

www.securenvoy.com

Installation & Configuration Guide v9.4.502

Authenticating Users Using SecurAccess Server by SecurEnvoy



SecurEnvoy SecurAccess Security Server Installation & Configuration Guide

Table of Contents

DISCLAIMER	3
LEGAL	3
GETTING STARTED	4
Things You Will Need	4
Authentication Processing Topology	4
System Installation	5
Installation of Microsoft IIS Web Service	6
INSTALLING & CONFIGURING SECURENVOY SECURACCESS	11
Downloading our Software	11
Installing SecurAccess	12
Welcome to the System Installer	12
License Agreement	13
Installation Path	13
Select Setup Type	
CONFIGURE YOUR SERVICE ACCOUNT	17
SECURENVOY SERVICE PERMISSIONS ACCOUNT WIZARD	17
CONFIGURING SECURENVOY SECURACCESS	19
SECURENVOY SECURACCESS DASHBOARD	24
Dashboard Components	24
CONFIGURE RADIUS CLIENT CONNECTIONS	26
REGISTERING YOUR FIRST DEVICE	28
Upgrading Your Server	31
Prior to Upgrade	31
Post Upgrade Tasks	
INSTALLING AN ADDITIONAL SECURENVOY SERVER.	
SUPPORT	
APPENDIX – SETTING SERVICE ACCOUNT PERMISSIONS MANUALLY	
APPENDIX – TCP / UDP COMMUNICATIONS / FIREWALL PORTS	



Disclaimer

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

Legal

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.



Getting Started

The purpose of this document is to outline the steps for the installation and validation of the SecurEnvoy Security Server Twofactor 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.

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 Microsoft Windows 2012 R2, 2016 or 2019 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/en-us/support#id4

- 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.

Microsoft's standard practices for hardware requirements are sufficient for the implementation.

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.



System Installation

The Microsoft Windows 2019 Server that we used in our lab to document this installation process for the SecurAccess Security Server Product has the following technical specifications.





Installation of Microsoft IIS Web Service

Microsoft IIS Web Services is a required Windows feature for our product. This will allow you to use either http or https (with a required SSL Certificate) as appropriate for your deployment, both internally and externally.

Using Server Manager, Add Roles and Features Wizard;

🚡 Server Manager				- 6	×
Server Ma	anager • Local Ser	rer 🔹 e 🖡 Manage	Tools	View	Help
Dashboard	PROPERTIES For LAB-SE-01	🚡 Add Roles and Features Wizard - 🗆 🗙		TASKS	•
Local Server All Servers File and Storage Services ▷	Computer name Workgroup	Select installation type	/s Update	:	
	Windows Defender Firewall Remote management Remote Desktop NIC Teaming Ethernet Operating system version Hardware information	Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD). Server Roles Features Confirmation Results Select the installation Install required role services for actual machine-based or session-based desktop deployment Select the Role-Based Installation Type option.	a) 0GHz		
	EVENTS All events 0 total			TASKS	•
	Server Name ID Severity	< Previous Next > Install Cancel			~

📥 Server Manager					- 0 ×
Server Ma	anager • Local Ser	ver	• ©	Manage	Tools View Help
Dashboard	For LAB-SE-01	📥 Add Roles and Features Wizard	-		TASKS 👻
Local Server All Servers File and Storage Services	Computer name Workgroup	Select destination	Server	INATION SERVER LAB-SE-01	rs Update
■ File and Storage Services ▷	EVENITE	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 LB-SE-01 192.168.200.123 Microsoft Windows Server 2019 Standar Computer(s) found This page shows servers that are running Windows Server 2012 or a newer release of Win and that have been added by using the Add Servers command in Server Manager. Offlin newly-added servers from which data collection is still incomplete are not shown. Previous Next > Install	ndows Server,	e) DGHz TASKS V















Server Manager	nager ▸ Local Ser	ver	- G X
Dashboard Local Server All Servers File and Storage Services	PROPERTIES For LAB-SE-01 Computer name Workgroup	Add Roles and Features Wizard	The installation of Microsoft Web Services will continue and may take a minute. DESTIMATION SERVER LAB-SE-DT
	Windows Defender Firewall Remote management Remote Desktop NIC Teaming Ethernet Operating system version Hardware information	Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results Results Role Server Role (IIS) Role Services Confirmation Results Results Role Server Role (IIS) Role Services Confirmation Results Results Role Server Role (IIS) Role Services Confirmation Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results Results	onsole atures ment wsing
	EVENTS All events 0 total <i>Filter</i> Server Name ID Severity	¹ Page again by clicking h Export configuration settings	stics





Server M	anager 🔸 Local Ser	ver	🕶 🕄 🖡 Manage Tools View Help
Dashboard	PROPERTIES For LAB-SE-01	add Roles and Features Wizard	– 🗆 X TASKS 🔻
Local Server All Servers File and Storage Services ▷	Computer name Workgroup	Installation progress	DESTINATION SERVER LAB-SE-01 IS Update
IIS	Windows Defender Firewall Remote Desktop NIC Teaming Ethernet Operating system version Hardware information	Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results View installation progress Installation succeeded on LAB-S Web Server (IIS) Management Tools IIS Management Console Web Server Common HTTP Features Default Document Directory Browsing HTTP Errors Static Content	SE-01. DGHz Once the installation has completed, you should close the Add Roles and Features Wizard.
	EVENTS All events 0 total Filter Server Name ID Severit	Export configuration settings	<pre>cut interrupting running tasks. View task progress or open this titions in the command bar, and then Task Details. </pre>

Pro Tip: For this installation, we've temporarily disabled the Microsoft Windows Firewall and Internet Explorer Enhanced Security for Administrators. If you plan to re-enable the Microsoft Windows Firewall after the installation is complete, we will guide you through the creation of a rule for RADIUS.



Installing & Configuring SecurEnvoy SecurAccess

The following steps are required to configure the SecurEnvoy SecurAccess product for use. We suggest that you gather the following listed items before getting started and have them available.

Note: This is the basic configuration to get the system installed and ready for use. Secure LDAP and SSL Certificates are strongly recommended for a production build. We cover those items further in this document.

Currently, you'll need;

- Microsoft Active Directory Domain FQDN and NetBIOS Name
- FQDN for at least one Domain Controller, two recommended
- Create (or use) an existing Service Account from your Active Directory
- SMTP Server FQDN, including port and encryption requirements
- Email Account credentials

Downloading our Software

You can find the most current version of our software available on our web site, shown below.

ر المعالم المعام المعام (المعام) المعام المعام (المعام) المعام (المعام) (المعام) المعام (المعام) (المعام) (الم	- ≞ ¢	Search	× ロ -
Two Factor Authentication ×		Startin	
		artners Login Try Us Today English (US	
	P2	riners Login III OS Today	,,, °
A Shearwater Group pic Company	Solutions - Integrations - Partners - Insights -	 Support ~ About Us ~ Contact 	Q
Whats New Developer Guides	Documents and Resources Downloads	SMS Gateway Technical Support	
SecurEnvoy version			
Request Full Product Set-HTTP			
Request Software >			
Important Notice			
Version o 3 is now available. Additionally, as	part of our commitment to providing the most secure produ	ucts on the market, we regularly check	
the security of our own product for known th	reats. As a result of these routine practices, we have a vg.3	release categorized as a High Priority	
Security Release. We recommend that all cu	stomers running v9.2 upgrade as soon as possible to v9.3 (available here).	
Thank you!			
Our software is available for download here.			
download here.	Click here to download our product.		
If you need a trial license, the license key is below:	The download is a zip file.		
in you need a that itemse, the itemse key is below.	Also, take note of your license key.		
The 30-day trial license key:			
······································			
TvA76hfuwiHUludhf86FFd66g	gH3BGF11gcPg2R6		
A member of our team may follow up with you roo	arding your trial. If you		
A member of our team may follow up with you reg have any questions about integrations or set-up, pl			
support area.			



File Home	Share	View				-	٥	× ~ ?
← → ~ ↑ <mark> </mark>	> Thi	is PC > Desktop >				5 ~		Q
🗸 🖈 Quick access		Name	Date modified	Туре	Size			
Desktop Downloads Documents Pictures	* * *	 readme Release Notes .pdf SecurEnvoy - SecurAccess Administratio SecurEnvoy - Server Installation Guide.pdf setup 	7/6/2019 12:49 AM 7/6/2019 12:49 AM 7/6/2019 12:49 AM 7/6/2019 12:49 AM 7/6/2019 12:49 AM	Text Document PDF File PDF File PDF File Application	2 KB 324 KB 5,809 KB 2,712 KB 32,388 KB			
> 🥩 Network						We've downloaded and extracted the files to the server desktop.		

We suggest extracting the files on the server to which you intend to install the product. Here we've extracted them to the desktop of the server. You can extract our download anywhere you like.

Installing SecurAccess

As we prepare to run setup.exe, it's important to remember that Active Directory membership for the SecurEnvoy SecurAccess Server is optional. If your server is part of the Active Directory, you should logon as a Domain or Local Administrator to complete the following steps.

Welcome to the System Installer





License Agreement

Please review and accept our licensing terms to continue.

😽 SecurEnvoy Server - InstallShield Wiz	ard		>
License Agreement Please read the following license agree	ment carefully.		
END-USER LICENCE AGREEMENT			^
This Licence Agreement ("Licence") is a le and [SecurEnvoy Limited, a company regis 04866711] ("Licensor", "us" or "we" or "ou This Licence applies to the computer prog licence, any data supplied with the softwa Release which is acquired by you during t all associated printed materials and online the Software ("Documentation").	stered in England a ur"). rams identified in y are and any assoc the subsistence o	and Wales under co your Order accompa stated media, and an f this Licence ("Soft	mpany number nying this y Software ware"); and to
O I accept the terms in the license agreem O I do not accept the terms in the license			
installShield —	< <u>B</u> ack	<u>N</u> ext >	Cancel

Installation Path

Although we recommend keeping the default installer path, you are free to change it to meet any requirements you may have. Please remember this, as you may find the default path referenced in some of our other documents.

😸 SecurEn	voy Server - InstallShield Wiz	zard		×
	i on Folder kt to install to this location, for	new installs you can	change this locati	ion
	upgrades MUST use the same C:\Program Files (x86)\Secur		ver\	Change
InstallShield -				
		< Back	Next >	Cancel



Select Setup Type

The typical install will install all features on the system. A custom install gives you the opportunity to select specific components. It's recommended that you use the typical installer, unless you are performing an advanced installation.

🛃 SecurEnvoy S	erver - InstallShield Wizard X	
Setup Type		
Choose the se	tup type that best suits your needs.	
Please select a	a setup type.	
Typical		
	All web portals will be installed	
	Colocting the Typical install will	
	Selecting the Typical install will install all product features.	
O Custom		
12	Choose which program features you want installed and where they will be installed. Recommended for advanced users.	
InstallShield ———		
	< Back Next > Cancel	

🕷 SecurEnvoy Server - InstallShield Wizard 🛛 🗙	
Ready to Install the Program	
The wizard is ready to begin installation.	
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
Current Settings:	
Setup Type:	
Typical	Click Install to get started.
Destination Folder:	Ŭ
C:\Program Files (x86)\SecurEnvoy\Security Server\	
User Information:	
Name: Windows User	
Company:	
Serial:	
InstallShield	
< Back Install Cancel	



The installer will now begin running through the tasks of installing the system.

SecurEm	voy Server - InstallShield Wizard — 🗌 🗙
Jes securent	
Installing	SecurEnvoy Server
The prog	ram features you selected are being installed.
15	Please wait while the InstallShield Wizard installs SecurEnvoy Server. This may take several minutes.
	Status:
	Copying new files
InstallShield	
	< Back Next > Cancel

Advanced Configuration Wizard	_		×	
Optimising Object Code, Please Wait				
		(
				Il be optimized for the
		s	ystem	. This may take a few minutes.
				minutes.

Most (if not all) systems will require the CGI module and the ASP.NET 4.5 Module, you'll be prompted and should accept.





🔀 Advanced Co	nfiguration Wizard —	×		
What type (f installation is this?			
New D	adicated Server			
-	nal Server (Replica)			
 Upgrad 	e			
	(
		Since t	nis is the first SecurAccess	
			in your environment, you	
			ld select New Dedicated	
			Server.	
	Continue			
	Continuo			
config		×		
Loning		^		
New Custome Files (x86)\Sec	r Encryption Key Created. You must backup C:\Progr urEnvoy\Security Server\config.db	/am		
	0	К		
🔀 Advanced Co	nfiguration Wizard —	×		
			Enter your comp	any details
			and licensing in	
YourC	ompany Name			
ompany Name:	ABC Company, Inc.			
Licenc	e Details			
	Paste a copy of your licence below or leave blank to enter this la	ater		
Licence:	ThdyiHiofuwouo&ty97h34tp80Ouhf0934oijo&*ho			
	Continue			



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. We strongly recommend that you create a general user account in the Active Directory to serve as the service account. This account does not need to be a Domain Administrator, it can be a simple standard user.

Pro Tip: It's advisable to set the password on this account to never expire.

The LDAP Admin service account used by SecurEnvoy for SecurAccess and SecurPassword require 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"

Note: It's important to remember that although you may logon to the SecurEnvoy SecurAccess Management console as a Domain Administrator, the service account is still the account that will reach the Active Directory.

SecurEnvoy Service Permissions Account Wizard

To avoid setting the service account as an administrator, its critical that the permissions for this account's access into the Active Directory be limited. As noted above, we only require access to specific fields of a users' account. Access to these fields are necessary for the system to perform functions such as adding and registering new users, adding mobile phone numbers to a user's account and updating email addresses.

- On the SecurEnvoy SecurAccess Server, navigate to C:\Program Files (x86)\SecurEnvoy\Security Server\Config
- Copy ServiceAccountWizard.exe tool to your Active Directory Domain Controller.





You will need to logon as a Domain Administrator and run this file with Administrative Authority.

Recycle Bin		You should run the Service Account Wizard as Administrator	
ntWi	Open Run as administrator Troubleshoot compatibility Pin to Start Share Give access to Pin to taskbar Restore previous versions Send to Cut Copy Create shortcut Delete Rename Properties		
= ク = <i>6</i> 🔚			

	SecurEnvoy Service Pe	rmissions Account Wi	izard (DC=lab,DC=local) -		
Enter your service account name here.			Domain Controller (DC) \ServiceAccountWizard.exe to your DC and	d run it Use this button to get the full DN for the account.	
	Service Account				
	First create the user manually	in AD Users and Comp	uters. Enter the usemame below, and client on UN" to get it	s full DN.	
cctive ectory	Service account name:	SecurEnvoyAcct	Get DN		
	Service account DN:	CN=SecurEnvoyAcct.0	CN=Users,DC=lab,DC=local		
	Organizational Unit Leave blank to apply permiss		D (18th) December ded)		
	Enterpise Admins, etc)	specific UU if only non-	priviliged users will be enrolled with SecurEnvoy (ie No Doma	This will populate automatically	
	OU:			when you use the Get DN	
				button.	
	Permissions:				
	Select the required write per	nissions:			
	Always required:	Optional:	Required for SecurPassword:		
	Primary Telex Number	🗹 m <mark>obile</mark>	Reset Password		
	telexNumber	mail	Change Password		
			✓ pwdLastSet		
			userAccountControl Ap		
	PrimaryTelexNumber:	e			
	Command:		NB\SecurEnvoyAcct:RP;primaryTelexNumber;us		
Select the permissions that you care to	/I:S	,DC=IOCAI /G "LA	ab\SecuranvoyAcct:xp;primarylelexNumber;us		
allow the service account to have.	Command: dsacls.exe DC=lab	DC=local /G "LA	AB\SecurEnvoyAcct:WP;primaryTelexNumber;us	er"	
	/I:S TelexNumber:			Once you're ready, click Apply here t	
This may vary, depending on your	Command:			assign the permissions to the servic	e
internal security policy.	Command:		<pre>\B\SecurEnvoyAcct:RP;telexNumber;user" /I: \B\SecurEnvoyAcct:WP;telexNumber:user" /I:</pre>	account.	
We recommend checking all required				You will see the results displayed belo	w.
and optional permissions.				internet in the second second	



Configuring SecurEnvoy SecurAccess

Once the installation has been completed, you will need to configure the system for use. It is required that you authenticate to the SecurEnvoy SecurAccess Security Server as a local administrator, or as a domain administrator if your system is part of an Active Directory.



Note: The Local Administrator will run under the account context that you have authenticated to this server with.

		- 0 X
(=)(=) (=) Iocalho		?ACTION=LOCALLOGIN&COOKIE=SecurEnvoyAdmin=localadmin:031900:11072019:ADMIN:F8A008024CC6F9 🝷 🖒 🛛 Search 🔎 🖛 🟠 🔅 🥴
		Hello localadmin 🗸 ^
<i>*</i> 1	nitial Setup Wizard	Setup Wizard
ធ	Dashboard	•
	Domains	Intro Licence Domain Email Settings External URLs SMS/Voice Radius Services Complete Gateways
hh (Config	Gateways
	Gateways	Introduction
F	Radius	Welcome to the SecurEnvoy Admin Setup Wizard. This short wizard will guide you through the initial configuration of the system to a production ready status. You should review the
<u>લ</u> ા	Jsers	requirements below, assuring that you have the information needed to complete to configuration
»))) r	NFC	If you need to change any of these settings in the future, you will be able to find them by using the menu to the left. On each page of the wizard, the location of the settings will be shown by this arrow next to the menu item.
E ı	.og Viewer	Prerequisites
F	Reporting	SMTP Server Server Address Authentication Details (if required)
∩ A	Alerting	Email Address to send admin emails from LDAP Server
	SecurMail	Option 1: An existing Microsoft AD, Novell eDirectory, OpenLDAP, Oracle Directory Server, then the following will be required:

Note: As you enter details for the system, the Continue button can be located below the bottom of the screen and you'll need to scroll down.





Note: We have entered some details for you to use as a reference in these screen captures. Please assure that you are entering the correct details for your network and organization.



Note: Make sure to click the Test Server button to assure that you have established working communications.





Configuring Email settings is an important part of the system. With these settings, the SecurEnvoy Security Server will be able to send welcome emails and other notifications to users and administrators of the system.

Note: The system will default to SMTP Port 25, unless you specify a different port. To specify a different port, you must add the port number to the end of your Email Server Host as follows:

<Your Mail Server>:<Port>

Example: smtp.gmail.com:587

	admin/?action=wizard§ion=email&senor		5040005776610		✓ ♂ Search		 م	□ × }☆∰ 🥲
Calhost ×		102=029449919243329059040420.	3949223090770019		• O Search		v.	I ₩ 253 ₩
Domains	Setup Wizard							^
			•					
하다 Config			— <u> </u>				-0	
Licence	Intro Licence	Domain	Email Settings	External URLs	SMS/Voice Gateways	Radius	Services	Complete
Authentication Types								
Temp and Static Code	Email Settings							
PIN Management	We will sometimes need to send o	ut a few emails to users that will h	a authenticating with Sec	urEnvov Diesse enter	the details of an SMTD server t	hat you have access to and the e	mail address that you	would
Mobile Number	like the emails to be sent from.	or a rew emails to users that will b	se autienticating with set	urenvoy. Piease enter	the details of all Swite server (hac you have access to, and the e	mait address that you	WOOLD
Direct Password Control	This gateway is required if you war	t to enrol users via email, enrol so	oft tokens, send passcode	s via email or install S	ecurMail			
Account Lockout	Email Server Host							
Emergency Helpdesk	lab-mx-01.lab.local:587	Enter the SMTP mail server	's hostname or IP address	used for sending ema	l to your email gateway or ISP	(example: mail.mycompany.com)		
SecurMail	Admin Email Address							
Migration	securenvoy@company.com	Enter Aministrator's Email	Address. Used for sendin	g automated email err	ors (example: admin@mycomp	any.com)		
Group Deployment Logging	 Authentication is required 							
Rest API	UserID		We have er	ntered the ema	il server			
Misc GUI Settings	securenvoy@company.com	7 \	host, port, s	specified authe	ntication			
Email Settings			and inclu	ided account d	etails.			
External URLs	Password							
Gateways				vironment may				
HH Guttings	Use SSL/TLS		differ	ent requiremer	nts.			
Radius								
Se Users	Test SMTP Mail Server							
	Send Test Message To							
)))) NFC								
Log Viewer	Test Mail Server							
								•
							_	
	dmin/7action=winzed8usaction=wd8usacaass	- 020440010245520020046426504	0225006776610		- C Sourch		-	
	admin/?action=wizard§ion=url&senonce	=829449919245529039046426594	19225096776619		 C Search 		- ター 位	□ × 3☆∰ (5)
(⇐) (⇐) (⇐) http://localhost/sec (⇐) localhost ×		=829449919245529039046426594	9225096776619		 ♥ ♥ Search) 🕁 🛱 🙂
Colhost ×		=829449919245529039046426594	19225096776619		v ⊄ Search			
		=829449919245529039046426594	19225096776619		▼ Ĉ) 🕁 🛱 🙂
Cocalhost X		=829449919245529039046426594	9225096776619		▼ Ĉ) 🕁 🛱 🙂
Colhost ×		=829449919245529039046426594	19225096776619		← Ĉ) 🕁 🛱 🙂
localhost ×		=829449919245529039046426594	9225096776619		- C Search) 🕁 🛱 🙂
Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Contro Control Control Control Control Contr	Setup Wizard						Hello lo) 슜 쯦 () catadmin ~
Contraction of the second sec			19225096776619	Externat URLs	- C Search	Radius) 🕁 🛱 🙂
Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Contro Control Control Control Control Contr	Setup Wizard			External URLs		Radius	Hello lo) 슜 쯦 () catadmin ~
Config Licence Licenc	Setup Wizard				SMS/Voice Gateways	Radius	Hello lo) 슜 쯦 영
localhost × Accoration (State Decomposition) Initial Setup Wizard Dashboard Domains Config Licence Authentication Types	Setup Wizard	Domain	Email Settings	You should ta	SMS/Voice Gateways	Radius equired, you do not need to publ	Hello lo Services	2 ☆ 際 🧐 caladmin 🗸 Complete
localhost × Secure Envoy Anovember (Kus de Company Initial Setup Wizard Dashboard Domains Licence Authentication Types Temp and Static Code	Setup Wizard	Domain curEnvoy system to work, such as	Email Settings	You should ta	SMS/Voice Gateways		Hello lo Services	Complete
Config Licence Authentication Types Temp and Static Code PIN Management	Setup Wizard Setup Wizard Licence External URLs In order for some aspects of the Se This IIS server supports HTT	Domain curEnvoy system to work, such as	Email Settings	You should ta	SMS/Voice Gateways		Hello lo Services	Complete
Config Licence Authentication Types Temp and Static Code PIN Management Mobile Number	Setup Wizard Setup Wizard External URLs In order for some aspects of the Set	Domain curEnvoy system to work, such as 5 enrolment and on-going token ty	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.		Hello lo Services	Complete
	Setup Wizard External URLs In order for some aspects of the Se This URLS Server supports HTT Enrolment and "Manage My Token This URL is used for both first time	Domain curEnvoy system to work, such as 5 enrolment and on-going token ty	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	Complete
	Setup Wizard External URLs In order for some aspects of the Se This IIS server supports HTT Enrotment and "Manage My Token This URL is used for both first time Inttp://LAB-SE-01/secenrol	Domain curEnvoy system to work, such as 5 enrolment and on-going token ty	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	Complete
	Setup Wizard External URLs In order for some aspects of the Se This URLS Server supports HTT Enrolment and "Manage My Token This URL is used for both first time	Domain CurEnvoy system to work, such as 55 enrolment and on-going token ty	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	2 ☆ 際 🧐 caladmin 🗸 Complete
localhost ×	Setup Wizard Licence External URLs In order for some aspects of the Se External URLs In order for some aspects of the Se This URL is used for both first time Inttp://LAB-SE-01/secenrol Agent Services This URL is used by Windows Login	Domain CurEnvoy system to work, such as 55 enrolment and on-going token ty	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	2 ☆ 際 🧐 caladmin 🗸 Complete
Icalhost × Icalhost × Accorate Coup of Composition Initial Setup Wizard Dashboard Domains Config Licence Authentication Types Temp and Static Code PIN Management Mobile Number Direct Password Control Account Lockout Emergency Helpdesk SecurMail	Setup Wizard Licence External URLS In order for some aspects of the See External URLS In order for some aspects of the See This IIS server supports HTT EnroIment and "Manage My Token This URL is used for both first time http://LAB-SE-01/secenver http://LAB-SE-01/secenver	Domain CurEnvoy system to work, such as 55 enrolment and on-going token ty	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	2 ☆ 際 🧐 caladmin 🗸 Complete
localhost ×	Setup Wizard Licence External URLs In order for some aspects of the Se External URLs In order for some aspects of the Se This URL is used for both first time Inttp://LAB-SE-01/secenrol Agent Services This URL is used by Windows Login	Domain Domain curEnvoy system to work, such as so enrolment and on-going token typ a Agent and SecurMail Outlook Ag	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	2 ☆ 際 🧐 caladmin 🗸 Complete
	Setup Wizard	Domain Domain curEnvoy system to work, such as so enrolment and on-going token typ a Agent and SecurMail Outlook Ag	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	Complete
	Setup Wizard Licence External URLs In order for some aspects of the Se External URLs In order for some aspects of the Se This URL is used for both first time http://LAB-SE-01/secervol Agent Services This URL is used by Windows Login http://LAB-SE-01/secrver SecurMail Recipient Pickup This URL is used by SecurMail recipient http://LAB-SE-01/secrmail	Domain Domain curEnvoy system to work, such as so enrolment and on-going token typ a Agent and SecurMail Outlook Ag	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	2 ☆ 際 🧐 caladmin 🗸 Complete
Iocalhost × Iocalhost × Iocalhost × Secure Environment Initial Setup Wizard Iocalia Domains Iocalia Domains Iocalia Iconfig Licence Authentication Types Temp and Static Code PIN Management Mobile Number Direct Password Control Account Lockout Emergency Helpdesk SecurMail Migration Group Deployment Logging Rest API	Setup Wizard	Domain Domain curEnvoy system to work, such as so enrolment and on-going token typ a Agent and SecurMail Outlook Ag	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	Complete
Iocalhost × Iocalhost × Secure Envoy Alternational Secure of Compary Initial Setup Wizard Dashboard Domains Config Licence Authentication Types Temp and Static Code PIN Management Mobile Number Direct Password Control. Account Lockout Emergency Helpdesk SecurMail Migration Group Deployment Logging Rest API Misc GUI Settings	Setup Wizard Licence External URLs In order for some aspects of the Se External URLs In order for some aspects of the Se This URL is used for both first time http://LAB-SE-01/secervol Agent Services This URL is used by Windows Login http://LAB-SE-01/secrver SecurMail Recipient Pickup This URL is used by SecurMail recipient http://LAB-SE-01/secrmail	Domain Domain curEnvoy system to work, such as so enrolment and on-going token typ a Agent and SecurMail Outlook Ag	Email Settings	You should ta URL's fo	SMS/Voice Gateways ke note of these r use later.	equired, you do not need to publ	Hello lo Services	Complete



The system defaults to an unsecured URL state, since it does not initially have an SSL Certificate for IIS. Once we complete the initial setup and configuration, we cover requirements for securing the system.











SecurEnvoy SecurAccess Dashboard

The system dashboard is a vital area for administrators to get information related to the systems health and the activities of users. The dashboard has several components which we've illustrated here.

Dashboard Components

This top section of the dashboard displays current and historical data. This part is useful, providing the administrator to select the period to review, from 7, 14 or 30 days.

How users are authenticating is an important part of understanding the community. This area will also display both successful and failed authentications, so you'll be able to spot issues easily.

SecurEnvoy	1								Hello administrator 🗸 📩
A Stewarester Group pic Company	Dashboa	ard							Show Stats for Last: 30 Days
de la config	User Stats								
Gateways	Authentication	is in Period	Authentication Met	hods Used					
Radius	Successful	Failed	One Time Code	Soft Token Code	Voice Call	Yubikey	Temp Code	Static Code	
Se Users	24	4	0	18	0	0	0	6	La Cart
))) NFC									

The middle section of the dashboard contains the most recent 10 actions from the logs and gateway status for quick reference. This section sis helpful as it provides an immediate view of system health in respect to communications and events.

og (Last 10)		Gateway Status			
UserID	Message	Туре	Name	Status	
administrator@securenvoy.us	Access Accepted with Static Code From ClientIP=LocalHost RemoteID=	SMS	AQL_Trial SMS	~	Ready
administrator@securenvoy.us	AD Password Accepted From ClientIP=LocalHost RemoteID= Passcode Check Still Required	SMS	CM_Trial SMS	0	Ready
Unknown	No UserID Entered	Voice	AQL_Voip_Trial	v	Ready
administrator@securenvoy.us	Access Accepted from Oneswipe Online Push ClientIP=192.168.3.201 RemoteID=	Push	ApplePushService	~	Ready
administrator@securenvoy.us	(GoogleCloudMessaging) Push Notification Sent	Push	GoogleCloudMessaging	0	Ready
administrator@securenvoy.us	PIN Check Skipped From ClientIP=192.168.3.201 RemoteID= Passcode Check Still Required	Push	MicrosoftPushService		Ready
administrator@securenvoy.us	Access Accepted from Oneswipe Online Push ClientIP=192.168.3.201 Remote/D=	Push	GoogleFirebase	v	Ready
administrator@securenvoy.us	(GoogleCloudMessaging) Push Notification Sent	Manage Gateways			
administrator@securenvoy.us	PIN Check Skipped From ClientIP=192.168.3.201 RemoteID= Passcode Check Still Required				
System	Batch Server Completed OK Next Run in 23 Hours and 40 Minutes				
ew Full Log					



Further, this section of the dashboard provides status of services running and connectivity to LDAP environments. If you have a system that is connected to more than one LDAP environment, all of them will be displayed.



The graph at the bottom of the dashboard illustrates trends on the system. This graph will automatically adjust it's timeframe to the same period as the rest of the dashboard.



Note: These illustrations of the dashboard includes data from our lab environment. Yours will not initially have any data.



Configure Radius Client Connections

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.

ASCII 127 is an industry standard character code set, which is basically your keyboard. Below is a table which outlines this code set. There are a few characters that should not be used when with a Radius Shared Secret and we've highlighted these for you. We've included both the character code and the character itself, so you'll see them paired together.

CODE	CHAR	16	CODE	CHAR	2	CODE	CHAR	CODE	CHAR	CODE	CHAR	CODE	CHAR
32	Space		48	0		64	@	80	Р	96	`	112	Р
33	!		49	1		65	А	81	Q	97	а	113	Q
34	"		50	2		66	В	82	R	98	b	114	R
35	#		51	3		67	С	83	S	99	С	115	S
36	\$		52	4		68	D	84	Т	100	D	116	Т
37	%		53	5		69	E	85	U	101	е	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	Н	88	Х	104	h	120	Х
41)		57	9		73	1	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	$\langle \rangle$	108	- I	124	
45	-		61	=		77	М	93]	109	m	125	}
46		Q.	62	>		78	N	94	^	110	N	126	~
47	/		63	?		79	0	95	_	111	0	127	Delete

All ASCII 127 codes and characters are allowable, with a few exceptions. Please try to avoid the ones highlighted in Orange.

Pro Tip: You'll notice that the first 31 are not used. These are control characters, like shift, return and line feed which are not characters you can use in text.



In order to process authentication, both devices (your VPN and this security server) need to communicate. They do this using the Radius protocol. Radius is a very popular standard for this form of communication.

There are two sides to this communication. You'll need to configure your device (Cisco VPN for example) to direct Radius traffic here and then you configure The SecurEnvoy SecurAccess Server to direct traffic back, essentially pointing the two devices to each other.



Once you click Update, your system is ready to receive Radius authentication requests from other devices within your network. If you have a requirement to configure advanced or specific settings related to the Radius configuration, you may click the Show Advanced Button.

Pro Tip: Rules for Radius authentication are in the Advanced Settings. Trusted Networks, Blocked Networks, LDAP Group Based Authentication and advanced Radius Attribute configurations are located here.



Registering Your First Device

For users to have the ability to use features like push notifications and soft tokens, they'll need to download the SecurEnvoy Authenticator form the Android or Apple app store.

We update our SecurEnvoy Authenticator often. You'll receive notifications when there are updates available.

Once they have installed the app, you will need to configure their user account for use with SecurEnvoy SecurAccess.











Authentication Type
One Time Code
Use Real Time Not regard
O Soft Token
Registered Phone Type = Android Resp. During initial device registration, you
O Voice Call user so they can use it to login to the
VOIP Call, landline or mobile registration system.
O Temp Code
Passcode Days
Max 14 Device Not Lost
O Static Code
Passcode
must be 6 digits long
Vublikey
Use a Yubikey as the sole method of authentication
Current Serial Number New Key
Update
OK, User Enrol Sent Via eMail
Once you click Update, you
will see this following message confirming.

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 two important components;

- The URL to the web site where user registers their device.
- The OTP that they'll need to get authenticated.

Manage My Token	The user follows the link and arrives here, at the registration site.
Manage My Token : Authentication	The user is instructed to use their Microsoft Active Directory Credentials.
UserID: swallace	
Enter Microsoft Password:	
Login	
A Shearwater Group plc Company	The user is then prompted for
A Shearwater Group plc Company Manage My Token	The user is then prompted for the One Time Passcode (OTP) that they received in the same
	The user is then prompted for the One Time Passcode (OTP)



Once the user has authenticated, they are presented with options on how to receive and use Multi-Factor Tokens when they logon to solutions that are integrated with the system.

Note: The options presented here to users is directly related to the options made available by the system administrator. For additional details, please reference our administrators guide.

Manage My Token	
Login Authentication Type Secret Questions Complete	
Send My Passcode Via SMS Note: Your mobile number will be encrypted and will only be used for receiving passcodes Enter Your Mobile Number Call My Phone Note: Your phone number will be encrypted and only used for authentication calls Enter Your Phone Number Format: + CountryCode Number (e.g. +11234567890) Setup My Soft Token App	
Step 1) Install the SecurEnvoy App on your phone Push Enabled? Step 2) Press the ADD button Step 3) Scan QROde with your phone's camera or manually ent this key VSGEYSDVGXSHE Step 4) Enter the displayed Code Complete Step 4 To Activate Your Token (click to enlarge)	
Compare stap in to Activate tool token	

If the user is planning to use Push Authentication, the selecting this option will present them with a QR code for scanning and they should complete the following steps.

Step 1, Click the Add Icon	Step 2, Click Scan QR	Complete
Secur Invey	Browse and login to your Organisation's "Manage My Token' Portal	Securitivey Employed 20 779789 Push Copy
	13 or 16 Character Rey 🚳 Manual Scan QR	
•		•
III O <	III O (III 0 <

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.

Upgrading Your Server

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

Prior to Upgrade

Before upgrading the SecurEnvoy Security Server software, please take a backup of the following item(s):

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

- config.db
- configpre54.db
- local.ini
- server.ini
- gateway.ini
- A full copy of the entire DATA directory
- Export the registry key HKLM\software\SecurEnvoy

Pro Tip: Please make sure that all SecurEnvoy Web Portals are closed in advance of the upgrade so that files which need to be replaced are not locked. A good method of doing this is to simply Stop IIS Web Services.

Upgrades performed are delivered directly over the existing installation.



- Download the latest version of our software.
- Extract to the server.
- Run Setup.exe.
- Select Upgrade.
- Follow along with the on-screen prompts.



1 Community () () () () () () () () () (
SecurEnvoy Server - Instal	ishield Wizard				7	23	
					1	124	
This Licence Agreemen ("Licensee" or "you") a England and Wales und or "we" or "our").	nd [SecurEnv	oy Limite	d, a c	ompany	registe	ered in	
This Licence applies to	the computer	programs	iden	tified in v	our O	rder	
accompanying this licen associated media, and a during the subsistence o	ce, any data ny Software	supplied w Release w	vith th vhich	e softwa is acquire	re and ed by y	any you	
I accept the terms in the lic I do not accept the terms in	-						
stallShield		< Back		Next >		Cancel]
SecurEnvoy Server - Instal	IShield Wizard				1	X	
upgrades MUST u C:\Program Files			erver)			Change	
nstallShield		< Back		Next >		Cancel	-
		< DOLK		ACAL >		Curice	
SecurEnvoy Server - Instal	IShield Wizard					×	
						1	
Please select a setup type.							
Typical All web por	tals will be insta	lled					
D C C							
	ich program fea				here th	ey	
will be insta	alled. Recommen	ided for adva	anced u	users.			
stallShield							_
		< Back		Next >		Cancel	
SecurEnvoy Server - Instal	IShield Winned		/			X	
g securenvoy server - instal	isinciu wizard				5		
If you want to review or ch	lange any of you	ur installation	settin	gs, dick Ba	:k. Click	Cancel to	
exit the wizard. Current Settings:							
Setup Type: Typical							
· / produ							
Destination Folder:							
C:\Program Files (x86)	\SecurEnvoy\Se	curity Server	١				
C:\Program Files (x86) User Information: Name: Windows User	\SecurEnvoy\Se	curity Server	١				
C:\Program Files (x86) User Information:	\SecurEnvoy\Se	curity Server	١				
C:\Program Files (x86) User Information: Name: Windows User Company:	\SecurEnvoy\Se	curity Server	١	Install		Cancel	_

Review and accept the licensing terms.

- The system installer will prompt for an install location.
- Because this is an upgrade, you need to assure that this location is the same as the original installation so files can be upgraded properly.

- Select Typical for most upgrades.
- Select Custom only if you had a custom installation previously.

Once you click Install, the upgrade process will begin.





When the upgrade has completed, click Finish.

Post Upgrade Tasks

Once the upgrade has completed, you should 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.

Installing an Additional SecurEnvoy Server

Some organizations wish to have more than one SecurEnvoy Security Server for failover, load balancing and other redundancy. SecurEnvoy itself does not have any load balancing features integrated within it, so this process will require load balancing services from a load balancer, like a F5, Citrix NetScaler or other.

Understanding that the services within SecurEnvoy will be using an SSL Certificate, it will be important to assure that you have configured SSL Session Persistency on your load balancer so that communication between the user and this system works properly.

Adding a second server is performed in the exact same manner as a standard installation, with only one exception;

🛪 Advanced Configuration Wizard	
What type of installation is this?	
O New Dedicated Server	
Additional Server (Replica)	
○ Upgrade	
Upload config.db and server.ini	
You need to import config.db a other security server. These are \Program Files\SecurEnvoy\Se	e usually located at
	Upload config.db OK
	Upload server.ini OK
Opt	ional Upload gateway.ini OK
Uploaded gateway.ini OK	
	Continue
	Continue

- Follow the previously described install steps, selecting Additional Server (Replica) as shown.
- Once you select Additional Server (Replic) you will be prompted for the following three files;
 - Config.db
 - Server.ini
 - Gateway.ini

These three files contain the working configuration for the first server you installed, but they do not contain everything.

- Radius Clients and settings.
- Custom templates.

Note: Additional Servers must use the same Service Account as the original.



Support

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

https://www.securenvoy.com/en-us/contact-us

We have a global team of experts to assist you. You can send an email to <u>info@securenvoy.com</u> for an immediate response.

Our Web Site is also full of useful information, documents and how-to guides.

Whats New Developer Guides	Documents and Resources Downloads	SMS Gateway Technical Support
Server Administration Guide	Server Installation Guide	SecurAccess Security Hardening
Download PDF	Download PDF	Guide Download PDF
Mobile Authenticator Customization	SecurAccess Upgrade Journey Download PDF	Full Historic Release Notes
Windows Login Agent Download PDF	Microsoft Server Agent Download PDF	



Appendix – Setting Service Account Permissions Manually

Some customers find that strict permissions on the Active Directory prevent the Service Account Wizard from assigning permissions to the SecurEnvoy Service Account properly or at all.

If this happens, you have two choices;

- Set the Service Account as a Domain Administrator
- Set the Permissions Manually using ADSI Edit

Note: We don't recommend giving the Service Account Domain Administrator permissions for a production environment.

Pro Tip: When creating your service account, it's recommended that you take note of the Display Name, which can be different than the actual account name. This can become important when referencing the account's DN.



		2		
Active Directory Users and Comp	uters		-	- 0 ×
File Action View Help				
(+ +) 🖄 📰 🔏 🗎 🗙 🛙	i a 🕞 🛛 🖬 🔧 🗽 în 🔻 🖻 🍇			
Active Directory Users and Com Active Directory Users and Com Solution Solution Solution Solution Solution Solution Solution Solution Active Directory Users Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution	Name & Administrator Allowed RODC Password Replication Group Cert Publishers Coneable Domain Controllers	Type User Security Group Security Group	Member Of Dial-in Environment Seasons Remote control Remote Desktop Services Profile COM+ General Address Account Pofile User logon name: SecurEnvoyAcct Image: Comparization User logon name (pre-Windows 2000): Image: Comparization Image: Comparization User logon name (pre-Windows 2000): Image: Comparization Image: Comparization User logon name (pre-Windows 2000): Image: Comparization Image: Comparization User logon name (pre-Windows 2000): Image: Comparization Image: Comparization User logon name (pre-Windows 2000): Image: Comparization Image: Comparization User logon name (pre-Windows 2000): Image: Comparization Image: Comparization User logon name (pre-Windows 2000): Image: Comparization Image: Comparization User logon name (pre-Windows 2000): Image: Comparization Image: Comparization User logon name (pre-Windows 2000): Image: Comparization Image: Comparization Image: Comparization Comparization Image: Comparization Image: Comparization Image: Comparization Comparization Image: Comparization Image: Comparization	9 for more informati
日 日 6	📄 🛷 🔢 🦹			









🕎 ADSI Edit					– a ×
File Action View Help					- 6 ^
ADSI Edit Name	Class	Distinguished Name			Actions
Default naming context [LAB-DC-01.lab.local]		These are iter	ns to show in this view.		CN=AdminSDHolder
✓ ☐ DC=lab,DC=local ☐ CN=Builtin		There are no iter	its to show in this view.		More Actions
CN=Computers					
OU=Domain Controllers					
CN=ForeignSecurityPrincipals			CN=AdminSDHolder Properti	ties ? ×	
CN=Keys					
CN=LostAndFound			Attribute Editor Security		
CN=Managed Service Accounts			– 🗆 X		
CN=Progr				nterprise Admins)	
V CN=Syste				histrators) atible Access (LAB\Pre-Windows 200	
CN=A Owner: Domain Admins (LAB\Domain Admin) Change			nvoyAcct@lab.local)	
CN=C	, change			cess Group (LAB Windows Authoriza	
CN=C Permissions Auditing Effective Access		(Servers (LAB\Terminal Server License Y	
		Find	the SecurEnvoy Serv	vice Account ^{dd} Remove	
CN=D For additional information, double-click a permission CN=D	ntry. To modify a pe		n the Advanced list. S		
CN=D Permission entries:			account only.		
CN=Fi Type Principal	Access	Inherited from	Applies to		
CN=Fi & Allow SYSTEM	Full control	None		Z G I I	
CN=IP CN=M Allow Domain Admins (LAB\Domain Admins)	Special	None	This object only		
CN-M Allow Enterprise Admins (LAB\Enterprise Adm	ns) Special	None	This object only		
CN=P; Allow Administrators (LAB\Administrators)	Special	None	This object only	inced settings, click Advanced	
CN=P Allow Pre-Windows 2000 Compatible Access (None	This object only	Advanced	
CN=P CN=P CN=R CN=R CN=R		None	This object only		
CN=R, Allow Everyone	Special Special	None None	This object only This object and al		
CN=R Allow SELF	Special	None	This object only	Cancel Apply Help	
CN=W <	opeciai	- Conc			
CN=TPM					
🖺 CN=Users Add Remove Edit 👡			Restore defaults		
Enable inheritance					
chapte intercance					
	(OK	Canc el Apply		
		With only the SecurEnv			
		Service Account Select	eu,		
		click Edit.			
🔳 🔎 🖽 🥔 🚔 🖉					

Once you click Edit above, you will be presented with a very detailed list of account permissions for the SecurEnvoy Service Account that you've created in the Microsoft Active Directory.

Please follow along, very specifically and exercise care to assure you are only assigning permissions required. Assigning additional or incorrect permissions may result in unusual behaviour.

It's important to know that the following screens are large and at times and lists of permissions can be long, we may only be showing a specific part of the screen.

📜 Permission Entry for AdminSDHolder			- 0 ×
Principal: SecurEnvoyAcct (SecurEnvoyAcct@lab.local) Type: Allow Applies to: Descendant User objects	Select a principal		
Permissions:	Make sure that you verify the Principal and type. Descendant User Objects is at the bottom of the list.	Create classStore objects Create FRS Subscriptions objects Create FRS Subscriptions objects Create ms-net-ieee-80211-GroupPolicy objects Create ms-net-ieee-8023-GroupPolicy objects Create ms-net-ieee-8023-GroupPolicy objects Classe ms-net-ieee-8023-GroupPolicy objects Classe ms-net-ieee-8023-GroupPolicy objects Allowed to authenticate Change password Reset password Send as	Located in the top permissions part, these two are only required if you are using our SecurPassword product.



The large security permissions list is alphabetical. Here, we are showing the following specific permissions that are required.

- Allow Write E-Mail Addresses
- Allow Write Telex Number
- Allow Write Telex Number (Other)
- Allow Write Mobile Number

Read dynamicLDAPServer	Write msTSBrokenConnectionAction
	Read msTSConnectClientDrives
Read E-Mail Address	Write msTSConnectClientDrives
Write E-Mail Address	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
Read E-Mail Address (Others)	Write msTSConnectPrinterDrives
Write E-Mail Address (Others)	Read msTSDefaultToMainPrinter
Read Employee ID	Write msTSDefaultToMainPrinter
Write Employee ID	🖂 Read msTSExpireDate
Read Middle Name	Write possibleInferiors
Write Middle Name	Read Post Office Box

Write Middle Name	Read Post Office Box	
Read Mobile Number	Write Post Office Box	
Write Mobile Number	Read postalAddress	
Read Mobile Number (Others)	Write postalAddress	
Write Mobile Number (Others)	Read preferredDeliveryMethod	
Read modifyTimeStamp	Write preferredDeliveryMethod	
Write modifyTimeStamp	Read preferredLanguage	
Write msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon	Read teletexTerminalldentifier	
Read msDS-GeoCoordinatesAltitude	Write teletexTerminalIdentifier	

Read msDS-GeoCoordinatesAltitude	Write teletexTerminalIdentifier
Write msDS-GeoCoordinatesAltitude	Read Telex Number
Read msDS-GeoCoordinatesLatitude	Write Telex Number
Write msDS-GeoCoordinatesLatitude	Read Telex Number (Others)
Read msDS-GeoCoordinatesLongitude	Write Telex Number (Others)
Write msDS-GeoCoordinatesLongitude	Read terminalServer
Read msDS-HABSeniorityIndex	Write terminalServer
Write msDS-HABSeniorityIndex	Read textEncodedORAddress

Note: If you have more than one SecurEnvoy SecurAccess Security Servers in your environment, they need to use the same service account to share the permissions you've set here.

Pro Tip: Once the security permissions have been applied, you can test in the SecurEnvoy Administration GUI, by looking up a user and entering a mobile number in the mobile number field.

When Successful, you'll receive a message; OK. Passcode Sent to Gateway. If you receive an error message, return here and validate your settings.



Appendix – TCP / UDP Communications / Firewall Ports

Below are all the necessary and optional port configurations for the SecurEnvoy SecurAccess Security Server. You should follow these guidelines when implementing a production system in a highly secure network.

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	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

Please Reach Out to Your Local SecurEnvoy Team...



UK & IRELAND

Belvedere House, Basing View Basingstoke, Hampshire RG21 4HG, 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
- 1 +012 9911 ///



USA - West Coast

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

General Information

- E info@SecurEnvoy.com
- Т (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



www.securenvoy.com

SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@SecurEnvoy.com T: 44 (0) 845 2600010 Company No. 04866711 VAT Number GB 862076128

C00010