

# **Ericom AccessNow**

# Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information				
SecurEnvoy	www.securenvoy.com	0845 2600010		
	Merlin House			
	Brunel Road			
	Theale			
	Reading			
	RG7 4AB			
Tony Davis	tdavis@securenvoy.com			

**Ericom AccessNow Integration Guide** 



This document describes how to integrate Ericom AccessNow with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Ericom AccessNow is the market's first high performance HTML5 RDP Client, providing browser access to Windows applications and desktops (virtual & physical), running on Windows Terminal Services / RDS / VDI platforms, including Microsoft Hyper-V and other hypervisors

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as AccessNow), without the complication of deploying hardware tokens or smartcards. Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP server and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing LDAP password. Utilizing the LDAP password as the PIN, allows the User to enter their UserID, Domain password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. It provides a seamless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilizes a web GUI for configuration. All notes within this integration guide refer to this type of approach.

### The equipment used for the integration process is listed below:

### Ericom AccessNow

Microsoft Server 2008 R2 Ericom AccessNow

### SecurEnvoy

Microsoft Server 2008 R2 IIS installed with SSL certificate (required for management and remote administration) Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v7.2.505

### Index

1.0	Prerequisites	3
1.1	Configure the Microsoft Server Agent for Default website	4
1.2	Configure the Microsoft Server Agent for AccessNow	5



2.0	Configure logout URL	6
2.1	Configure AccessNow Template	. 7
2.2	Configure AccessNow Logoff and redirect	. 7
3.0	Test the Two Factor Authentication	. 8
4.0	Notes	10

# 1.0 Prerequisites

It is assumed that the Ericom AccessNow has been installed and is authenticating with a username and password.

Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory. If firewalls are between the SecurEnvoy Security server, Active Directory servers, and the AccessNow server(s), additional open ports will be required.

Microsoft Server Agent has been installed as per the SecurEnvoy Microsoft Server Agent and Admin Guide:

https://www.securenvoy.com/integrationguides/iis%20agent%20installation%20guide.pdf



You MUST install the Microsoft Server Agent version 7.3 or higher

The following table shows what token types are supported.

Token Type Supported			
Real Time SMS or Email	$\checkmark$		
Preload SMS or Email	$\checkmark$		
Soft Token Code	$\checkmark$		
Soft Token Next Code	$\checkmark$		
Voice Call	$\checkmark$		



## **1.1** Configure the Microsoft Server Agent for Default website

Launch the IIS management interface, either from "Start", "Administration Tools" or from the Server Manager

Expand the sites list on the navigation pane and select "Default Web Site", then scroll down the centre panel and press the "SecurEnvoy Two Factor" icon.

Q Def	ault Web	Site Home	e			
Filter:		- 🗿 Go - 🔽	Show All G	oup by: Area		-
IIS						
	CGI	-	0		404	
Authentication	CGI	Compression	Default Document	Directory Browsing	Error Pages	Handl Mappir
	<b>F</b>	and the second s		8	9	
Logging	MIME Types	Modules	Output Caching	Request Filtering	SSL Settings	
Manageme	nt					
Configuration Editor						
Other						
R						
SecurEnvoy Two Factor						
	Def Filter: II5 Authentication Logging Manageme Configuration Editor Other Other Securitary Wro Factor	Default Web	Default Web Site Hom         Fiter:       Image: Compression         IIS       Image: Compression         Authentication       CGI       Compression         Logging       Image: Compression       Image: Compression         Logging       Image: Compression       Image: Compression         Configuration       Editor       Modules         Other       Image: Compression       Image: Compression         Secure: Envoy       Two Factor       Image: Compression	Default Web Site Home         Fiter:          •          •          •	Default Web Site Home         Filter:	Default Web Site Home         Fiter:          •          •          •



Enable the tick box to "Enable Authentication On Site Default Web Site"

Click "Apply" when complete.

SecurEnvoy Two Factor Authentication	
Enable Authentication On Default Web Site	
Protect All Resources On Site Default Web Site     Forms Based Authentication     HTTP Basic Authentication	
Apply Cancel	
	Enable Authentication On Default Web Site     Protect All Resources On Site Default Web Site     Forms Based Authentication     C HITTP Basic Authentication

# 1.2 Configure the Microsoft Server Agent for AccessNow

Select the virtual web site you want to protect. For AccessNow select "AccessNow", scroll down the centre panel and select "SecurEnvoy Two Factor"





Select the tick box "Enable Authentication On / AccessNow" Select "Form Based Authentication" (The Default) Click "Apply" to finish Cancel restart IIS when prompted.



# 🗹 Note

The virtual directory SecurEnvoyAuth is automatically set to the application pool "DefaultAppPool". This must be maintained for correct operation.

# 2.0 Configure logout URL



In the Navigation pane, select top level host name (the 2nd line down). Scroll down the centre panel and press the "SecurEnvoy Two Factor" icon.

Setup your required inactivity timeout.

Add the logout URL logoff.htm

ile View Help	
ansttoine Sant Tage Acciliant Ford Acciliant Ford Defail Web Ste Defail	SecurEnvoy Two Factor Authentication         Authentication Timeout (munices) [50         C Treacut innuctivity @ Timeout after list auth Overdite reduced hostsmane with[

Restart IIS when prompted.

# 2.1 **Configure** AccessNow Template

Copy the contents of AccessNow (C:\Program Files (x86)\SecurEnvoy\Microsoft Server Agent\SAMPLES) to

 $\label{eq:WEBAUTHTEMPLATE (C:\Program Files (x86)\SecurEnvoy\Microsoft Server Agent), backing up existing files.$ 

# 2.2 Configure AccessNow Logoff and redirect

Create `logoff.htm' within the following directory `C:\Program Files (x86)\Ericom Software\Ericom AccessNow Web Component" and add the following code:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<script language="javascript" >
function load() {
window.location.href = window.location.protocol+"//"+window.location.host+"/accessnow/";
}
</script>
</head>
<body onload="load();" >
Logoff successful.
</body>
</html>
```

Open `config.js' (``C:\Program Files (x86)\Ericom Software\Ericom AccessNow Web Component") and navigate to line 39. Uncomment and change to the following:

endURL: "http://yourservername/accessnow/logoff.htm",



# 3.0 Test the Two Factor Authentication

Test the Two Factor Web authentication by opening a browser and going to the URL for the Web server i.e.

https://your\_server\_name/accessnow (Don't forget the https)

User logon screen is	SecurEnvoy Tokenless Two F ×	- • X
snown.	← → C ㎡ 🗋 127.0.0.1/accessnow	ର 🏠 🔳
Enter your UsedID and Password:	SecurEnvoj	
	SecurEnvoy Tokenless Authentication One Swipe	
	Enter UserID.	
	Enter Pin or Windows Password:	
	Ericom Access Server: Leave empty if some as Web Server	
	RDP Host: Leave empty if same as Access Server	
	Domain: domain on host	
	Compression and Acceleration: 🗹	
	Acceleration / Quality: Very Fast / Good Quality (Recommended) 🔻	
	Screen resolution: Fit to browser window	
	Login Manage My Token	
	Consultation Distantiand Tolescher Turn Contro Automational	
	Securiting Faterade rokeness monación Adriaticaduri	

User is then presented with their two factor authentication type:

•	<ul> <li>Pre load, Realtime and Soft tokens:</li> </ul>	SecurEnvoy Tokenless Authentication
		Enter Your 6 Digit Passcode
•	VOICE tokens:	SecurEnvoy Tokenless Authentication
		Answer Phone, Passcode 794850, Then Login
•	One Swipe:	
		One-Swipe



User authenticates successfully and is presented with AccessNow:



## 🗹 Note

Configure your domain name within seiis.ini (C:\Windows):

# Default Domain Name to use if no domain information is included in this UserID (leave blank if not required) DefaultDomain="yourdomain"

This will allow your users to logon to AccessNow without specifying the domain name: domain\UserID



4.0 Notes