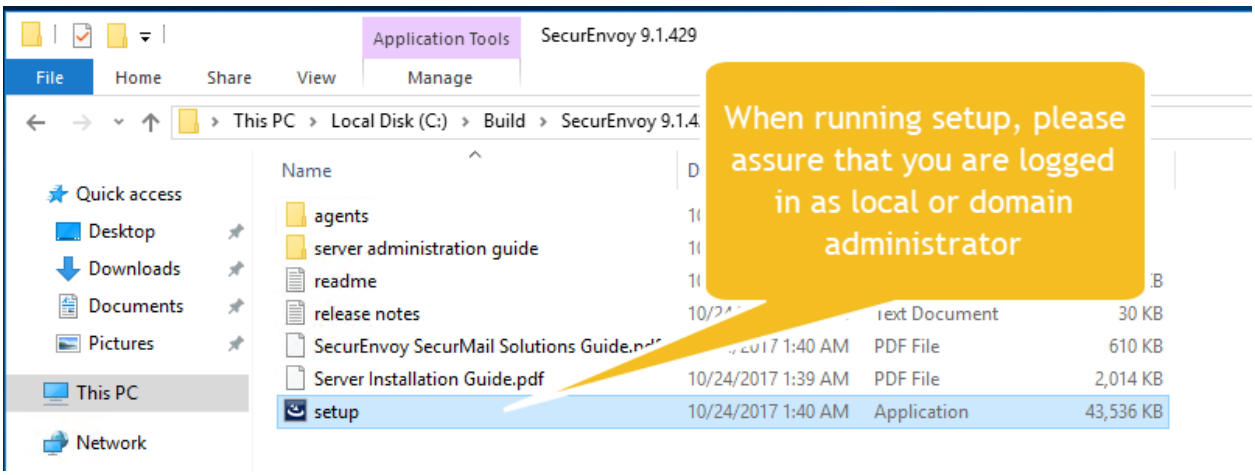
We suggest gathering the following before getting started to make things easy.

- Microsoft Active Directory Service FQDN and NetBIOS name
- FQDN for at least one Domain Controller
- Create (or use) a Service Account – only needs to be a domain user.
- Email server FQDN
- Email account with credentials

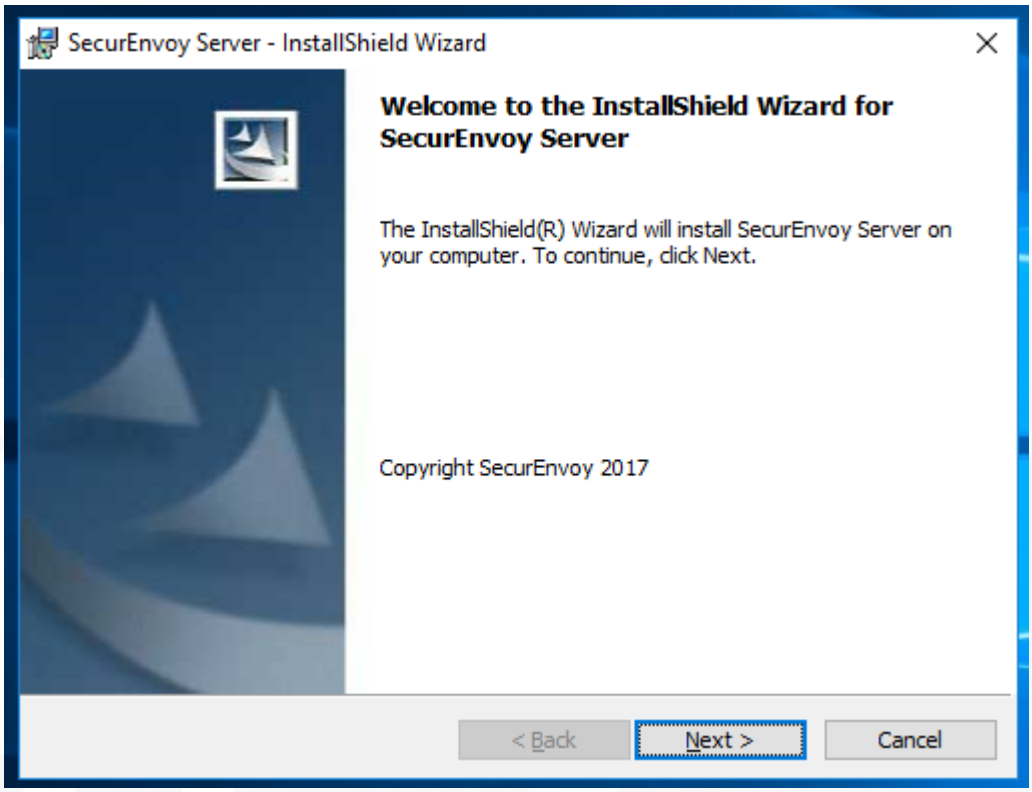
We will begin with the base installation of the SecurEnvoy SecurAccess product.
Download is available here: https://www.securenvoy.com/products/securaccess/key-features.shtm



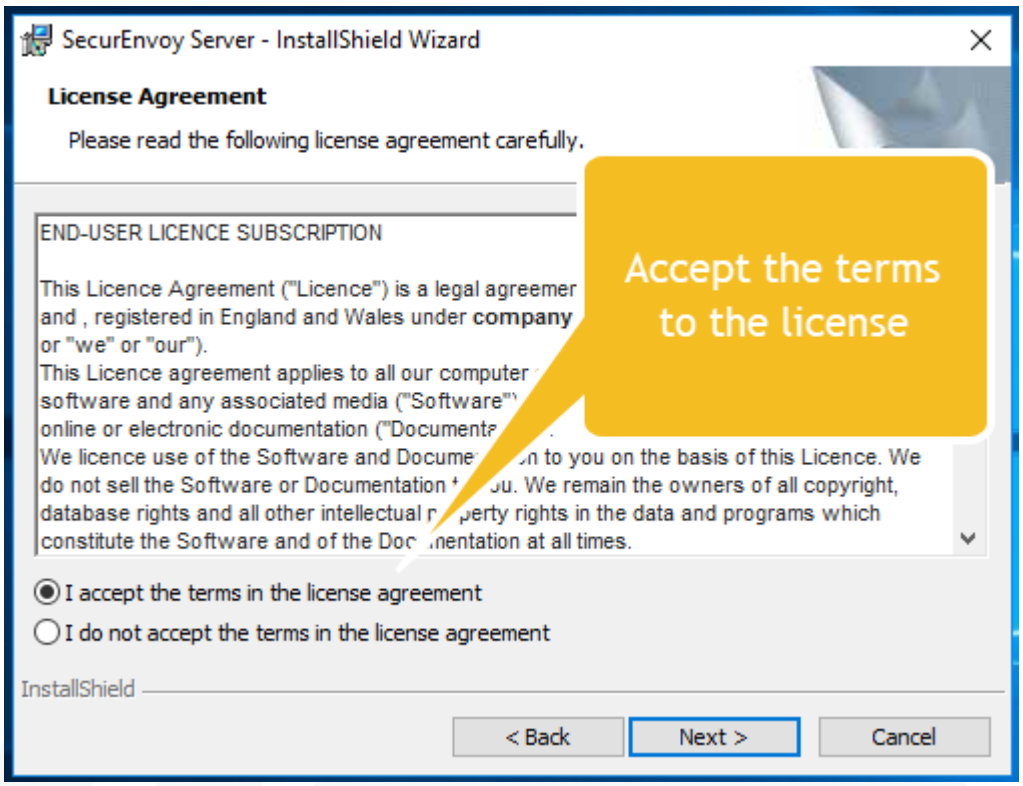
As you can see from the illustration, we've also created a build folder at the root of our server volume. Although we suggest this, it's not mandatory. You can extract our download anywhere you like.



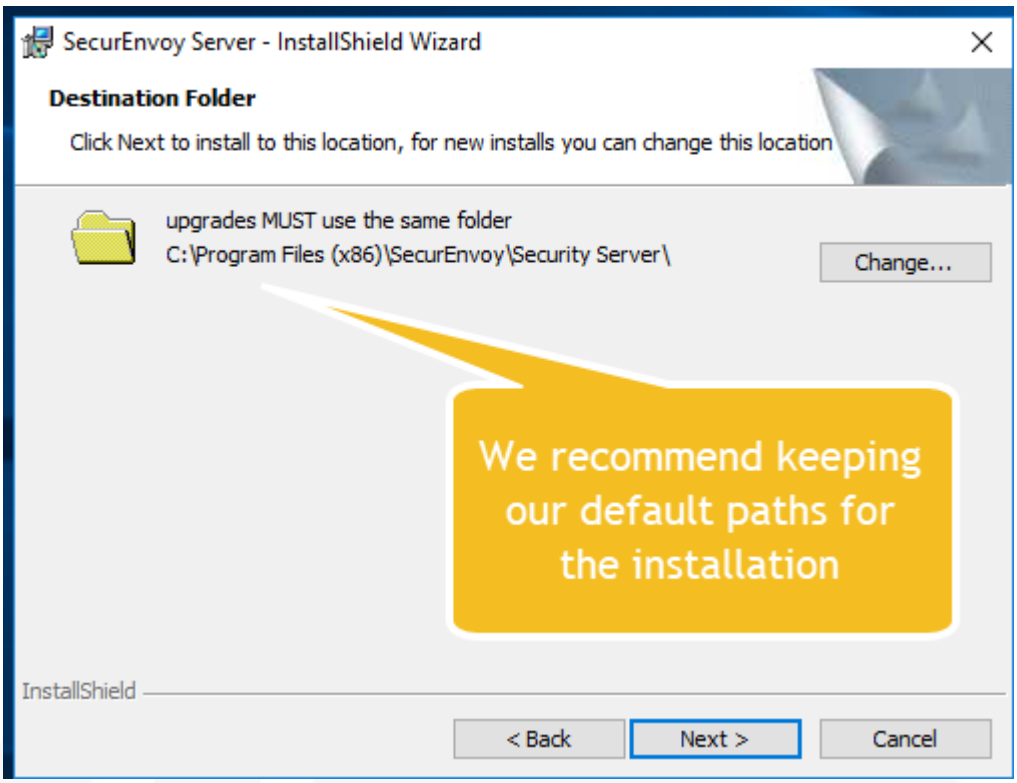
Active Directory Membership for the SecurEnvoy SecurAccess Server is optional. If your server is part of the Microsoft Active Directory, we suggest logging in as a Domain Administrator.



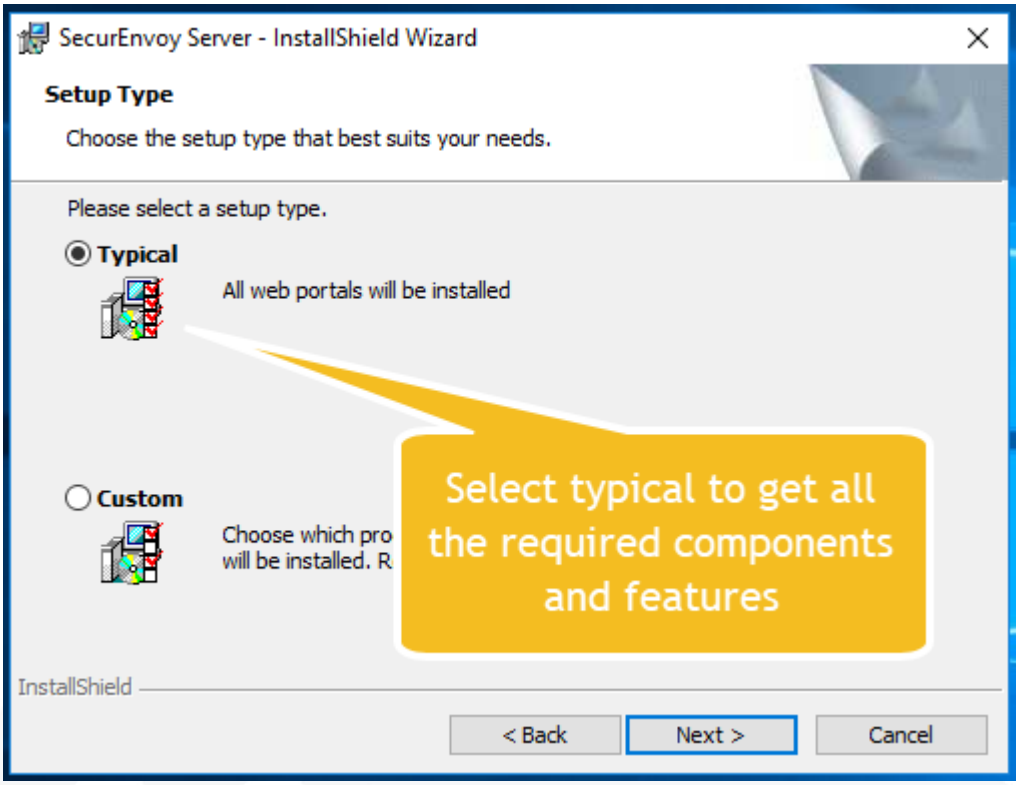
Welcome to the installer!



Please make sure to read the contents of the End User Licensing Agreement. There are updates from previous versions.

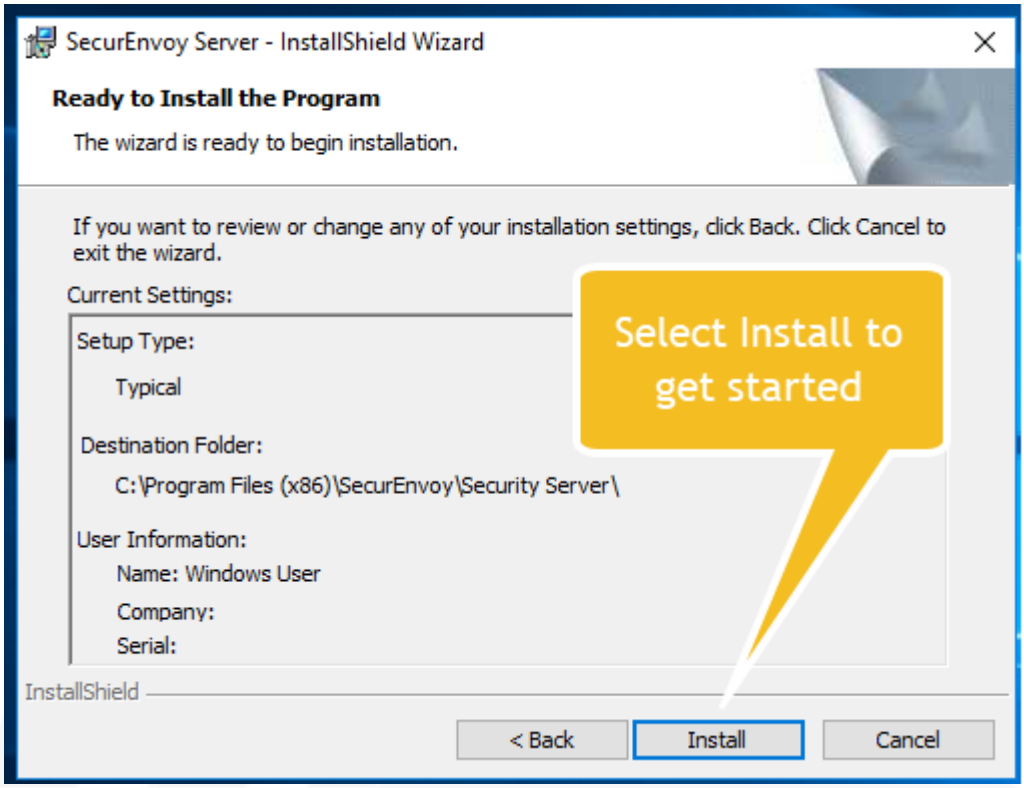


We would like you to keep the standard default paths if possible. However, if you must change it, please take note of the new location, because you will need that later for future upgrades.

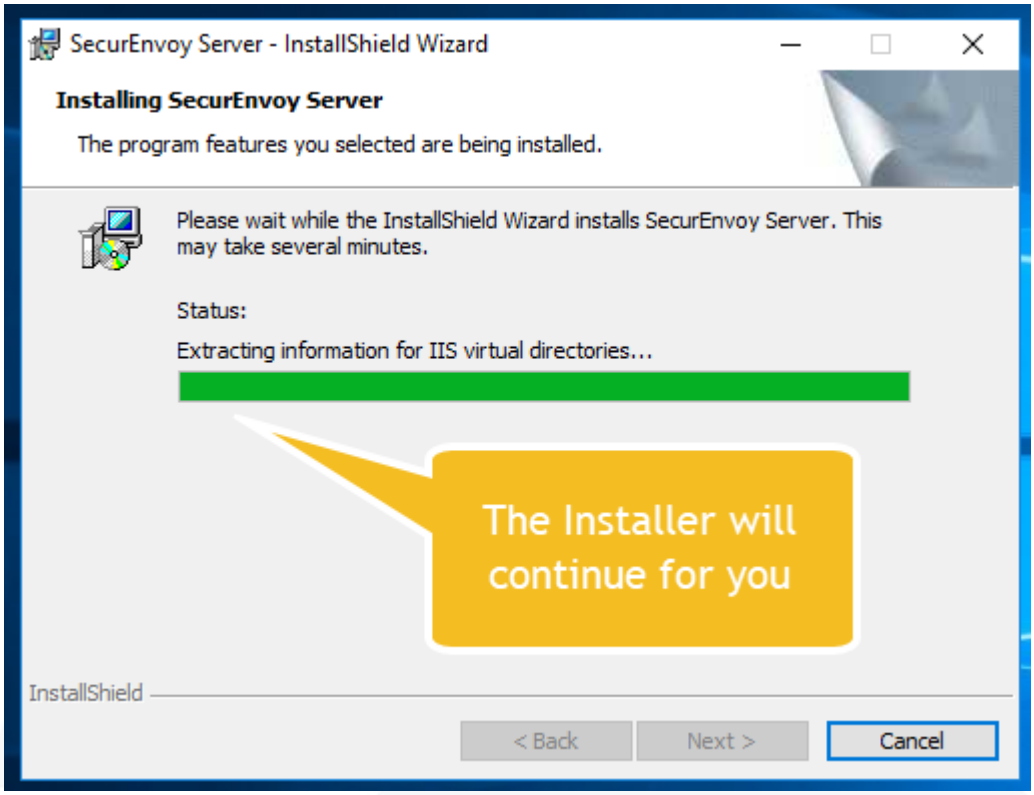


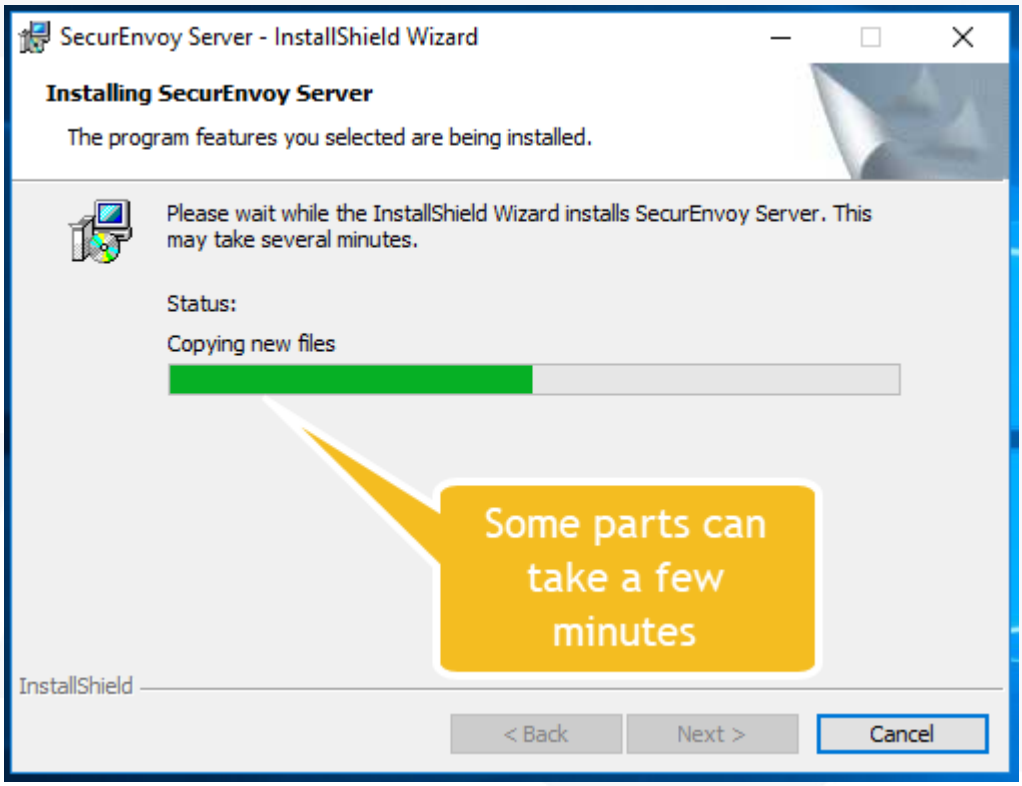
A typical installation is suitable for most small and medium sized businesses. This setup assumes that the SecurEnvoy SecurAccess server is behind a firewall and NAT'd.

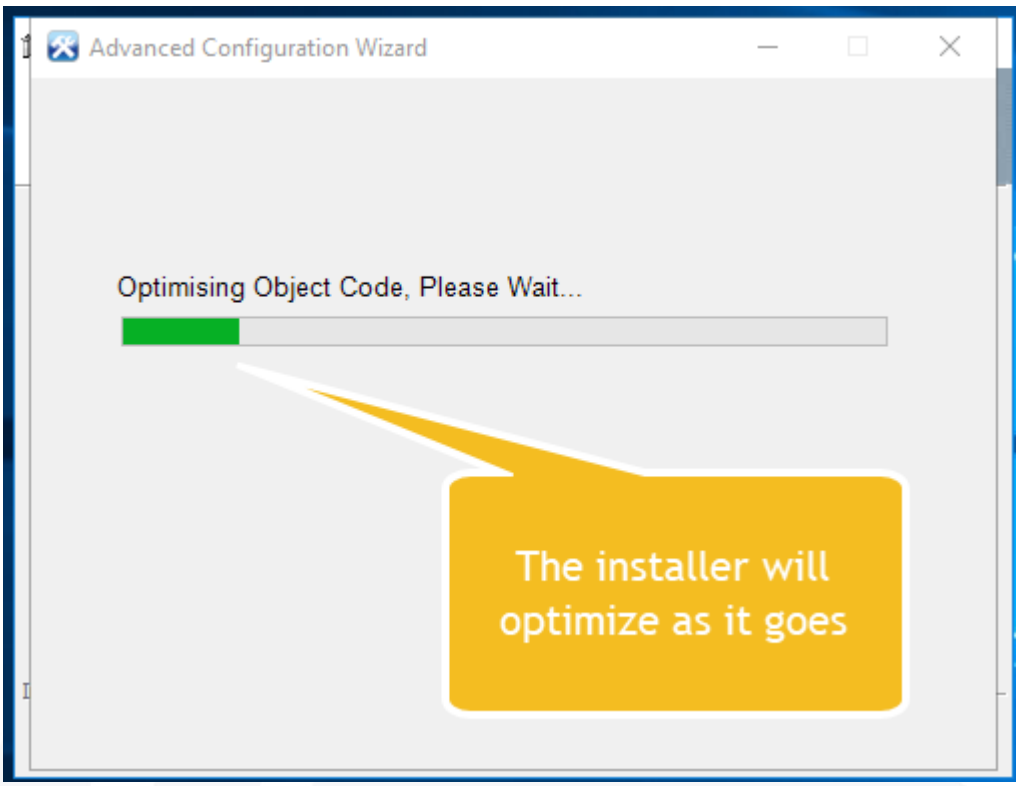
Highly Available options are available and described in the Advanced Administrators Guide.

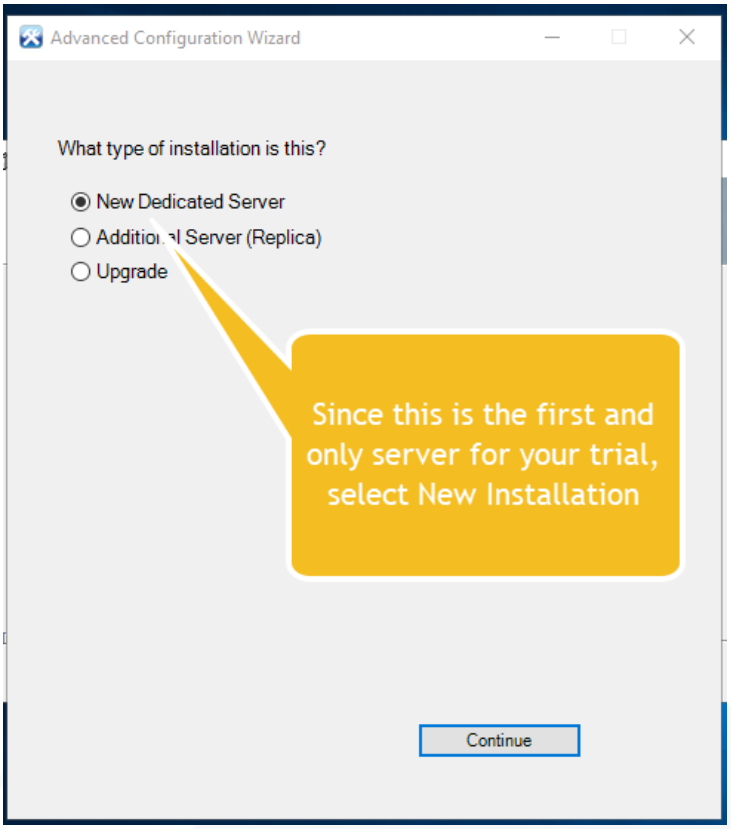


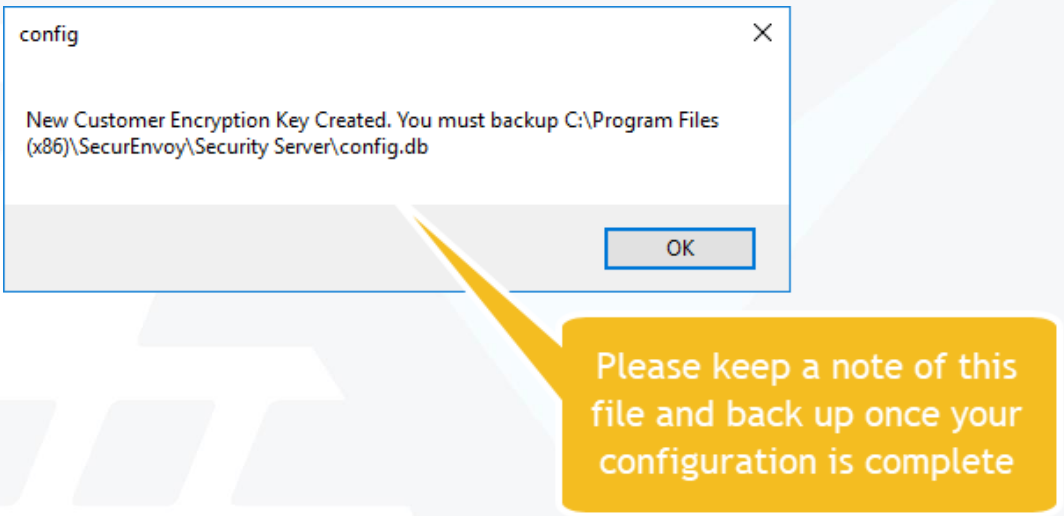
The install can take up to 10 minutes.

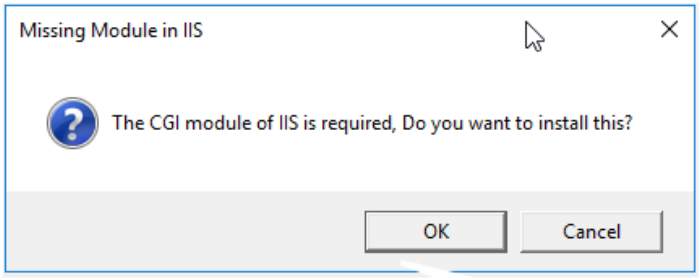

SecurEnvoy Server - InstallShield Wizard
Installing SecurEnvoy Server
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs SecurEnvoy Server. This may take several minutes.
Status:
Extracting information for IIS virtual directories...
The Installer will continue for you
InstallShield
< Back
Next >
Cancel


SecurEnvoy Server - InstallShield Wizard
Installing SecurEnvoy Server
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs SecurEnvoy Server. This may take several minutes.
Status:
Copying new files
Some parts can take a few minutes
InstallShield
< Back
Next >
Cancel

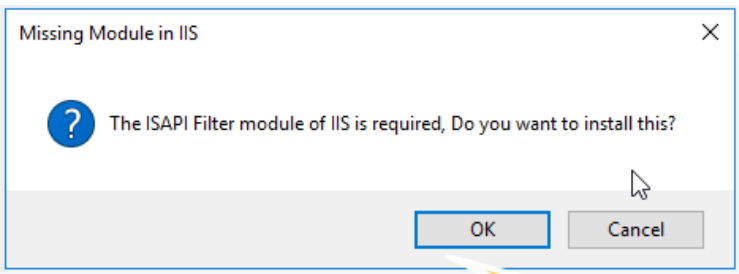

Advanced Configuration Wizard
Optimising Object Code, Please Wait...
The installer will optimize as it goes


Advanced Configuration Wizard
What type of installation is this?
New Dedicated Server
Additio l Server (Replica)
Upgrade
Since this is the first and only server for your trial, select New Installation
Continue

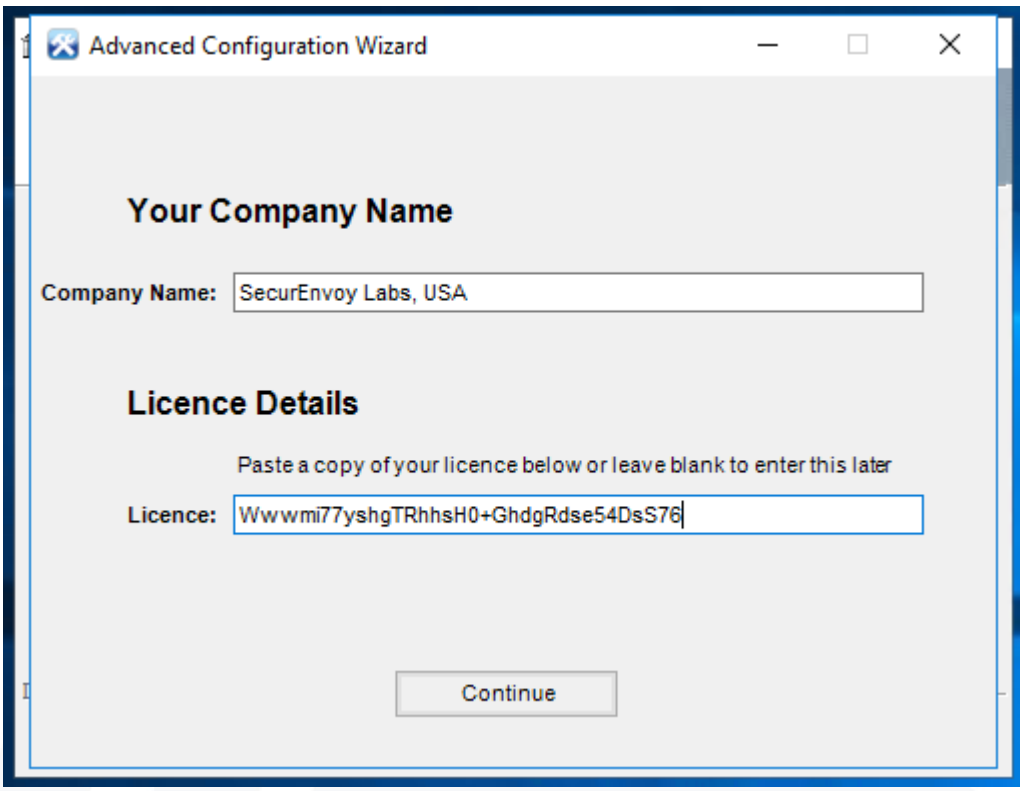

config
New Customer Encryption Key Created. You must backup C:\Program Files (x86)\SecurEnvoy\Security Server\config.db
OK
Please keep a note of this file and back up once your configuration is complete



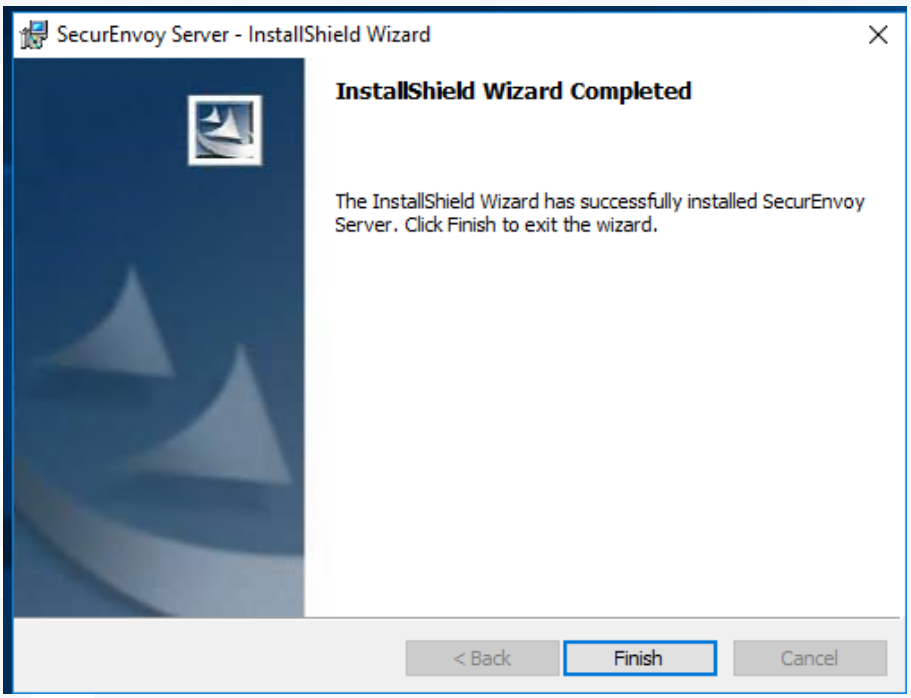
The CGI Module for IIS is a requirement



The ISAPI module for IIS is also a requirement

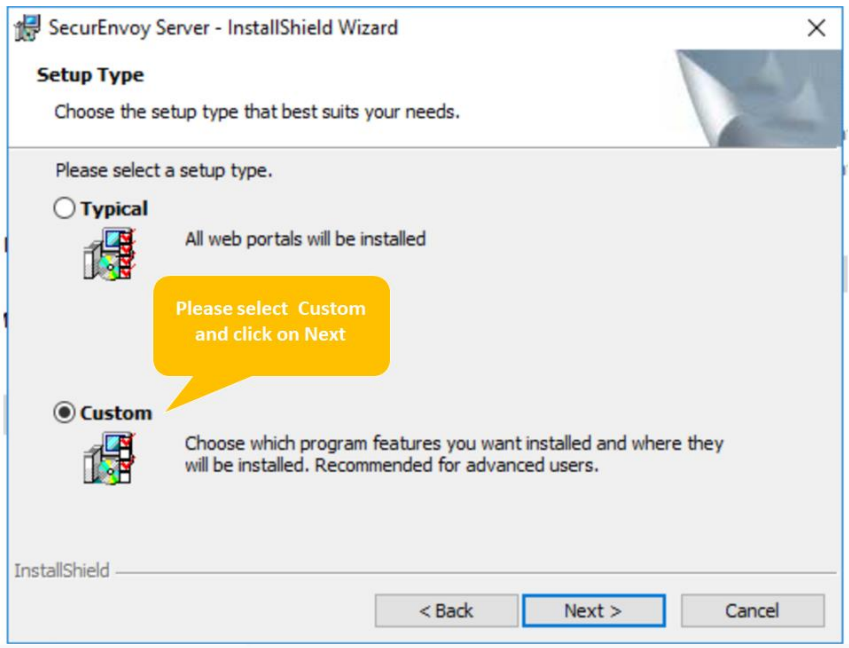


When you downloaded our product, you should have also received your trial license. If you have not, please contact sales or support for assistance.

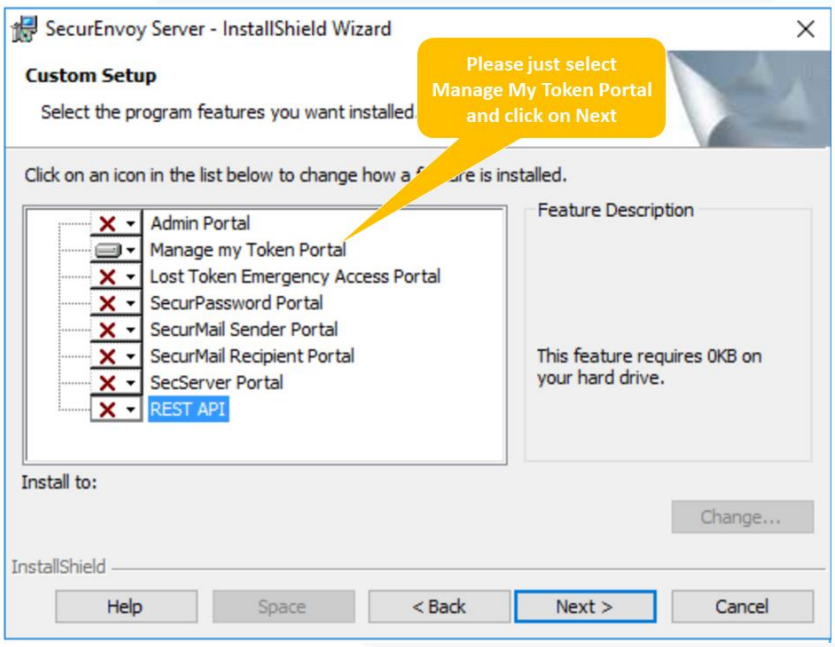


1.6 Customised Installation of SecurEnvoy SecurAccess

Please follow the steps described in Installing & Configuring SecurEnvoy SecurAccess until you get to the "Setup Type" page, then select Custom.



Select the portals as required (please refer to Available SecurEnvoy Web Portals) and click on Next. In the below example only the Manage My Token portal is going to be installed.



Continue to install as per Installing & Configuring SecurEnvoy SecurAccess.

1.7 Configure Your Service Account

For our system to query the Active Directory for usernames and passwords, we need an account with permissions to do that function. 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: –

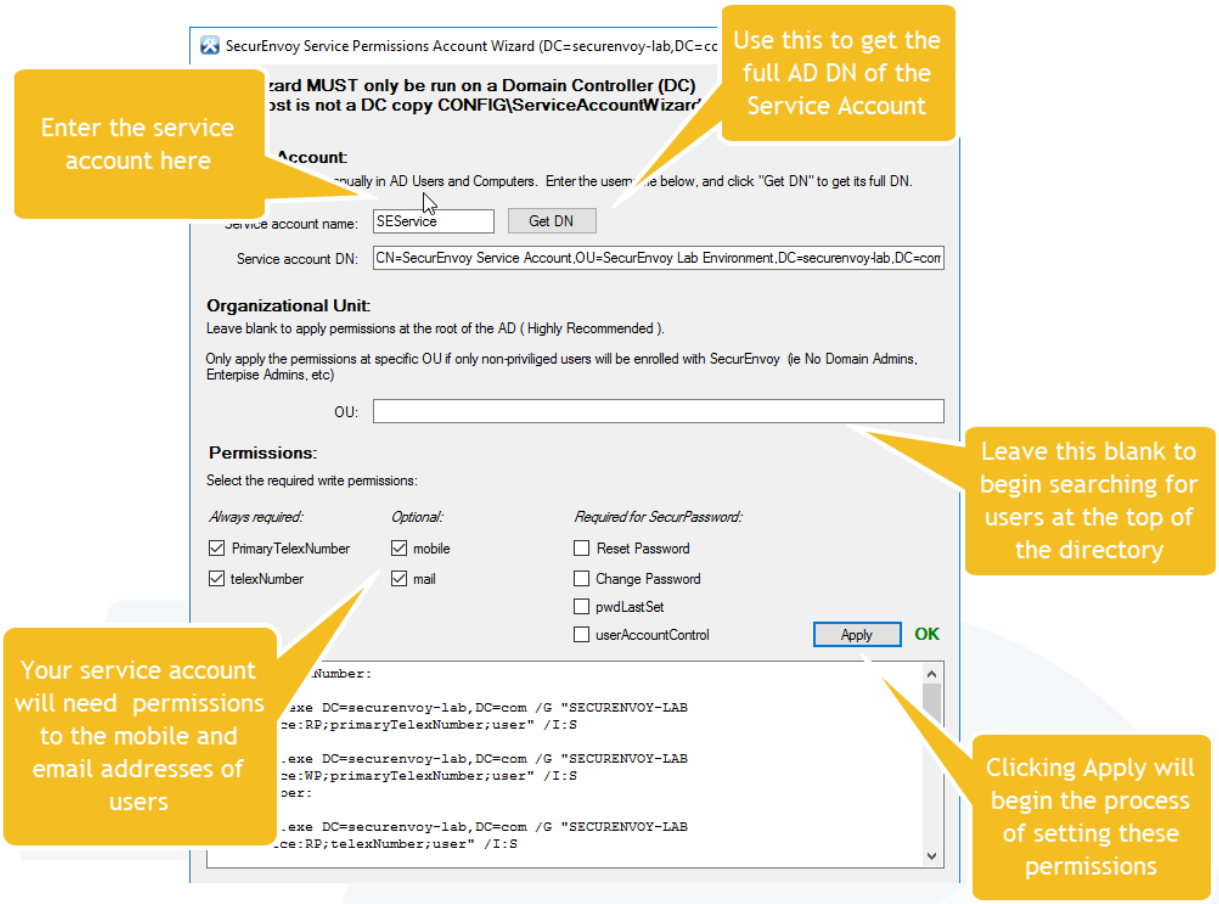
- User Object: "Reset Password"
- User Object: "Change Password"

1.7.1 SecurEnvoy Service Permissions Account Wizard

We strongly recommend that you create a general user account in the Active Directory. Again, this account does not need to be a Domain Administrator, it can be a simple standard user. This process only happens once.
Once you have the user created (in our case, SEService) you should logon to your Domain Controller as a Domain Administrator.

- Navigate to \\Server\c$
- Browse to the location C:\Program Files (x86)\SecurEnvoy\Security Server\Config
- Copy ServiceAccountWizard.exe to your domain controller
- Run ServiceAccountWizard.exe

The below dialog will appear:



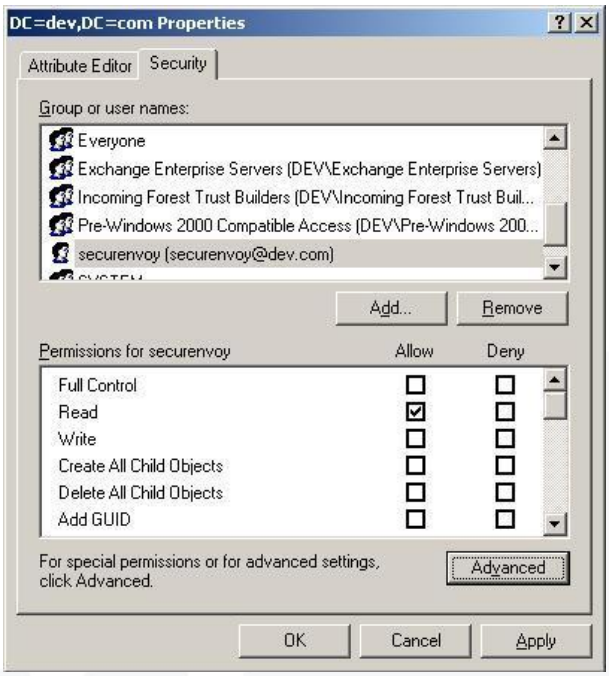
Once you have completed this step, the system is installed and ready for your configuration.

1.7.2 Manually Apply Service Account Permissions with ADSIEDIT

Important

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

For Windows 2008 Server - Example: Admin User "SecurEnvoy" setup with ADSI Edit

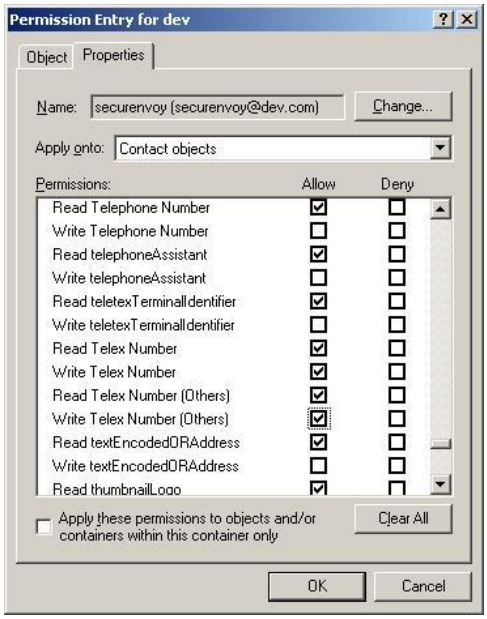


1. Create a user called "securenvoy" in the normal way and set "Password never expires" as this is a system account.

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.

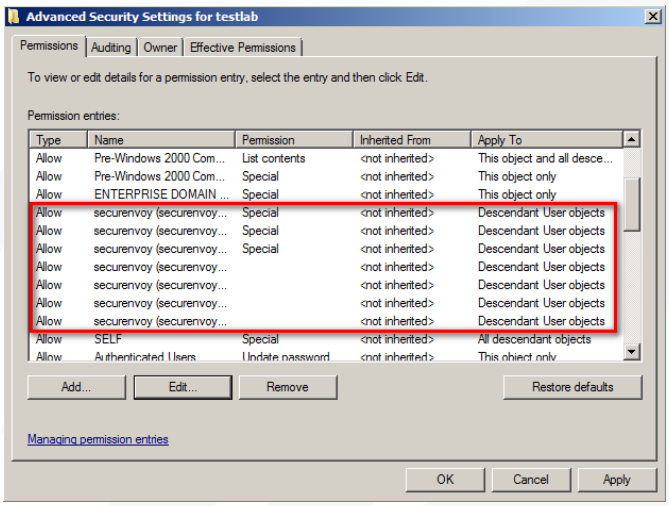
3. Select the "Security" tab and press the "Add" button to add the user securenvoy that you created in the first step.

4. Press the "Advanced" button.

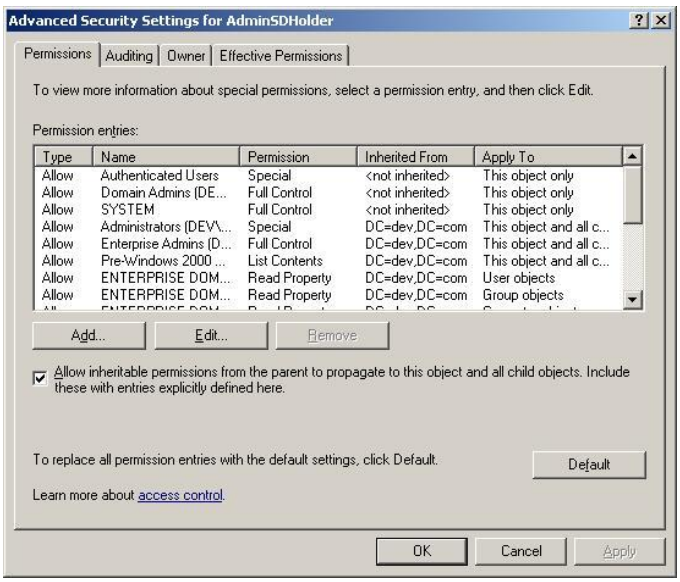


5. Re-select the user in the Permission entries list.
6. Press the “Edit…” button and select the “Properties” tab.
7. In the "Apply onto" field select “Descendant Contact objects”
a. Tick Allow Write Telex Number
b. Tick Allow Write Telex Number (Others)
c. Tick Allow Write Mobile Number
d. Tick Allow 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*).



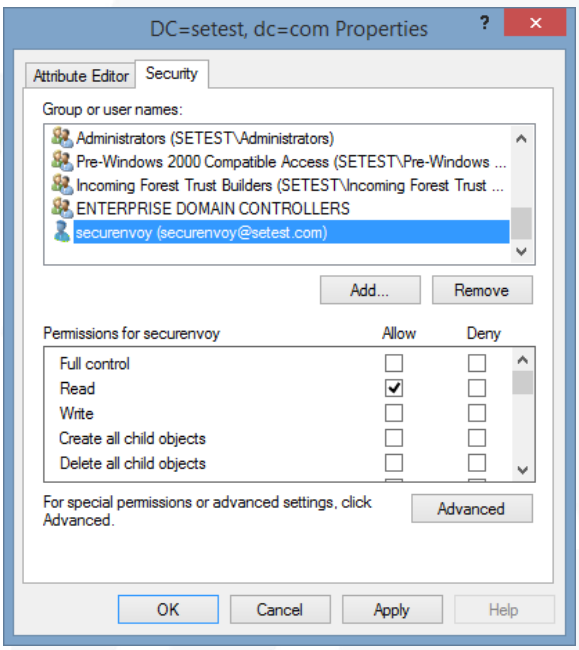
14. Right-click “AdminSDHolder” under the directory CN=system and select “Properties”. Select the check box "Allow inheritable permissions”. Press “OK”. This adds support for users that are members of the following protected groups

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 R2 and 2016 Server

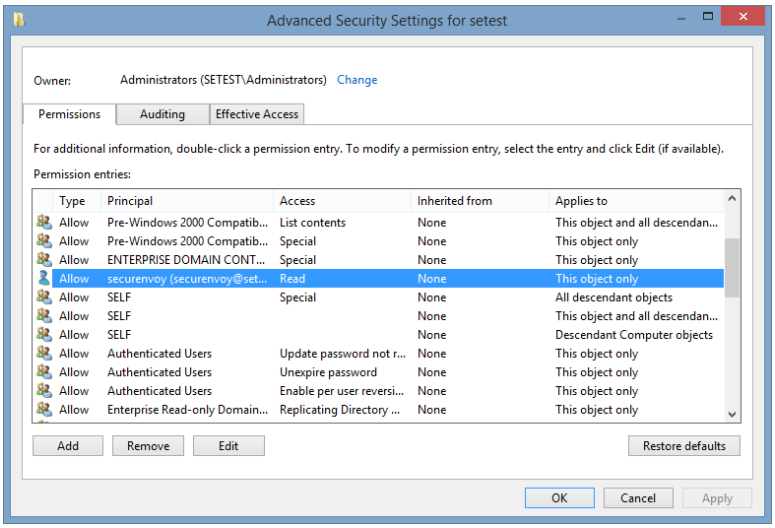


1. Create a user called "securenvoy" in the normal way and set "Password never expires" as this is a system account.

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.

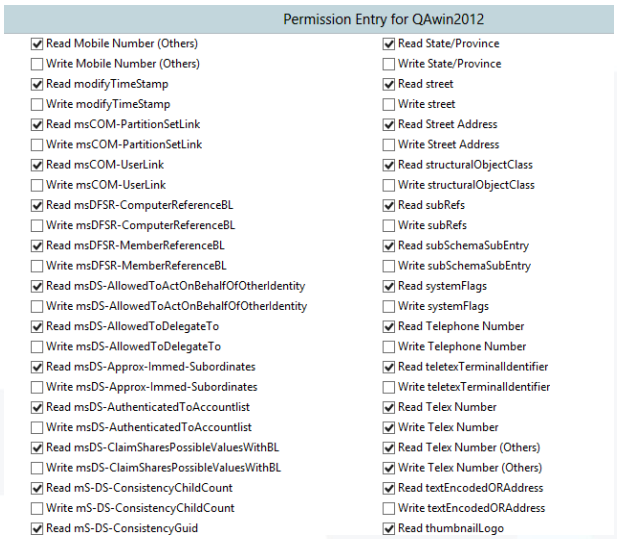
4. Select the “Security” tab and press the "Add" button to add the user securenvoy that you created in the first step.



5. Press the “Advanced” button.

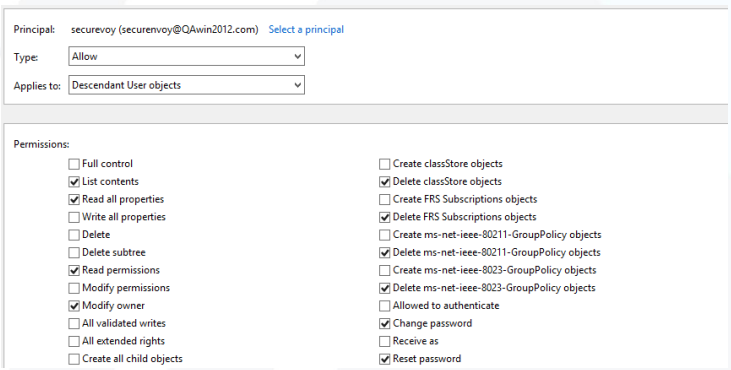
6. Re-select the user in the Permission entries list.

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”



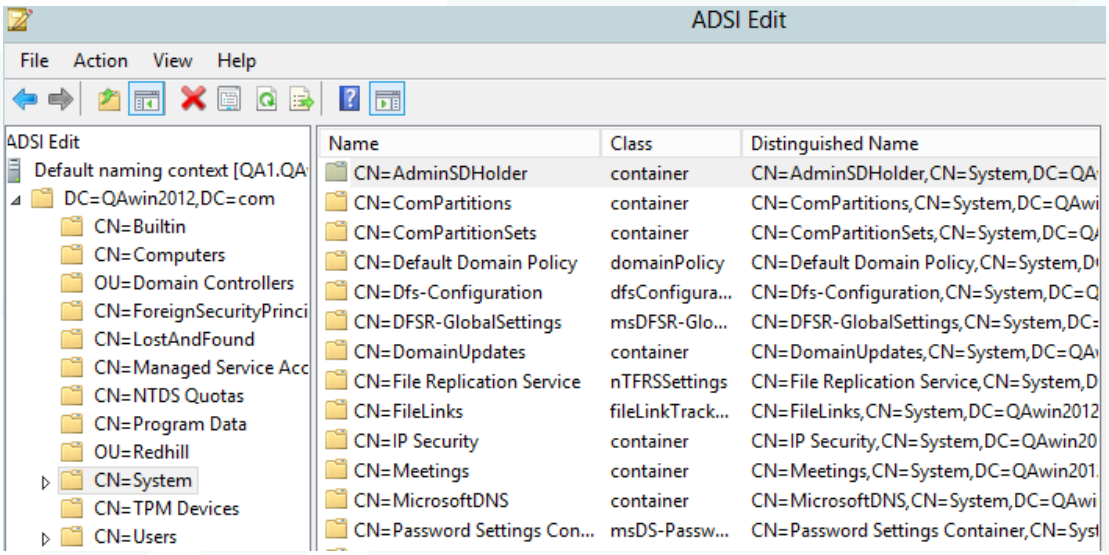
9. At the ‘Advanced Security Settings’, click edit. In the “Applies to” field select “Descendant User objects” Tick Reset Password and Change Password (Both required only for SecurPassword or Windows Login Agent)

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.

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.

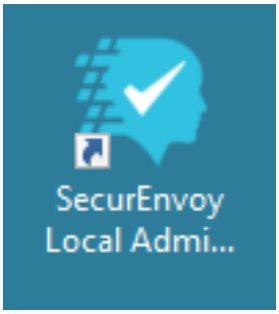
1.8 TCP/UDP Communication Flow (Firewall Ports)

Requirement	Description	TCP/UDP Port	Direction
User Authentication	RADIUS Client Communication (i.e FW, RAS or Application Server with SecurEnvoy Server Agent installed)	UDP/1812	Inbound to SecurAccess Server
LDAP User Lookup	Communication between SecurAccess and LDAP/AD servers	(LDAP) TCP/389 or LDAPS TCP/636	Inbound to LDAP Server from SecurAccess
Syslog	Syslog's pushed to SIEM or Log Collector Solution	UDP/514	Inbound to SIEM Server from SecurAccess
Replication	Replication connection between one or more SecurAccess Servers	TCP/443	Bidirectional
Email Enrolments	SMTP connection to mail relay server	TCP/25	Inbound to SMTP Mail Server
SMS Enrollments and tokens	HTTP connection to public SMS Gateways	TCP/443	Outbound HTTP Access to Public SMS Services
SecurAccess Portals	Client connectivity to Enrol Tokens, Change Passwords or Helpdesk	TCP/443	Inbound to SecurAccess Server
Push Authentication (Outbound)	Push Authentication to Mobile Tokens	TCP/443 Apple = TCP/2195 (prior to Win 16 TCP/443 after)	Outbound to gcm-http.googleapis.com Outbound to gateway.push.apple.com Outbound to a.notify.live.net
Push Authentication (Inbound)	Push Authentication Acceptance from Mobile	TCP/443	Inbound to SecurAccess SECENROL portal (Requires publishing to public Internet via Reverse Proxy)
Push (Apple Certificate)	Required to update apple.p12 cert on a yearly basis	TCP/443	Outbound to www.securenvoy.com

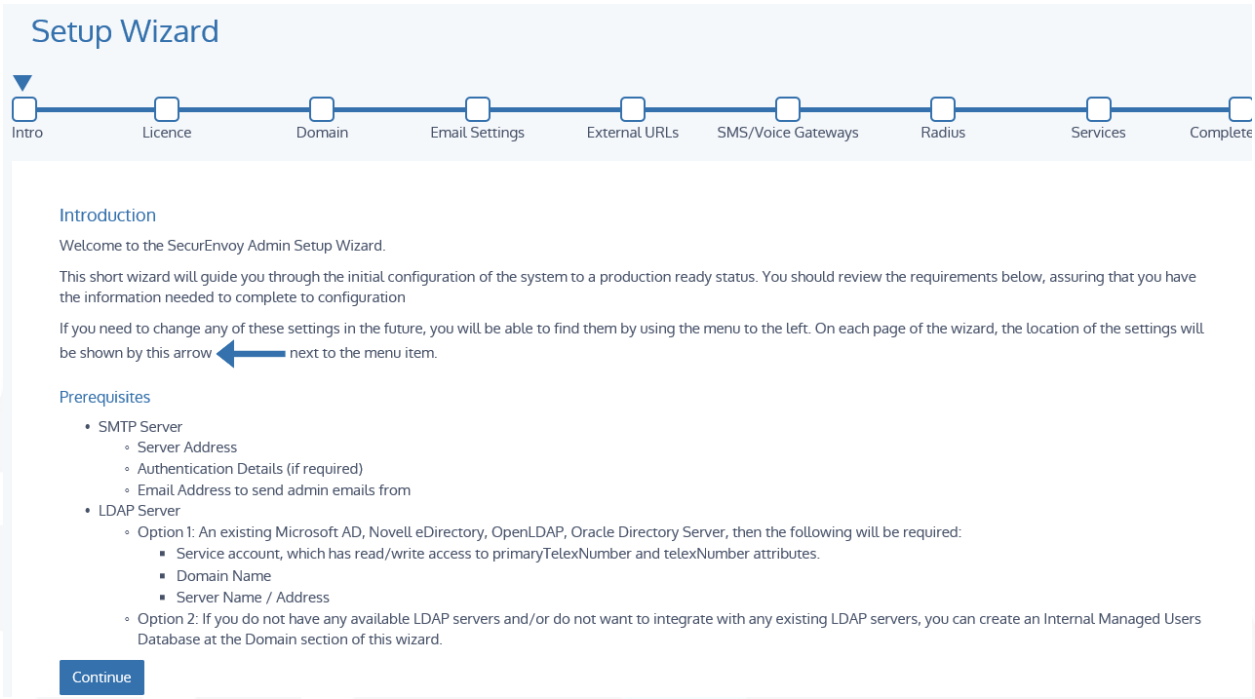
1.9 Configuring SecurEnvoy SecurAccess

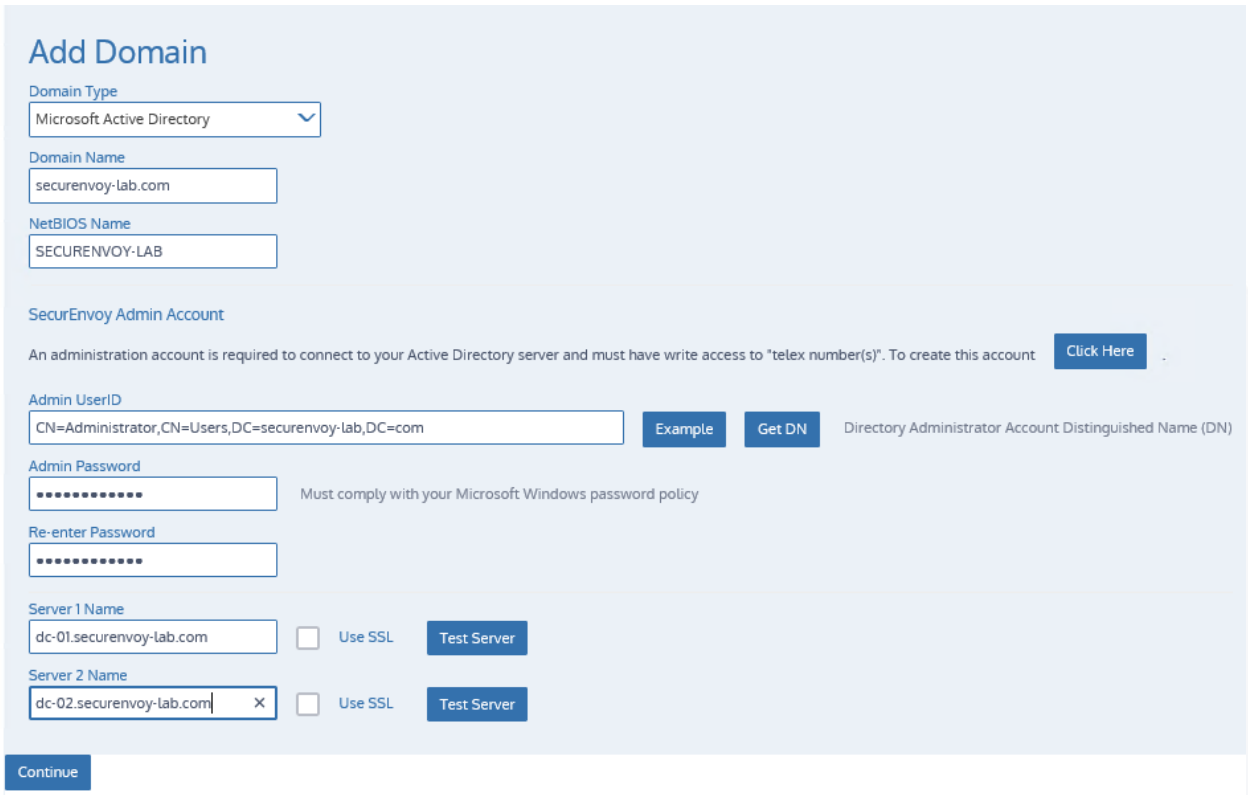
Once the installation has completed, you will need to be logged in to the SecurEnvoy Server a local or domain administrator.

On the Desktop you will find the SecurEnvoy Local Admin.

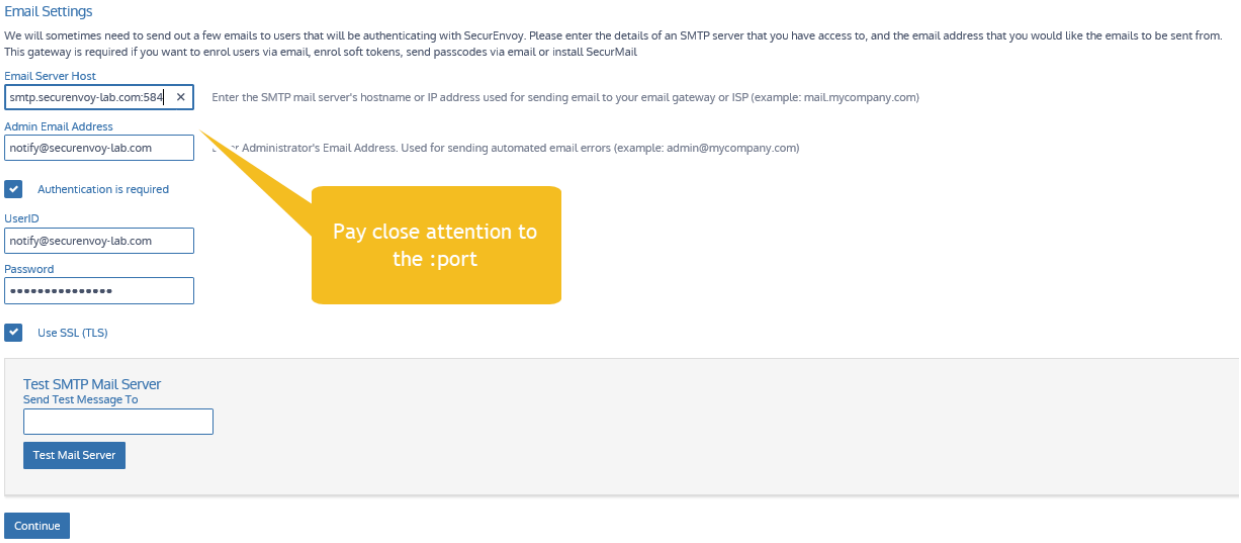


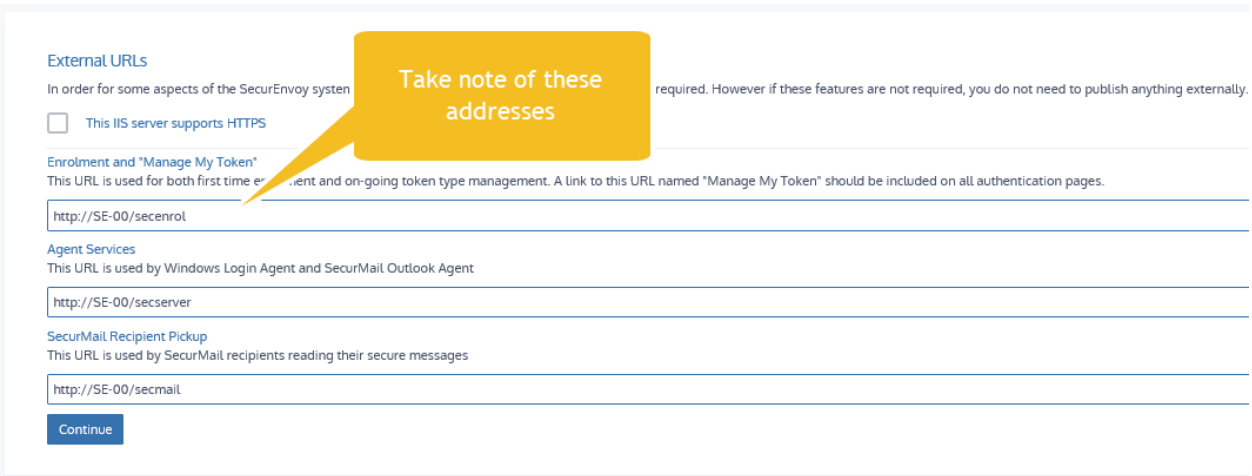
When it is launched for the first time, you will be prompted with a setup wizard for your environment. The set-up wizard is designed to guide you through the configuration of the system.

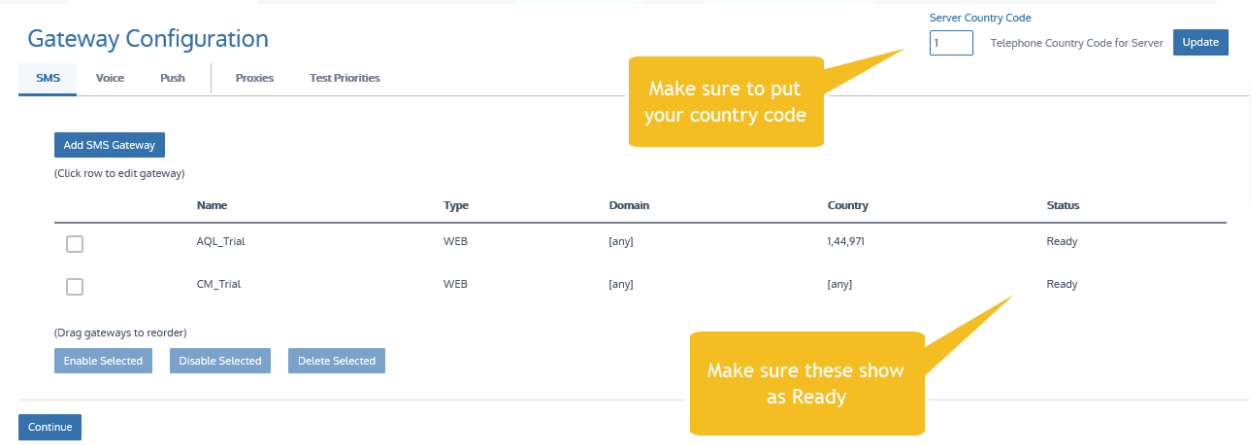


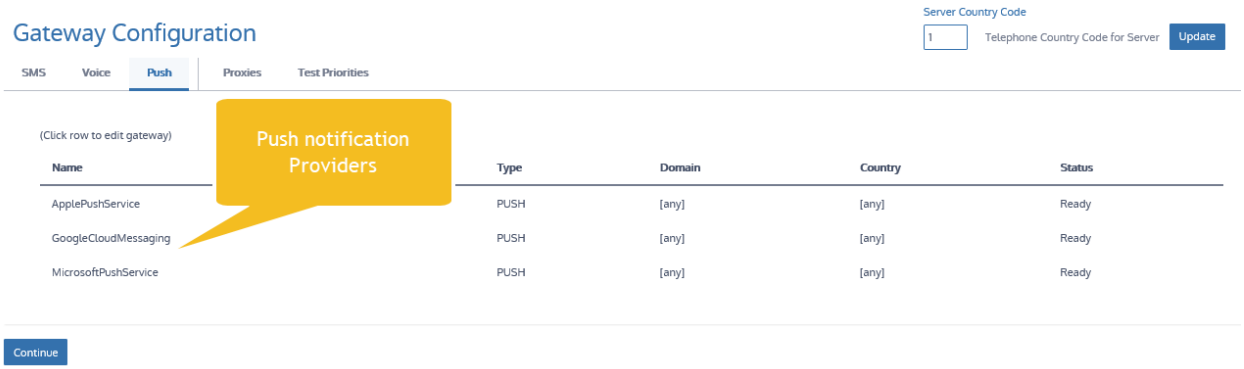


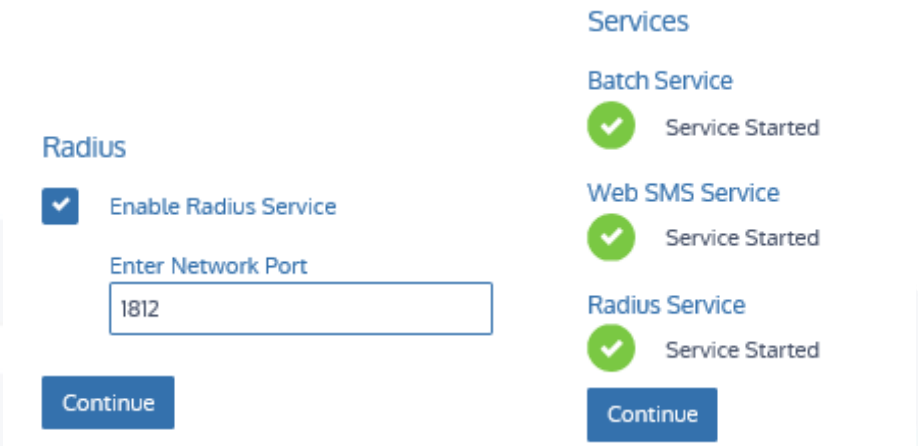
We have filled in some example data to illustrate what should go where. Please note that the servers listed at the bottom are domain controllers.

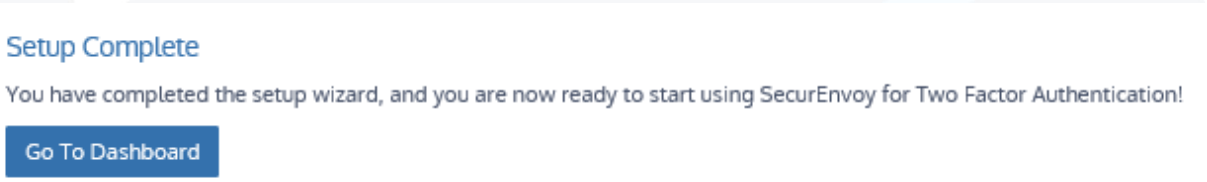

Email Settings
We will sometimes need to send out a few emails to users that will be authenticating with SecurEnvoy. Please enter the details of an SMTP server that you have access to, and the email address that you would like the emails to be sent from. This gateway is required if you want to enrol users via email, enrol soft tokens, send passcodes via email or install SecurMail
Email Server Host
smtp.securenvoy-lab.com:584
Enter the SMTP mail server's hostname or IP address used for sending email to your email gateway or ISP (example: mail.mycompany.com)
Admin Email Address
notify@securenvoy-lab.com
Administrator's Email Address. Used for sending automated email errors (example: admin@mycompany.com)
Authentication is required
UserID
notify@securenvoy-lab.com
Password
Use SSL (TLS)
Pay close attention to the :port
Test SMTP Mail Server
Send Test Message To
Test Mail Server
Continue


External URLs
In order for some aspects of the SecurEnvoy system required. However if these features are not required, you do not need to publish anything externally.
This IIS server supports HTTPS
Take note of these addresses
Enrolment and "Manage My Token"
This URL is used for both first time enrolment and on-going token type management. A link to this URL named "Manage My Token" should be included on all authentication pages.
http://SE-00/secenrol
Agent Services
This URL is used by Windows Login Agent and SecurMail Outlook Agent
http://SE-00/secserver
SecurMail Recipient Pickup
This URL is used by SecurMail recipients reading their secure messages
http://SE-00/secmail
Continue


Gateway Configuration
Server Country Code
1
Telephone Country Code for Server
Update
SMS
Voice
Push
Proxies
Test Priorities
Make sure to put your country code
Add SMS Gateway
(Click row to edit gateway)
Name
Type
Domain
Country
Status
AQL_Trial
WEB
[any]
1,44,971
Ready
CM_Trial
WEB
[any]
[any]
Ready
(Drag gateways to reorder)
Enable Selected
Disable Selected
Delete Selected
Make sure these show as Ready
Continue

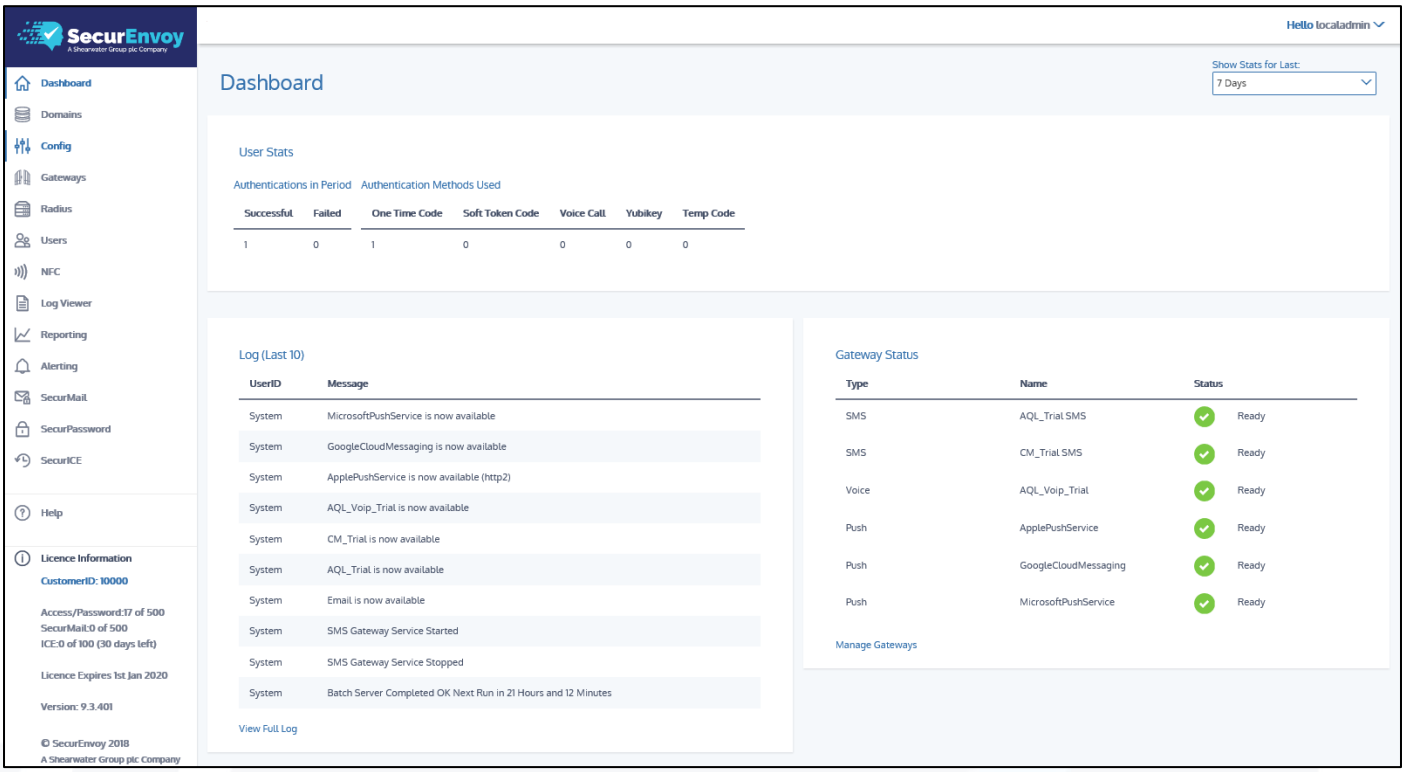

Gateway Configuration
Server Country Code
1
Telephone Country Code for Server
Update
SMS
Voice
Push
Proxies
Test Priorities
(Click row to edit gateway)
Push notification Providers
Name
Type
Domain
Country
Status
ApplePushService
PUSH
[any]
[any]
Ready
GoogleCloudMessaging
PUSH
[any]
[any]
Ready
MicrosoftPushService
PUSH
[any]
[any]
Ready
Continue


Radius
Enable Radius Service
Enter Network Port
1812
Continue
Services
Batch Service
Service Started
Web SMS Service
Service Started
Radius Service
Service Started
Continue


Setup Complete
You have completed the setup wizard, and you are now ready to start using SecurEnvoy for Two Factor Authentication!
Go To Dashboard

1.9.1 The Main Dashboard

The main dashboard is full of useful information, logs and recent transaction details. Configuration items on the left navigation make it easy to find the settings you are looking for.



1.10 Configure your RADIUS Client

Now that you have completed the setup and configuration of the SecurEnvoy Security Server, if you wish to use SecurAccess or SecurIce you will need to configure and allow other devices to work with it. That process begins with creating security entries to allow devices to communicate. These are called RADIUS Clients.

A RADIUS Client would be something like your VPN Server, Citrix NetScaler, Check Point Firewall VPN, etc. When you are configuring a RADIUS Client, you'll need to do two things.

- IP Address of your RADIUS Client
- A Shared Secret (ASCII 127 Printable Characters – With some exclusions)

A Shared Secret is a password or passphrase that these two devices will use to validate each other. For the trial, you can keep these simple, but for a production environment they should be complex. It's also important to know that you can have more than one RADIUS Client and that the Shared Secret can be different for each RADIUS Client.

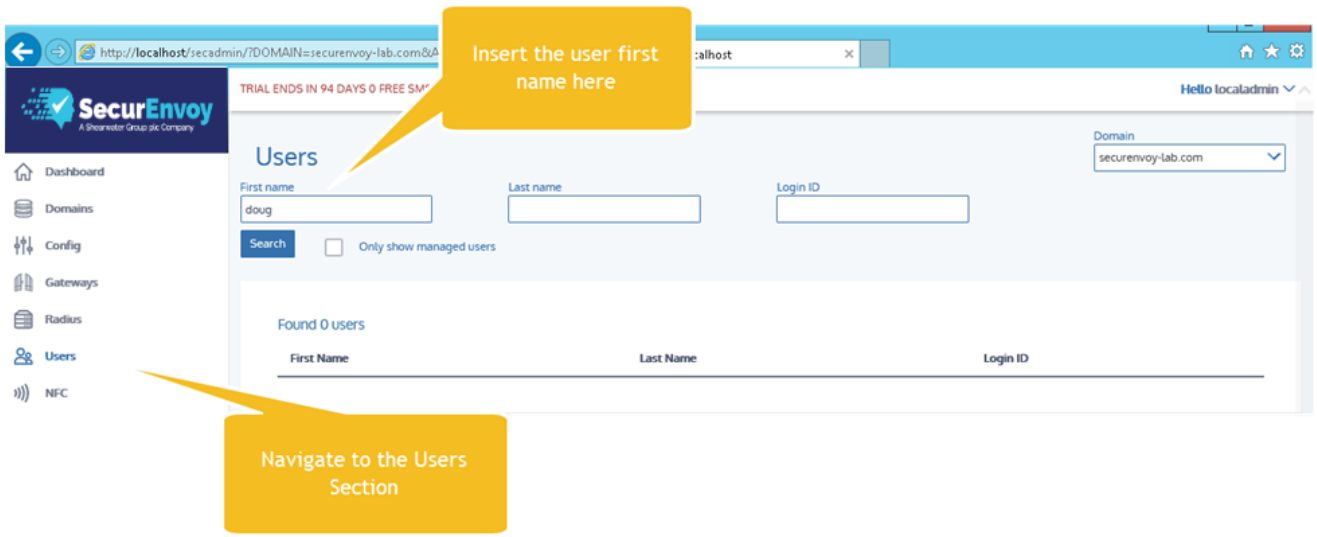
Code	Char	Code	Char	Code	Char	Code	Char	Code	Char	Code	Char
32	[space]	48	0	64	@	80	P	96	`	112	p
33	!	49	1	65	A	81	Q	97	a	113	q
34	"	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v
39	'	55	7	71	G	87	W	103	g	119	w
40	(	56	8	72	H	88	X	104	h	120	x
41	)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[	107	k	123	{
44	,	60	<	76	L	92	\	108	l	124	|
45	-	61	=	77	M	93	]	109	m	125	}
46	.	62	>	78	N	94	^	110	n	126	~
47	/	63	?	79	O	95	_	111	o	127	[backspace]

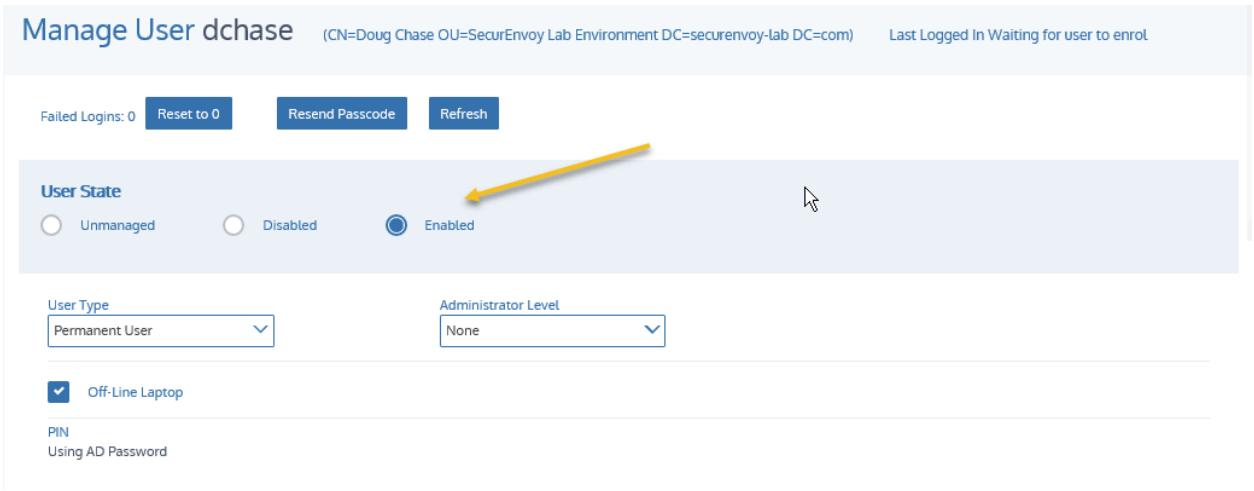
Characters Highlighted above should be avoided in RADIUS Shared Secret

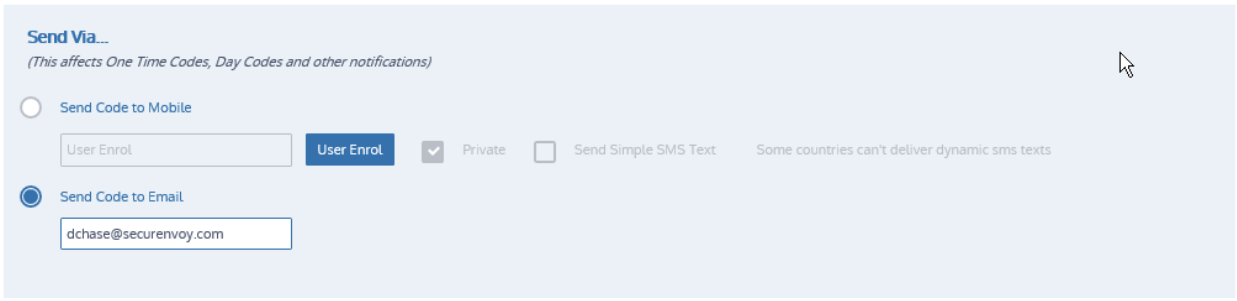
Remember that you will need to put the same shared secret on the other side of the connection.

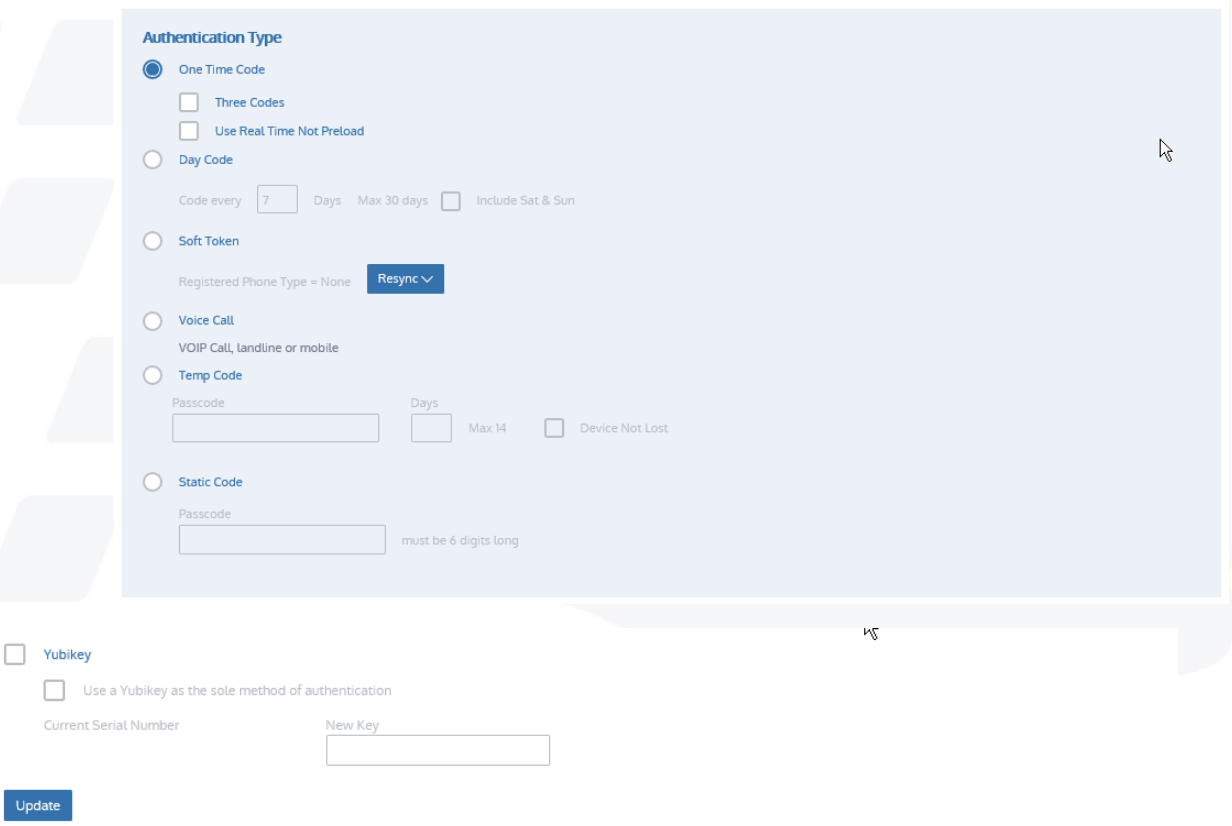
1.11 Registering your First Device

SecurEnvoy Soft Tokens need to be registered to the system to work. To do this, navigate to the User Tab. It will be important to note a few things here, in this configuration for the trial we are searching the entire directory and that means your list of users may be long.

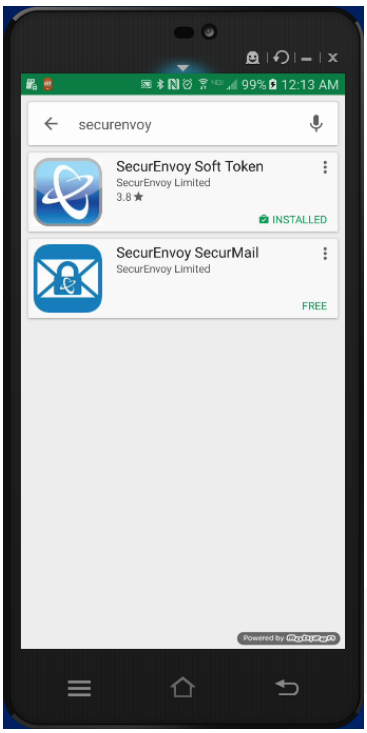



Manage User dchase
(CN=Doug Chase OU=SecurEnvoy Lab Environment DC=securenvoy-lab DC=com)
Last Logged In Waiting for user to enrol
Failed Logins: 0
Reset to 0
Resend Passcode
Refresh
User State
Unmanaged
Disabled
Enabled
User Type
Permanent User
Administrator Level
None
Off-Line Laptop
PIN
Using AD Password


Send Via...
(This affects One Time Codes, Day Codes and other notifications)
Send Code to Mobile
User Enrol
User Enrol
Private
Send Simple SMS Text
Some countries can't deliver dynamic sms texts
Send Code to Email
dchase@securenvoy.com


Authentication Type
One Time Code
Three Codes
Use Real Time Not Preload
Day Code
Code every
7
Days
Max 30 days
Include Sat & Sun
Soft Token
Registered Phone Type = None
Resync
Voice Call
VOIP Call, landline or mobile
Temp Code
Passcode
Days
Max 14
Device Not Lost
Static Code
Passcode
must be 6 digits long
Yubikey
Use a Yubikey as the sole method of authentication
Current Serial Number
New Key
Update

Once you click Update, the system will use the email configuration you specified earlier to deliver a message to the user. This email will contain the URL for enrolment as well as a one-time code that they will need to complete their authentication



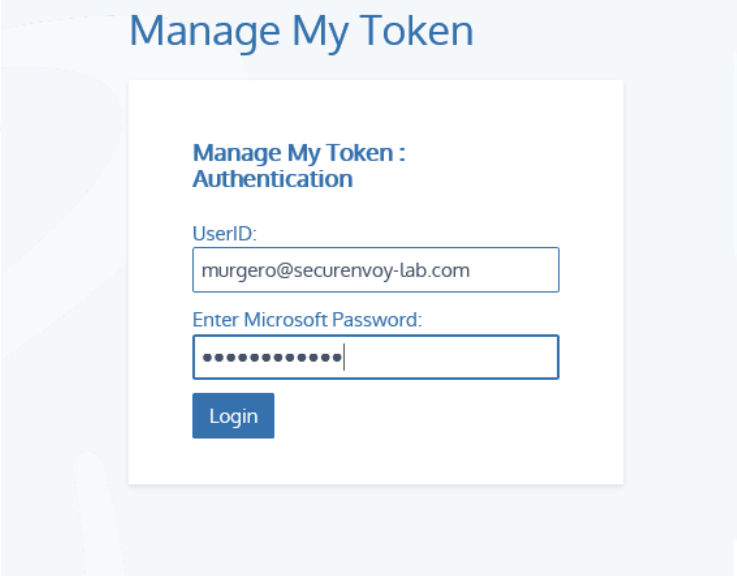
From the user side, you will need to load the SecurEnvoy Soft Token Application on your smart phone device.

SecurEnvoy has applications in all the major markets, simply search for SecurEnvoy.

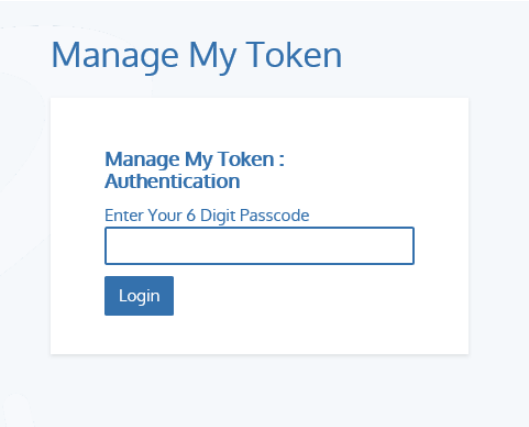
When you locate the SecurEnvoy Soft Token Application, install to your smart phone device. You will receive several prompts that need to be accepted.

Once you have completed the installation of the SecurEnvoy Soft Token Application from the market, you will need to get ready for enrolment and have probably received an enrolment email by now.

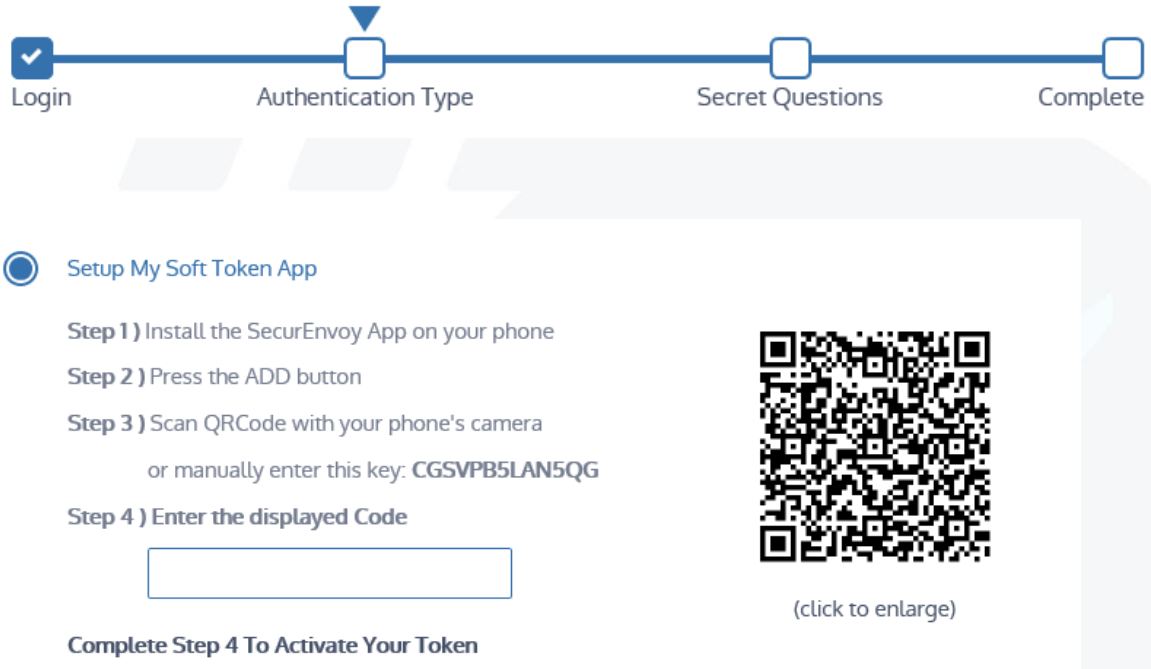
Navigate your browser to the following URL: http://<yourserverFQDN>/secenrol. You should reference the IIS URLs page from the SecurEnvoy Config → External URLs page in the admin console on your server to get this address.



You will logon to this site with your Microsoft Active Directory Credentials and will be prompted for the one-time code that you received in your enrolment email to setup your token.



You'll setup your SecurEnvoy SecurAccess Soft Token using the QR Code shown on the page. The QR Code contains the URL that the SecurEnvoy SecurAccess server will use to communicate with your Soft Token.



Once your token is activated, you're ready to go. You will now need to configure your VPN, Citrix NetScaler, Check Point Firewall or other service for RADIUS authentication.

SecurEnvoy SecurAccess works with many different vendors and is a the most flexible two-factor authentication solution on the market today.

1.12 Upgrading

Upgrade Path

It is possible to upgrade directly to SecurAccess 9.3.x from version 7 or 8 but it is recommended to upgrade prior releases to version 7.3.501 using the following steps before finally upgrading to version 9.3.x

Ver 5.0 → Ver 6.0 → Ver 7.3.501 → Ver 9.3.x

If a software version prior to version 9 is required to deliver a step upgrade, please contact support@securenvoy.com for access to previous software versions or download from our FTP site.

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
- gateway.ini (optional)

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 and 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

Important

Please ensure that all SecurEnvoy web portals are closed in advance of upgrading the software so that files which need to be replaced are not locked.

.

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.

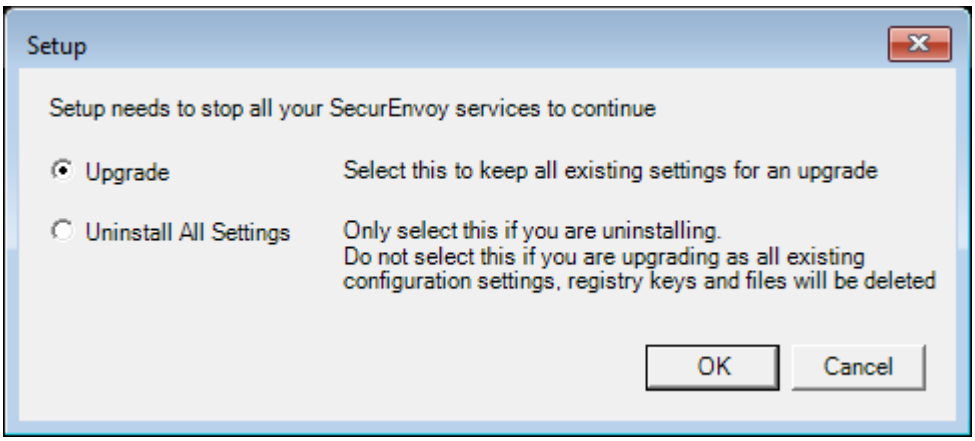
Note

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

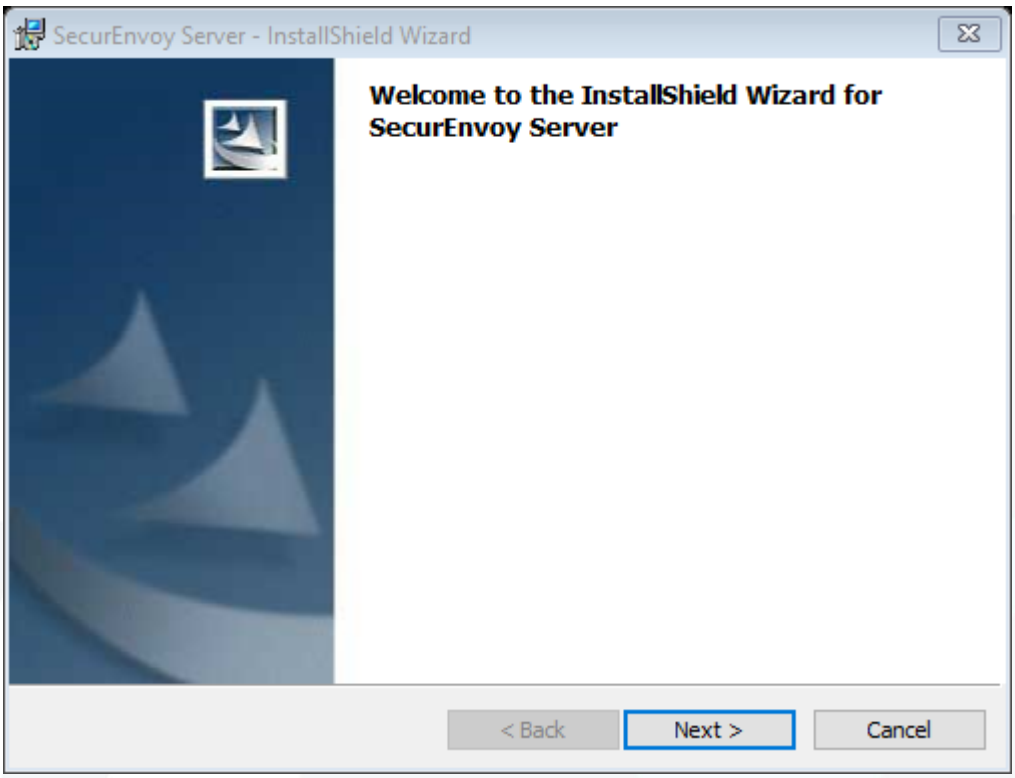
When the setup is executing, it will check to see if Microsoft .Net Framework 4.5 is installed.

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

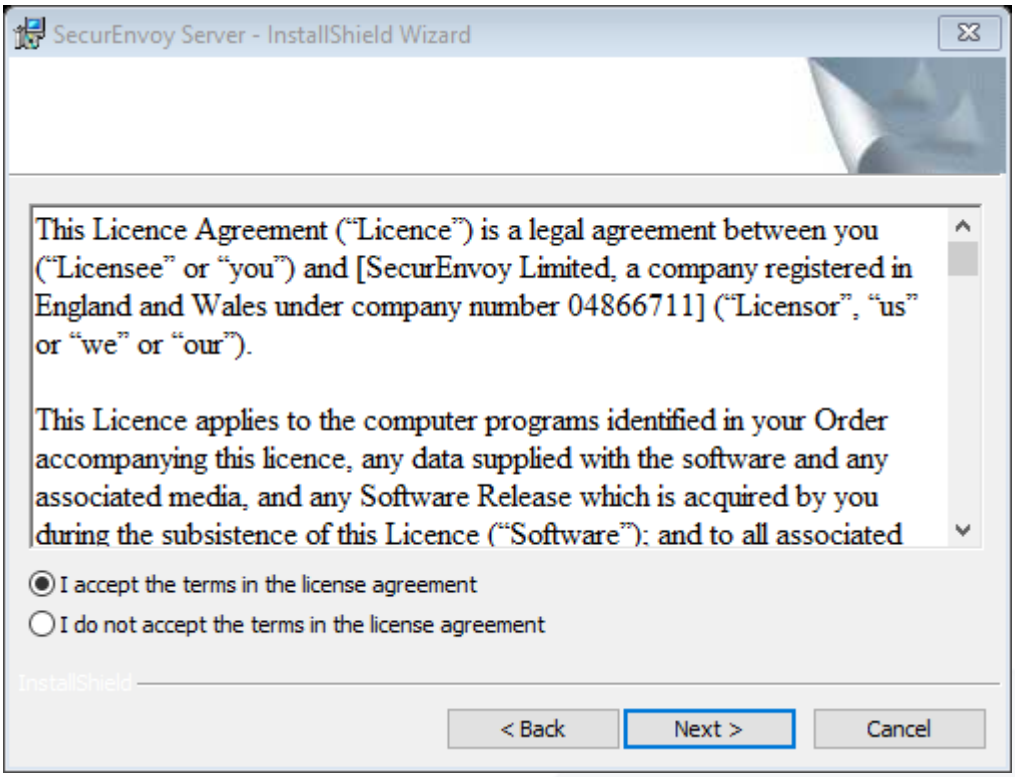
Select Upgrade and click on OK



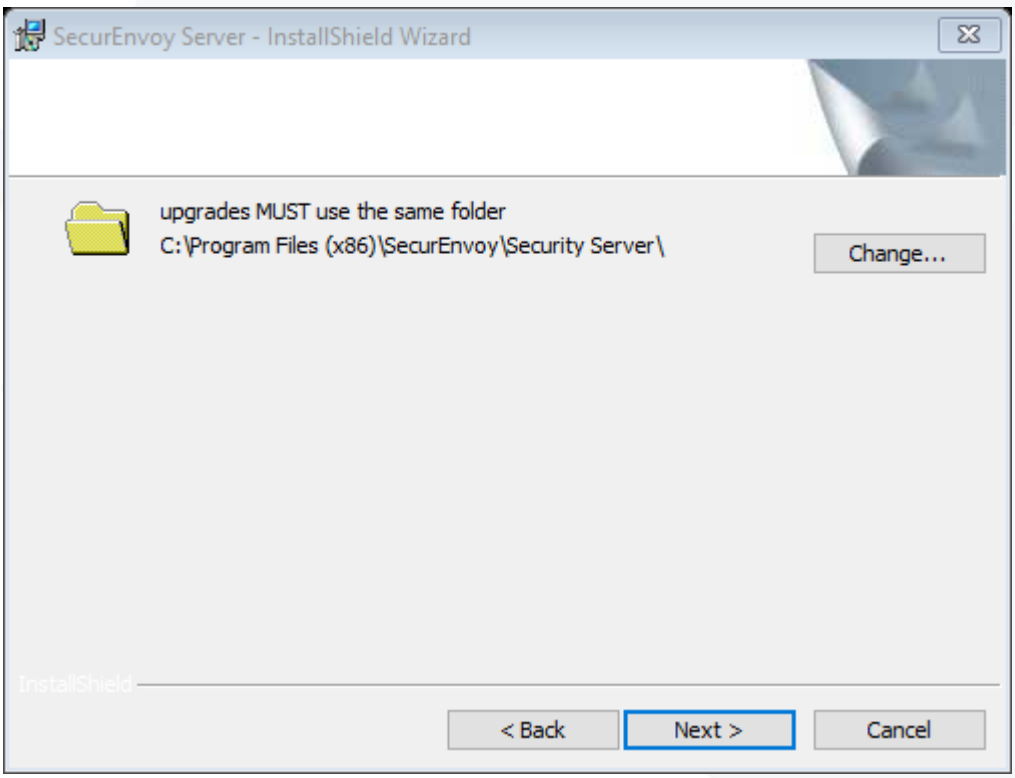
Click on Next



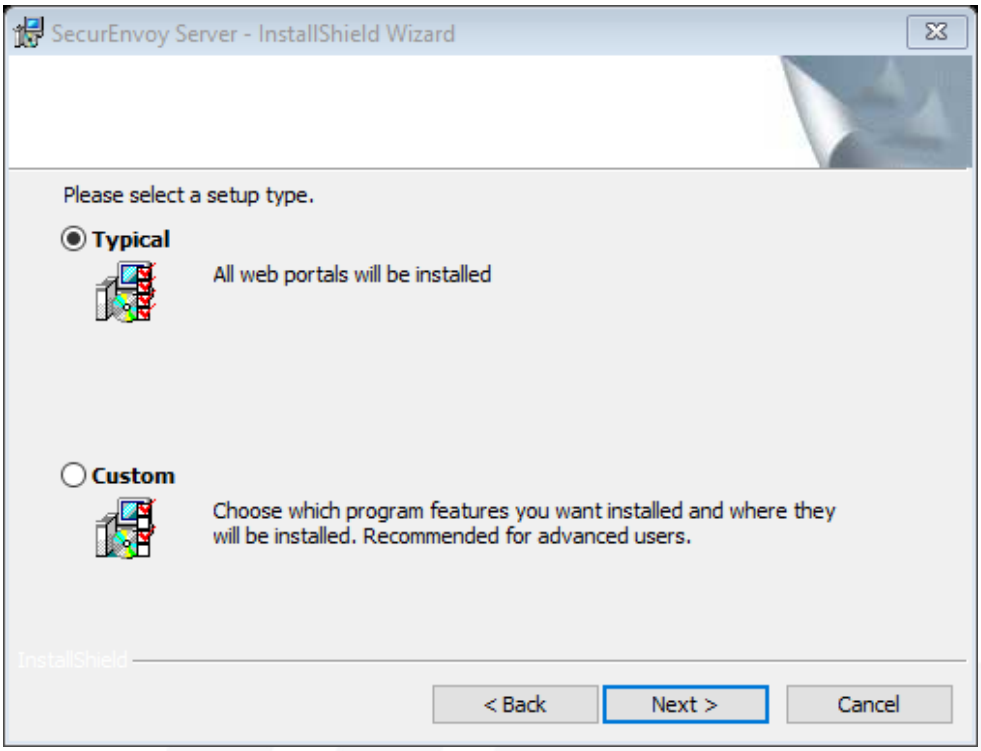
Now we'll accept the licence agreement.



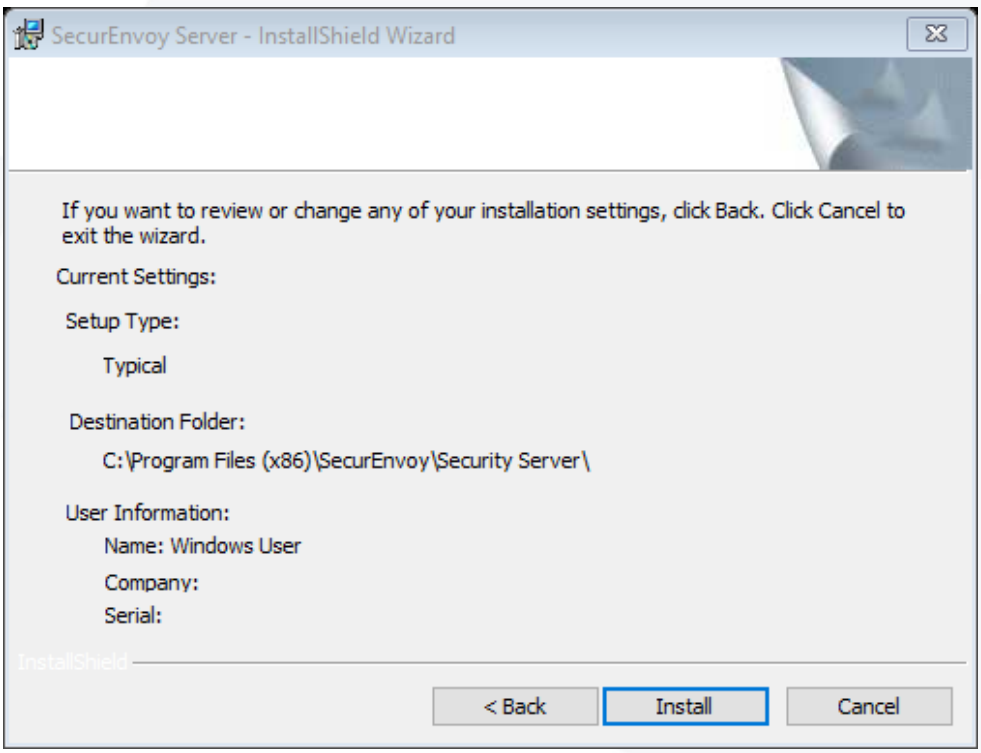
Upgrades must keep the same folder as the previous version.



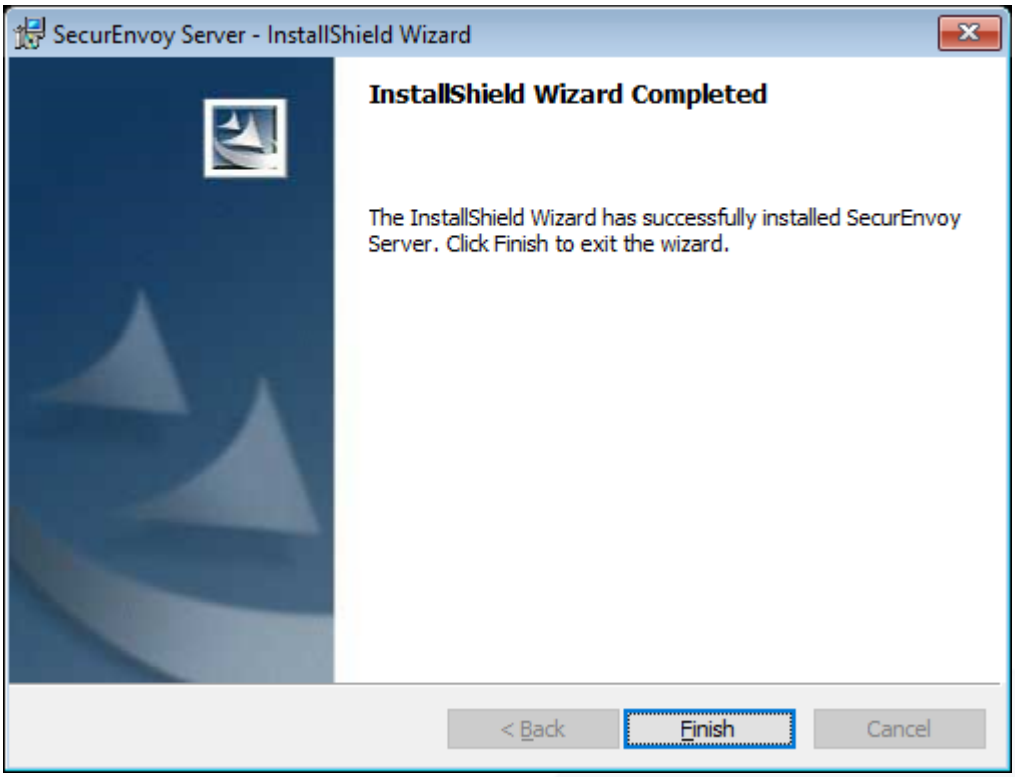
Select a Typical Installation



Click on Install



Please wait for the Optimising Object Code to complete and click on Finish.



Please now launch the SecurEnvoy SecurAccess Admin Console. The Initial Setup Wizard will run, pre-populated with the settings from the previous installation. You have the option to change these settings or accept the existing ones as required.

1.13 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 fully operational, the original can then be decommissioned.

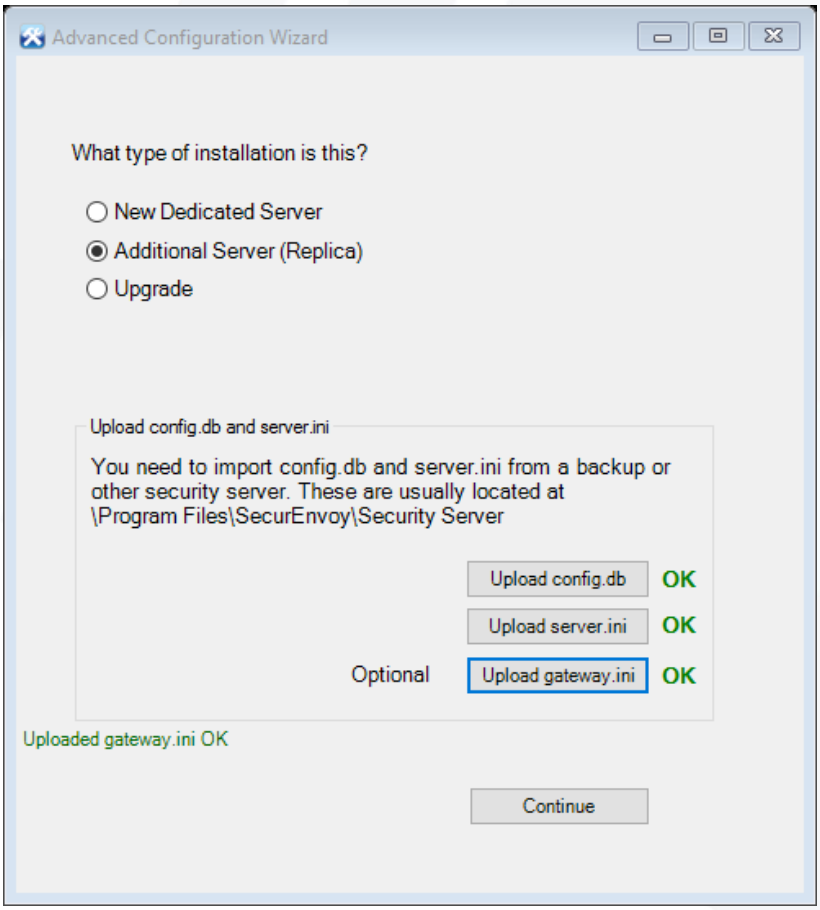
Please note that Radius clients, IIS and Windows login agents will require updating so that they communicate with the correct SecurEnvoy server.

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 Server

Run setup.exe and follow the steps outlined in the “Installing & Configuring SecurEnvoy SecurAccess” section earlier in this guide.

The Advanced Configuration Wizard will prompt you to choose an installation type, please select Additional Server (Replica). 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 C:\Program Files(x86)\SecurEnvoy\Security Server. 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

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.

1.14 Support for Your Trial

We're happy to help you get things setup and running. If you have any questions or need help with your trial, please reach out to us – we would be happy to help.

1.15 What's Next

Now that you have the SecurEnvoy SecurAccess Two-Factor Authentication configuration completed, you will need to refer to the integration guide for the product that you're working with.

- Citrix RADIUS Integration
- Palo Alto VPN Firewall Integration
- Cisco VPN Integration

And many more. Please refer to our web site for additional product integration.

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com