



# **Sonicwall (SMA) Secure Mobile Access Guide**

**SecurAccess Integration Guide**

# Sonicwall SMA Integration Guide

## Contents

1.1	SOLUTION SUMMARY.....	3
1.2	GUIDE USAGE.....	3
1.3	PREREQUISITES.....	3
1.4	AUTHENTICATION.....	4
1.41	SETUP RADIUS - SECURACCESS.....	4
1.41	SETUP RADIUS - SONICWALL.....	5
1.41	ASSIGN AUTHENTICATION SERVERS TO REALMS.....	8
1.5	CLIENT LOGON.....	9
1.51	CLIENTLESS SSL LOGIN.....	9
1.52	VPN CLIENT LOGIN.....	11

## 1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution integrates with Sonicwall's Secure Mobile Access appliance through the use of RADIUS Server for authorisation and access control.

*The software used for the integration process is listed below:*

Sonicwall SMA 8200v Release 11.4.0-468  
SecurEnvoy SecurAccess Release v9.3.502

## 1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and common to most deployments. It is important to note two things:

- Every organization is different and may require additional or different configuration.
- Some configuration may have other methods to accomplish the same task than those described.

## 1.3 Prerequisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

- A SecurAccess MFA server installed, configured and working on a system with:
  - Windows Server 2003 or higher.
  - An LDAP or Lightweight Directory Service database of users

*Note: Please see SecurEnvoy's SecurAccess version 9.3 deployment guide on how to setup MFA server solution (On the [www.securenvoy.com](http://www.securenvoy.com) website)*
- A Sonicwall SMA virtual or physical appliance running version 11.0 and above, (previous versions of Sonicwall may work but have not been tested with full functionality)
- Sonicwall Connect client software installed/ deployed on all clients that connect remotely to the appliance unless the Clientless solution will be used.
- This guide assumes that Sonicwall has been installed and previously configured to authenticate users with a username and password already.
- Familiarity with the following technologies:
  - RADIUS configuration
  - Sonicwall Administration Interface

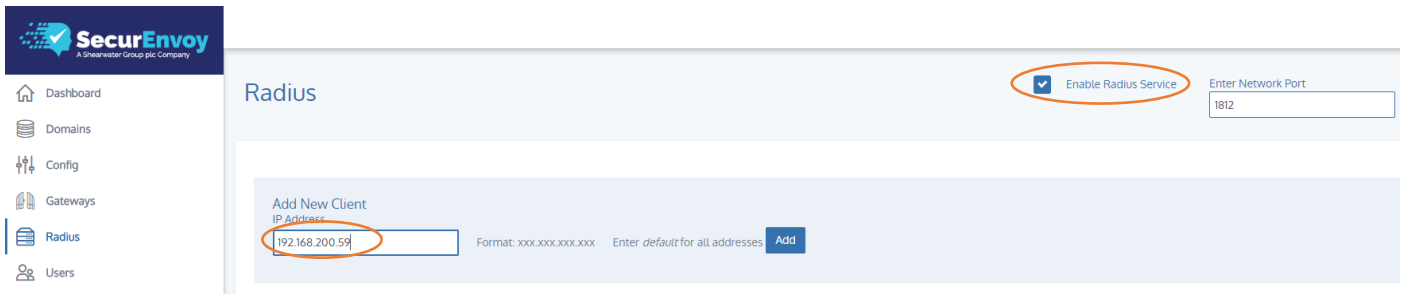
## 1.4 Authentication

The following section describes the steps required to configure the Sonicwall SMA appliance to authenticate users via RADIUS through the SecurEnvoy SecurAccess Solution.

### 1.4.1 Setup RADIUS - SecurAccess

Within the SecurAccess configuration, we will need to configure the Sonicwall appliance as an authorised RADIUS client.

- Navigate to RADIUS in the administrator dashboard.
- Ensure the RADIUS Service is enabled in the top right-hand side of the screen and make sure the port number is left as default 1812.
- Enter the internal IP address of the Sonicwall Appliance and click "Add"



SecurEnvoy  
A Shearwater Group plc Company

Dashboard  
Domains  
Config  
Gateways  
Radius  
Users

Radius

Enable Radius Service

Enter Network Port  
1812

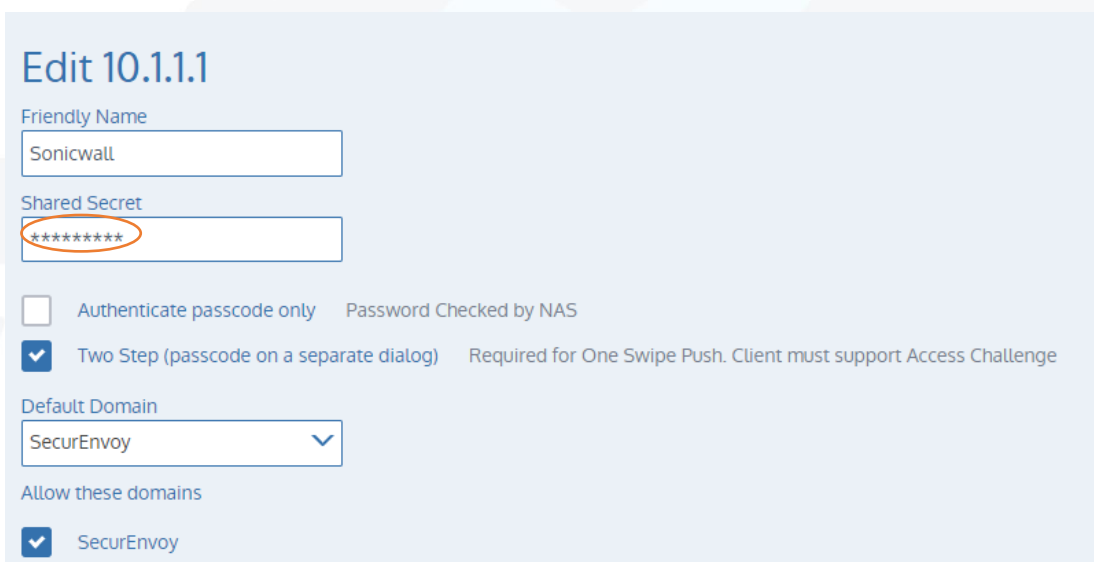
Add New Client

IP Address  
192.168.200.59

Format: xxx.xxx.xxx.xxx Enter default for all addresses

Add

- Enter in a shared secret or common password and select the domains that will be authenticated against (if there is more than one domain configured in SecurAccess)
- Click Update



Edit 10.1.1

Friendly Name  
Sonicwall

Shared Secret  
\*\*\*\*\*

Authenticate passcode only Password Checked by NAS

Two Step (passcode on a separate dialog) Required for One Swipe Push. Client must support Access Challenge

Default Domain  
SecurEnvoy

Allow these domains

SecurEnvoy

## 1.41 Setup RADIUS – Sonicwall

Navigate to System Configuration\Authentication Servers within the Sonicwall administration portal select New, to configure a new Authentication Server.

**Security Administration**

- Access Control
- Resources
- Users & Groups

**User Access**

- Realms
- WorkPlace
- Agent Configuration
- End Point Control

**System Configuration**

- General Settings
- Network Settings
- SSL Settings
- Authentication Servers**
- Services
- Virtual Assist
- Maintenance

**Monitoring**

- User Sessions
- System Status
- Logging
- Troubleshooting

**Authentication Servers**

**Authentication servers**

Authentication servers are referenced by a realm. [New...](#)

<b>SecurEnvoy</b>		<a href="#">Edit</a>   <a href="#">Delete</a>
Type:	RADIUS	
Credentials:	Username/Password	
Uses SSL:	N/A	
Used by realms:	<a href="#">Securlab</a>	

**Other servers**

**RADIUS Accounting** [Edit](#)

Sends accounting information to a RADIUS server for billing purposes.

Enabled:	No	
Primary:	N/A	
Secondary:	N/A	

**One-Time Passwords** [Edit](#)

Sends randomly generated single-use passwords via email to provide two-factor authentication.

SMTP enabled:	No	
SMTP server:	N/A	
SMTP authentication:	Disabled	

09/18

5

Sonicwall SMA Integration Guide  
[www.securenvoy.com](http://www.securenvoy.com)

Select RADIUS from the Authentication Directory list and select Username/Password, from the credentials type.

Click Continue to proceed

### New Authentication Server [Authentication Servers](#) > [New Authentication Server](#)

Choose the protocol used to access your user store, and specify how users will authenticate. Click **Continue** to configure the authentication server.

**User store** \_\_\_\_\_

Choose the directory type or authentication method:

**Authentication directory**

- Dell Defender
- Microsoft Active Directory (Basic) A single domain.
- Microsoft Active Directory (Advanced) Multiple domains in a tree or forest.
- LDAP
- RADIUS**
- RSA Authentication Manager
- Public key infrastructure (PKI)
- SAML 2.0 Identity Provider

**Single sign-on server**

- RSA ClearTrust Sign-on to ClearTrust is supported only from a Web browser.

**Local user storage**

- Local users

**Credential type** \_\_\_\_\_

Specify how users will authenticate:

- Digital certificate
- Token/SecurID
- Username/Password**

Provide the RADIUS configuration with a name, add the IP address of the RADIUS Server, followed by the Shared Secret entered in the previous section and make sure the connection timeout is set to 20 seconds.

Click Save to continue

### Configure Authentication Server Authentication Servers > Configure Authentication Server


Configure authentication settings for a RADIUS server.


**Credential type:** Username/Password

Name:\*

---

**General**

Primary RADIUS server:\*  
 

Secondary RADIUS server:  
 

Shared secret: \*

Match RADIUS groups by:

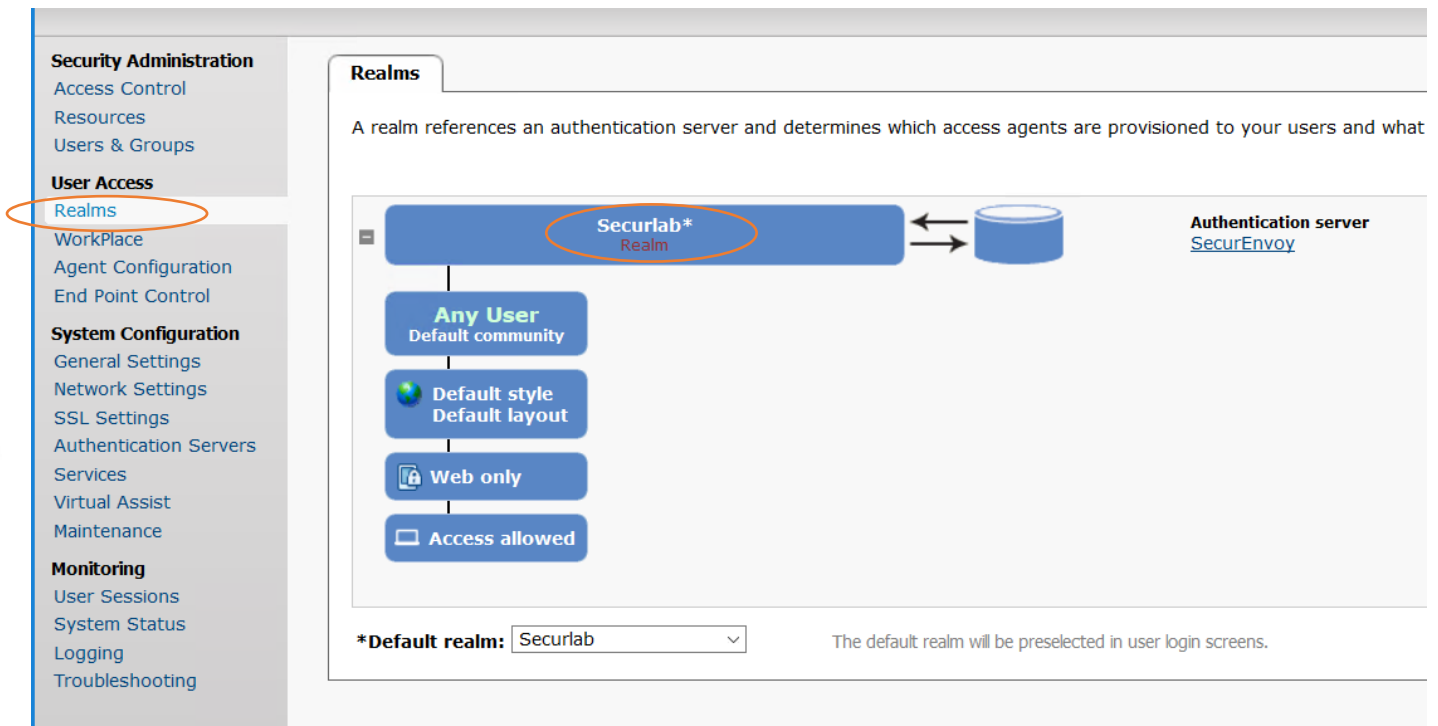
Connection timeout:  seconds When using PhoneFactor, increase this value to give users time to receive the confirmation call.

---

**Advanced** ▼

## 1.41 Assign Authentication Servers to Realms

Navigate to User Access\Realms and select your existing Realm which is likely to have local or AD authentication set.



**Security Administration**  
 Access Control  
 Resources  
 Users & Groups

**User Access**  
**Realms**  
 WorkPlace  
 Agent Configuration  
 End Point Control

**System Configuration**  
 General Settings  
 Network Settings  
 SSL Settings  
 Authentication Servers  
 Services  
 Virtual Assist  
 Maintenance

**Monitoring**  
 User Sessions  
 System Status  
 Logging  
 Troubleshooting

**Realms**

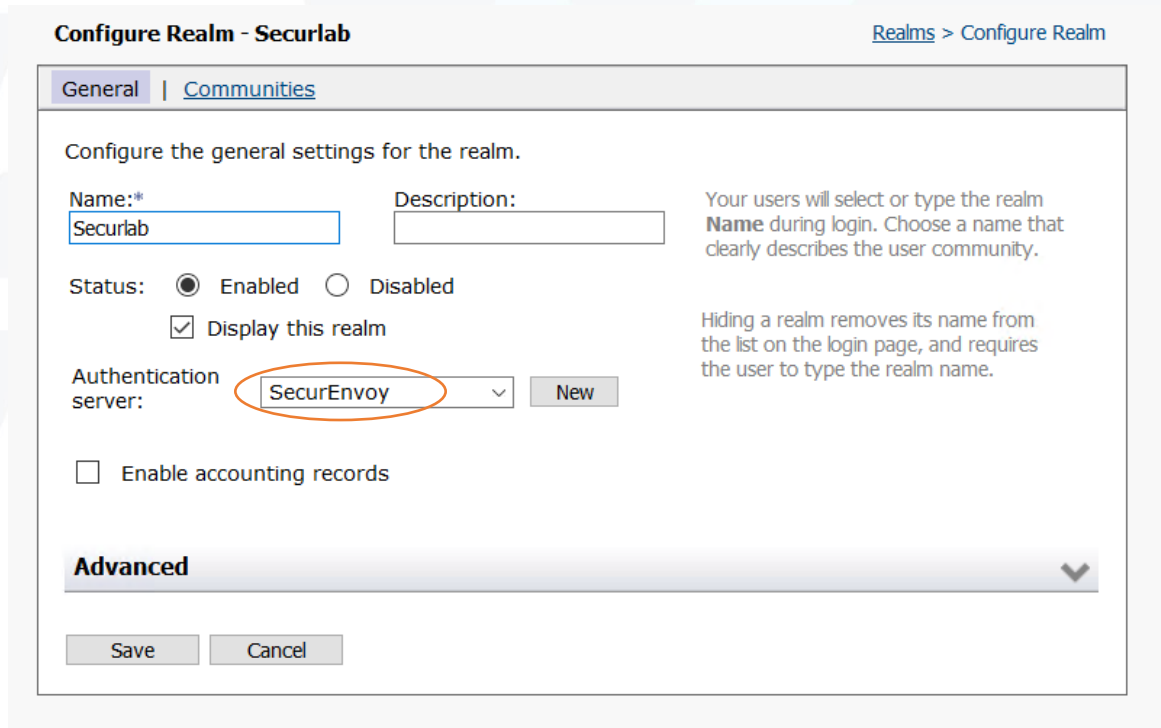
A realm references an authentication server and determines which access agents are provisioned to your users and what

**Securlab\* Realm** ↔ **Authentication server SecurEnvoy**

- Any User  
Default community
- Default style  
Default layout
- Web only
- Access allowed

\*Default realm: Securlab  The default realm will be preselected in user login screens.

Within the Realm, select the Radius Authentication Servers configured in the previous section, from the drop-down list and click Save



**Configure Realm - Securlab** [Realms > Configure Realm](#)

General | [Communities](#)

Configure the general settings for the realm.

Name:\*  Description:

Your users will select or type the realm **Name** during login. Choose a name that clearly describes the user community.

Status:  Enabled  Disabled

Display this realm

Hiding a realm removes its name from the list on the login page, and requires the user to type the realm name.

Authentication server:

Enable accounting records

**Advanced**



## 1.5 Client Logon

### 1.5.1 Clientless SSL Login

The following section describes the login process and demonstrates what will be presented back to the user.

- Browse to your Sonicwall SMA Workspace Login Screen
- Enter in your username from Active Directory or Local Directory Service account
- Enter your domain password and click Login In



**Please log in**

Log in here to establish a secure connection to your network resources.

Username:

Password:

© 2016 Dell

When prompted, enter the 6-digit token or yubikey token and click ok



**Please log in**

Log in here to establish a secure connection to your network resources.

Enter Your 6 Digit Code or Yubikey

© 2016 Dell





[Log out](#) | [Help](#) | [Details](#)

Access: [Web](#) User: [dclare-enrol](#) Session start: [16:38](#)

**Home**

To access a resource, click its name from the list below.

 **Network Explorer**  
Browse a Windows network containing shared files and folders.

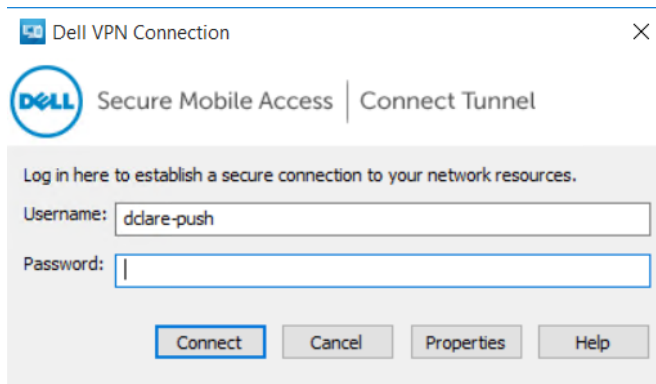
 **Install Connect Tunnel**  
Get the latest version of Connect Tunnel.

**Intranet Address:**   [Help](#)

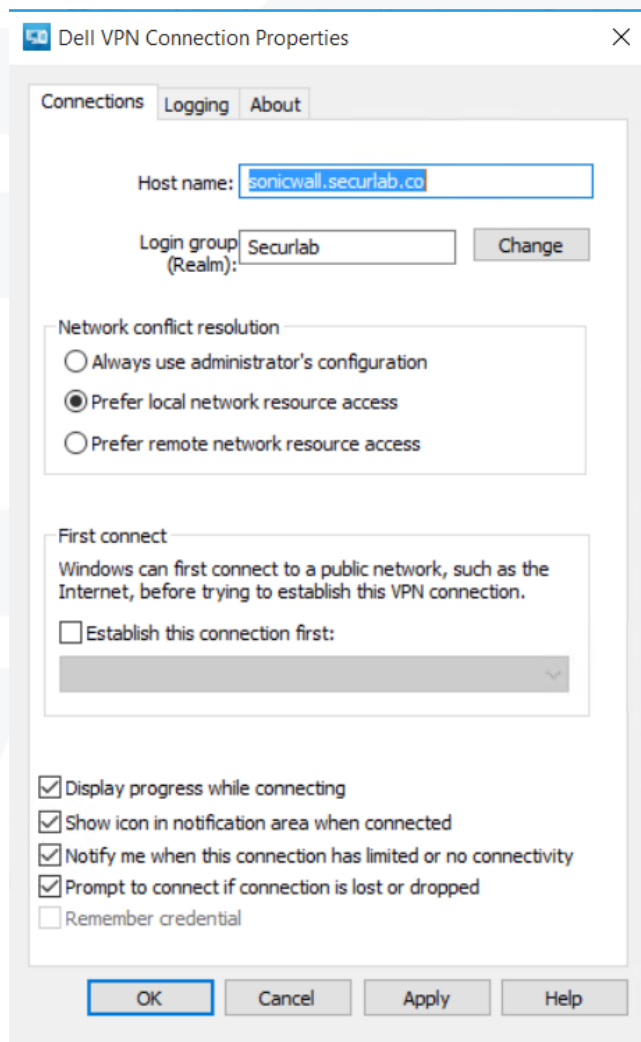
© 2016 Dell

## 1.52 VPN Client Login

Load the Secure Mobile Access client and select Properties

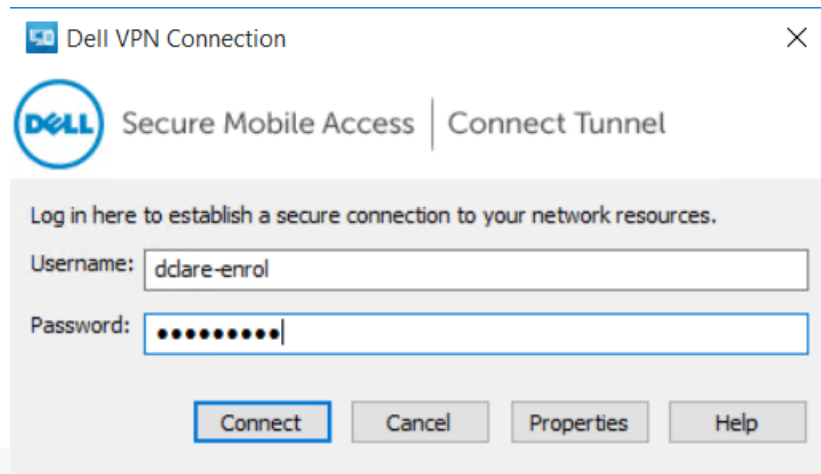


On presentation of the properties of the client, make sure that the hostname or IP address of the External interface of the Sonicwall SMA is set, along with the Login Group Realm (Configured under the authentication section).  
Click Apply and close the dialogue.



The following section describes the login process and demonstrates what will be presented back to the user.

- Enter in your username from Active Directory or Local Directory Service account
- Enter your domain password and click Connect



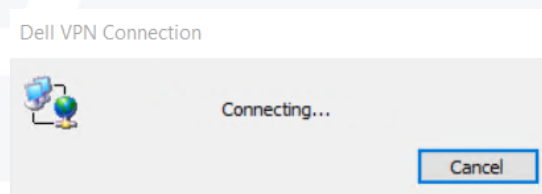
Dell VPN Connection

**DELL** Secure Mobile Access | Connect Tunnel

Log in here to establish a secure connection to your network resources.

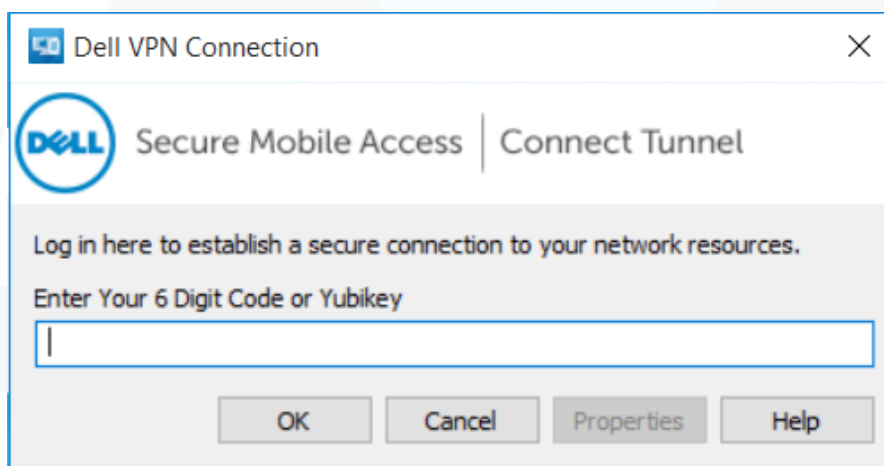
Username:

Password:



Dell VPN Connection

When prompted, enter the 6-digit token or yubikey token and click ok



Dell VPN Connection

**DELL** Secure Mobile Access | Connect Tunnel

Log in here to establish a secure connection to your network resources.

Enter Your 6 Digit Code or Yubikey

# Please Reach Out to Your Local SecurEnvoy Team...



## UK & IRELAND

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

### Sales

E [sales@SecurEnvoy.com](mailto:sales@SecurEnvoy.com)  
T 44 (0) 845 2600011

### Technical Support

E [support@SecurEnvoy.com](mailto:support@SecurEnvoy.com)  
T 44 (0) 845 2600012



## EUROPE

Freibadstraße 30,  
81543 München,  
Germany

### General Information

E [info@SecurEnvoy.com](mailto:info@SecurEnvoy.com)  
T +49 89 70074522



## ASIA-PAC

Level 40 100 Miller Street  
North Sydney  
NSW 2060

### Sales

E [info@SecurEnvoy.com](mailto: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](mailto:info@SecurEnvoy.com)  
T (866)777-6211



## USA - Mid West

3333 Warrenville Rd  
Suite #200  
Lisle, IL 60532

### General Information

E [info@SecurEnvoy.com](mailto:info@SecurEnvoy.com)  
T (866)777-6211



## USA - East Coast

373 Park Ave South  
New York,  
NY 10016

### General Information

E [info@SecurEnvoy.com](mailto:info@SecurEnvoy.com)  
T (866)777-6211



A Shearwater Group plc Company

[www.securenvoy.com](http://www.securenvoy.com)