Installation & Configuration Guide
v9.4.502

Authenticating Users Using SecurAccess Server by SecurEnvoy
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISCLAIMER</td>
<td>3</td>
</tr>
<tr>
<td>LEGAL</td>
<td>3</td>
</tr>
<tr>
<td>GETTING STARTED</td>
<td>4</td>
</tr>
<tr>
<td>Things You Will Need</td>
<td>4</td>
</tr>
<tr>
<td>Authentication Processing Topology</td>
<td>4</td>
</tr>
<tr>
<td>SYSTEM INSTALLATION</td>
<td>5</td>
</tr>
<tr>
<td>Installation of Microsoft IIS Web Service</td>
<td>6</td>
</tr>
<tr>
<td>INSTALLING &amp; CONFIGURING SECURITYOY SECURACCESS</td>
<td>11</td>
</tr>
<tr>
<td>Installing SecurAccess</td>
<td>12</td>
</tr>
<tr>
<td>Welcome to the System Installer</td>
<td>12</td>
</tr>
<tr>
<td>License Agreement</td>
<td>13</td>
</tr>
<tr>
<td>Select Setup Type</td>
<td>14</td>
</tr>
<tr>
<td>CONFIGURE YOUR SERVICE ACCOUNT</td>
<td>17</td>
</tr>
<tr>
<td>SECURITYOY SERVICE PERMISSIONS ACCOUNT WIZARD</td>
<td>17</td>
</tr>
<tr>
<td>CONFIGURING SECURITYOY SECURACCESS</td>
<td>19</td>
</tr>
<tr>
<td>SECURITYOY SECURACCESS DASHBOARD</td>
<td>24</td>
</tr>
<tr>
<td>Dashboard Components</td>
<td>24</td>
</tr>
<tr>
<td>CONFIGURE RADIUS CLIENT CONNECTIONS</td>
<td>26</td>
</tr>
<tr>
<td>REGISTERING YOUR FIRST DEVICE</td>
<td>28</td>
</tr>
<tr>
<td>UPGRADING YOUR SERVER</td>
<td>31</td>
</tr>
<tr>
<td>Prior to Upgrade</td>
<td>31</td>
</tr>
<tr>
<td>Post Upgrade Tasks</td>
<td>33</td>
</tr>
<tr>
<td>INSTALLING AN ADDITIONAL SECURITYOY SERVER</td>
<td>33</td>
</tr>
<tr>
<td>SUPPORT</td>
<td>34</td>
</tr>
<tr>
<td>APPENDIX — SETTING SERVICE ACCOUNT PERMISSIONS MANUALLY</td>
<td>35</td>
</tr>
<tr>
<td>APPENDIX — TCP / UDP COMMUNICATIONS / FIREWALL PORTS</td>
<td>39</td>
</tr>
</tbody>
</table>
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 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.

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.

**CPU**
- **Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz**
- Utilization: 1%
- Speed: 2.49 GHz
- Base speed: 2.40 GHz
- Sockets: 1
- Virtual processors: 4
- Virtual machine: Yes
- L1 cache: N/A

**Memory**
- Total: 8.0 GB
- Available: 1.4 GB
- Committed: 1.1 GB (0 MB) + 367 MB
- Cashed: 1.2/2.7 GB + 340 MB
- Paged pool: 87.0 MB
- Non-paged pool: 79.6 MB
- In use: 0
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:

1. Select the Role-Based Installation Type option.
2. Make sure that your server is selected.
Select the Server Role, Web Server.

Acknowledge the Add features dialog. You will need the Management Console later, if you plan to implement SSL certificates.
Accept the defaults here. There is no requirement to make any adjustments.

Check the Restart box here. Generally, the installation of Microsoft Web Services does not require a restart.

Select Install to complete this step and begin installing the Microsoft Web Server.
The installation of Microsoft Web Services will continue and may take a minute.

Once the installation has completed, you should close the Add Roles and Features Wizard.
**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.

[Image of SecurEnvoy web page]

Important Notice
Version 9.3 is now available. Additionally, as part of our commitment to providing the most secure products on the market, we regularly check the security of our own product for known threats. As a result of these routine practices, we have a v9.3 release categorized as a High Priority Security Release. We recommend that all customers running v9.2 upgrade as soon as possible to v9.3 (available here).

Thank you!
Our software is available for download here.

If you need a trial license, the license key is below:

The 30-day trial license key:

TvA76hfuwiHUluhhf86FFd66gH3BGF11gcPg2R6

A member of our team may follow up with you regarding your trial. If you have any questions about integrations or set-up, please refer to our support area.
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.

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.
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.

Selecting the Typical install will install all product features.

Click Install to get started.
The installer will now begin running through the tasks of installing the system.

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

Code will be optimized for the system. This may take a few minutes.
Since this is the first SecurAccess Server in your environment, you should select New Dedicated Server.

Enter your company details and licensing information.
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”

Optional, 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, it’s 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.
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.

Setup Wizard

Introduction
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 requirements below, assuring that you have the information needed to complete to configuration.
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.

Prerequisites
- SMTP Server
  - Server Address
- Authentication Details (if required)
- Email Address to send admin emails from
- LDAP Server
  - 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.

On the server desktop, you’ll find our local system administration GUI.
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*

We have entered the email server host, port, specified authentication and included account details. Your environment may have different requirements.

You should take note of these URL's for use later.
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.

**Gateway Configuration**

- **Add SMS Gateway**
  - Name: AOL_I Trial
  - Type: WEB
  - Domain: [empty]
  - Country: 1.4.3.1
  - Status: Please wait...

- **RADIUS**
  - Default Port: 1812
  - If you have a requirement to adjust this port, you can do so here, either now or later.
Services will start and show green when finished.

Now that the initial configuration is complete, you can click here and go to the dashboard.
SecurEnvoy SecurAccess Dashboard

The system dashboard is a vital area for administrators to get information related to the system's 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.

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

**Note:** You can also restart any of these services from this location.

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.

<table>
<thead>
<tr>
<th>CODE</th>
<th>CHAR</th>
<th>CODE</th>
<th>CHAR</th>
<th>CODE</th>
<th>CHAR</th>
<th>CODE</th>
<th>CHAR</th>
<th>CODE</th>
<th>CHAR</th>
<th>CODE</th>
<th>CHAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>Space</td>
<td>48</td>
<td>@</td>
<td>64</td>
<td>O</td>
<td>80</td>
<td>P</td>
<td>96</td>
<td>,</td>
<td>112</td>
<td>P</td>
</tr>
<tr>
<td>33</td>
<td>!</td>
<td>49</td>
<td>1</td>
<td>65</td>
<td>A</td>
<td>81</td>
<td>Q</td>
<td>97</td>
<td>a</td>
<td>113</td>
<td>Q</td>
</tr>
<tr>
<td>34</td>
<td>&quot;</td>
<td>50</td>
<td>2</td>
<td>66</td>
<td>B</td>
<td>82</td>
<td>R</td>
<td>98</td>
<td>b</td>
<td>114</td>
<td>R</td>
</tr>
<tr>
<td>35</td>
<td>#</td>
<td>51</td>
<td>3</td>
<td>67</td>
<td>C</td>
<td>83</td>
<td>S</td>
<td>99</td>
<td>c</td>
<td>115</td>
<td>S</td>
</tr>
<tr>
<td>36</td>
<td>$</td>
<td>52</td>
<td>4</td>
<td>68</td>
<td>D</td>
<td>84</td>
<td>T</td>
<td>100</td>
<td>D</td>
<td>116</td>
<td>T</td>
</tr>
<tr>
<td>37</td>
<td>%</td>
<td>53</td>
<td>5</td>
<td>69</td>
<td>E</td>
<td>85</td>
<td>U</td>
<td>101</td>
<td>E</td>
<td>117</td>
<td>U</td>
</tr>
<tr>
<td>38</td>
<td>&amp;</td>
<td>54</td>
<td>6</td>
<td>70</td>
<td>F</td>
<td>86</td>
<td>V</td>
<td>102</td>
<td>F</td>
<td>118</td>
<td>V</td>
</tr>
<tr>
<td>39</td>
<td>'</td>
<td>55</td>
<td>7</td>
<td>71</td>
<td>G</td>
<td>87</td>
<td>W</td>
<td>103</td>
<td>g</td>
<td>119</td>
<td>W</td>
</tr>
<tr>
<td>40</td>
<td>(</td>
<td>56</td>
<td>8</td>
<td>72</td>
<td>H</td>
<td>88</td>
<td>X</td>
<td>104</td>
<td>h</td>
<td>120</td>
<td>X</td>
</tr>
<tr>
<td>41</td>
<td>)</td>
<td>57</td>
<td>9</td>
<td>73</td>
<td>I</td>
<td>89</td>
<td>Y</td>
<td>105</td>
<td>i</td>
<td>121</td>
<td>Y</td>
</tr>
<tr>
<td>42</td>
<td>*</td>
<td>58</td>
<td>:</td>
<td>74</td>
<td>J</td>
<td>90</td>
<td>Z</td>
<td>106</td>
<td>J</td>
<td>122</td>
<td>Z</td>
</tr>
<tr>
<td>43</td>
<td>+</td>
<td>59</td>
<td>;</td>
<td>75</td>
<td>K</td>
<td>91</td>
<td>]</td>
<td>107</td>
<td>K</td>
<td>123</td>
<td>(</td>
</tr>
<tr>
<td>44</td>
<td>,</td>
<td>60</td>
<td>&lt;</td>
<td>76</td>
<td>L</td>
<td>92</td>
<td>\</td>
<td>108</td>
<td>I</td>
<td>124</td>
<td>)</td>
</tr>
<tr>
<td>45</td>
<td>-</td>
<td>61</td>
<td>=</td>
<td>77</td>
<td>M</td>
<td>93</td>
<td>)</td>
<td>109</td>
<td>m</td>
<td>125</td>
<td>}</td>
</tr>
<tr>
<td>46</td>
<td>.</td>
<td>62</td>
<td>&gt;</td>
<td>78</td>
<td>N</td>
<td>94</td>
<td>^</td>
<td>110</td>
<td>N</td>
<td>126</td>
<td>~</td>
</tr>
<tr>
<td>47</td>
<td>/</td>
<td>63</td>
<td>?</td>
<td>79</td>
<td>O</td>
<td>95</td>
<td>_</td>
<td>111</td>
<td>o</td>
<td>127</td>
<td>Delete</td>
</tr>
</tbody>
</table>

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 from 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.
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.
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.

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**

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 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 support@securevoy.com 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.
- 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.
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;

- Follow the previously described install steps, selecting Additional Server (Replica) as shown.

- Once you select Additional Server (Replica) 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 info@securenvoy.com for an immediate response.

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

Note that the Display name and the Account Name are identical.

This is because we only used the First Name field when creating our service account. If we would have used both first and last name fields, the display name would have a space, even though the username would not.
On the Domain Controller, you'll find the ADI Edit tool with the rest of the Administrative Tools.

Make sure your Active Directory is selected.

Locate the Admin$\#\$Id\$r\$h location here, under System.

Add the SecurEnvoy Service Account you had created here.

Once the SecurEnvoy Service Account has been added, highlight the account and click Advanced.
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.
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

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.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>TCP/UDP Port</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Authentication</td>
<td>RADIUS Client Communication (i.e FW, RAS or Application Server with SecurEnvoy Server Agent installed)</td>
<td>UDP/1812</td>
<td>Inbound to SecurAccess Server</td>
</tr>
<tr>
<td>LDAP User Lookup</td>
<td>Communication between SecurAccess and LDAP/AD servers</td>
<td>(LDAP) TCP/389 or LDAPS TCP/636</td>
<td>Inbound to LDAP Server from SecurAccess</td>
</tr>
<tr>
<td>Syslog</td>
<td>Syslog’s pushed to SIEM or Log Collector Solution</td>
<td>UDP/514</td>
<td>Inbound to SIEM Server from SecurAccess</td>
</tr>
<tr>
<td>Replication</td>
<td>Replication connection between one or more SecurAccess Servers</td>
<td>TCP/443</td>
<td>Bidirectional</td>
</tr>
<tr>
<td>Email Enrolments</td>
<td>SMTP connection to mail relay server</td>
<td>TCP/25</td>
<td>Inbound to SMTP Mail Server</td>
</tr>
<tr>
<td>SMS Enrollments and tokens</td>
<td>HTTP connection to public SMS Gateways</td>
<td>TCP/443</td>
<td>Outbound HTTP Access to Public SMS Services</td>
</tr>
<tr>
<td>SecurAccess Portals</td>
<td>Client connectivity to Enrol Tokens, Change Passwords or Helpdesk</td>
<td>TCP/443</td>
<td>Inbound to SecurAccess Server</td>
</tr>
<tr>
<td>Push Authentication (Outbound)</td>
<td>Push Authentication to Mobile Tokens</td>
<td>TCP/443 Apple = TCP/2195</td>
<td>Outbound to gcm-http.googleapis.com Outbound to gateway.push.apple.com Outbound to a.notify.live.net</td>
</tr>
<tr>
<td>Push Authentication (Inbound)</td>
<td>Push Authentication Acceptance from Mobile</td>
<td>TCP/443</td>
<td>Inbound to SecurAccess SECENROL portal (Requires publishing to public Internet via Reverse Proxy)</td>
</tr>
<tr>
<td>Push (Apple Certificate)</td>
<td>Required to update apple.p12 cert on a yearly basis</td>
<td>TCP/443</td>
<td>Outbound to <a href="http://www.securenvoy.com">www.securenvoy.com</a></td>
</tr>
</tbody>
</table>
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
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
USA - Mid West
3333 Warrenville Rd
Suite #200
Lisle, IL 60532

www.securenvoy.com