

**External Authentication with Windows 2008R2 Server  
with Remote Desktop Web Gateway**

**Authenticating Users Using SecurAccess Server by  
SecurEnvoy**

<b>Contact information</b>		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Andy Kemshall	akemshall@securenvoy.com	

## Windows 2008R2 Server with Remote Desktop Web Gateway Integration Guide

This document describes how to integrate a Windows 2008 R2 Remote Desktop Web (RDWeb) Gateway installed with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Microsoft Windows 2008R2 Remote Desktop provides Web based Secure Application Access to the internal corporate network.

Connections to Remote Desktop must be made from a browser and not directly from a terminal server client.

### Note

**This document relates only to RDWeb access. If you want to authenticate Remote Desktop Client connections as well you will need to install Windows Login Agent on the Terminal Server hosts instead of this solution: see <http://www.securenvoy.com/integrationguides/Windows%20Login%20Agent.pdf>**

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Microsoft), 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 Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed via the SecurEnvoy IIS Web Agent via the HTTP protocol (authentication packet is encrypted by AES 128bit) to the SecurEnvoy server where it carries out a Two-Factor authentication. It provides a seamless login into the Windows 2008R2 Remote Desktop environment by entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, whereas the Microsoft Windows Server environment uses a GUI application. All notes within this integration guide refer to this type of approach.

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

#### Microsoft Windows Server 2008R2

Installed roles:

Remote Desktop Services

#### SecurEnvoy

SecurAccess Server software release v5.2.501

IIS Web Agent V5.3.501

### Note

**You must use IIS Agent version 5.3.501 or higher**  
**You must use Security Server version 5.2.500 or higher**

## Contents

1.0	Pre Requisites.....	4
2.0	Configuration of Remote Desktop Gateway Server .....	4
2.1	Configure IIS to protect Rpc and RDWeb.....	4
2.2	RemoteApp Manager Configuration .....	7
2.3	Setting Up Single Sign-On .....	8
3.0	Configuration of SecurEnvoy Server .....	8
4.0	Test Logon .....	9

### 1.0 Pre Requisites

*It is assumed that Remote Desktop Services has been installed upon the relevant server(s). An existing Domain user can authenticate using a windows user name and domain password and access applications. All communications are over HTTPS (port 443) for client browser to /RDWeb.*

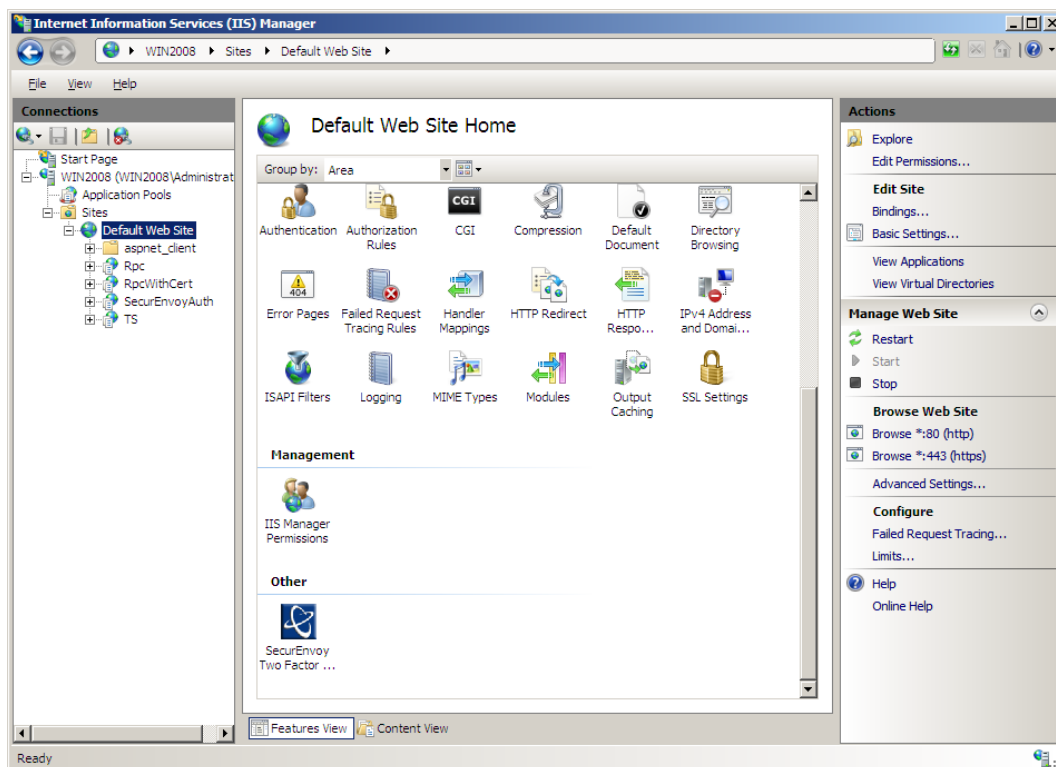
#### Note

**You must use SecurEnvoy IIS Agent version 5.3.501 or higher**  
**You must use SecurEnvoy Security Server version 5.2.500 or higher**

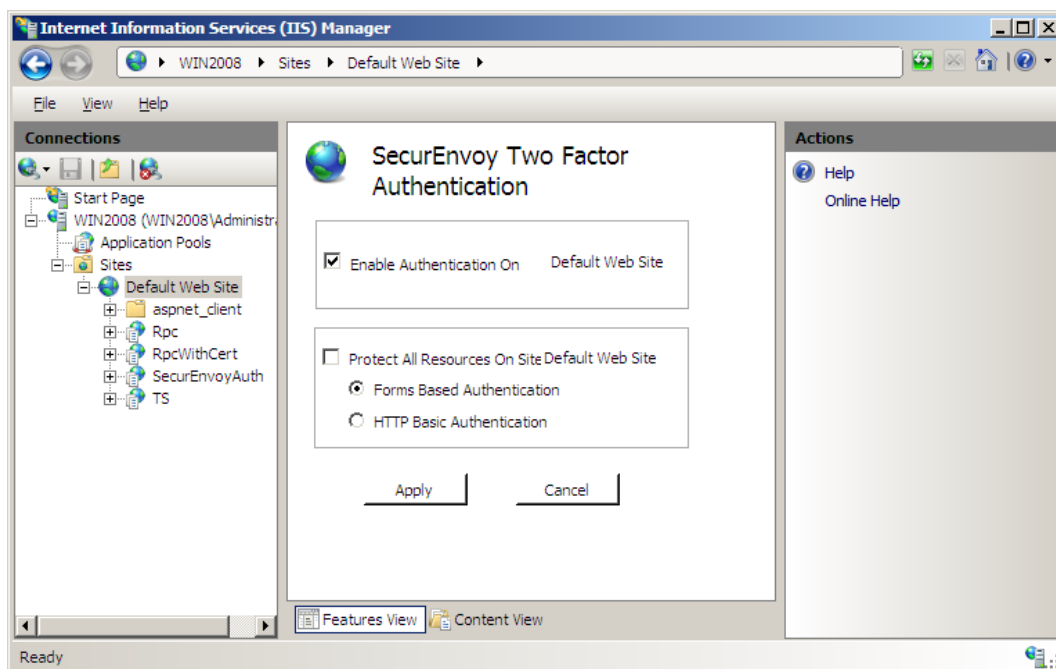
### 2.0 Configuration of Remote Desktop Gateway Server

#### 2.1 Configure IIS to protect Rpc and RDWeb

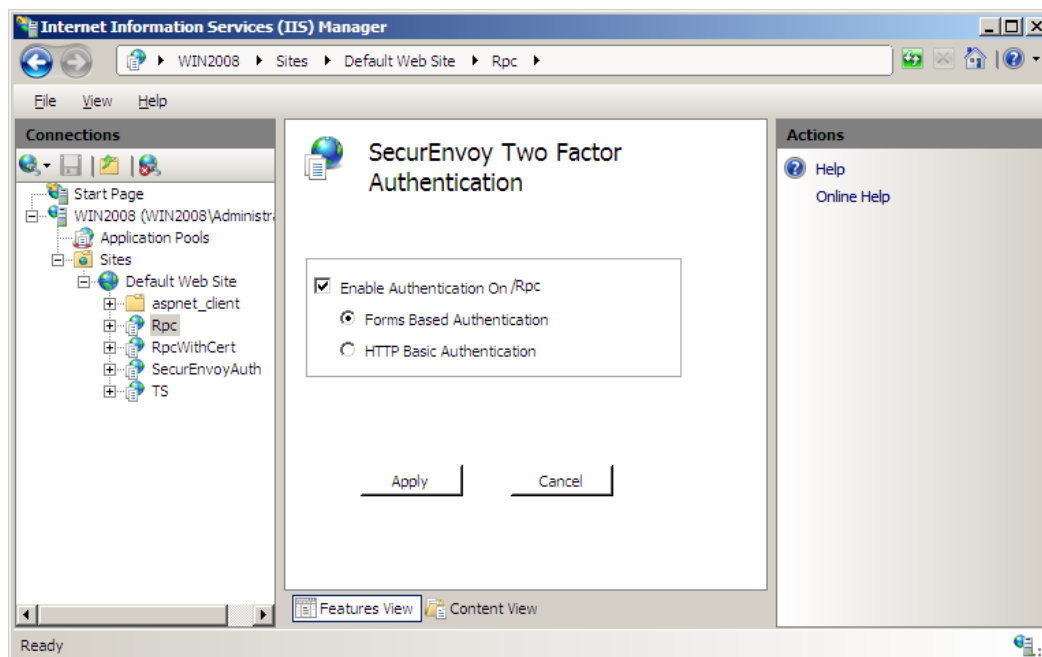
- a. Install SecurEnvoy IIS Web Agent v5.2.501 or higher on the remote desktop gateway server that hosts the IIS virtual directory "RDWeb"
- b. Start IIS Manager
- c. Select Default web site under connections pane.
- d. Select the SecurEnvoy Icon



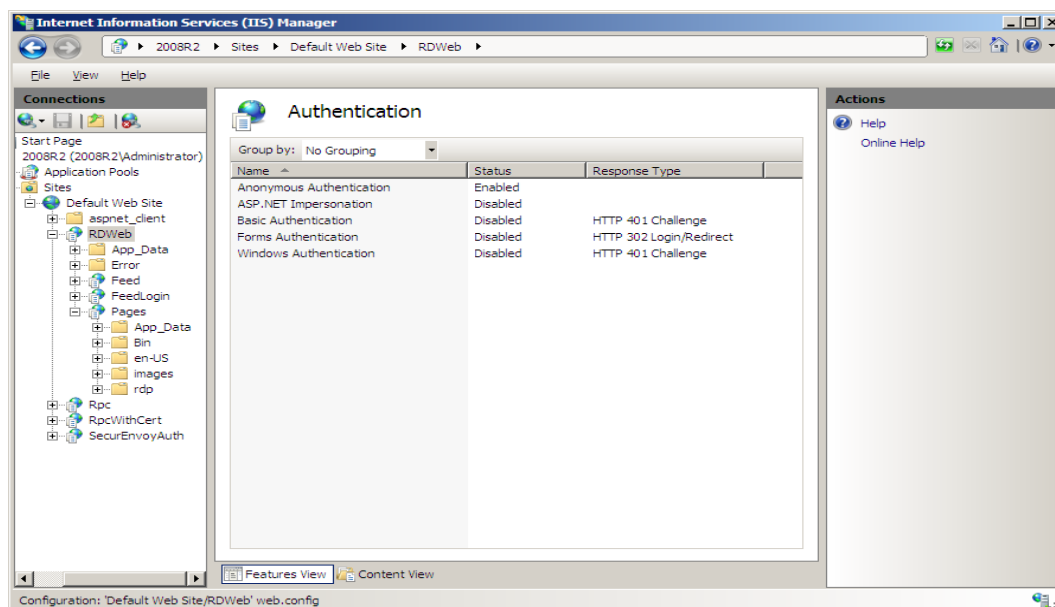
e. Select **Enable Authentication On Default Web Site**.



- f. Apply changes
- g. Select **Rpc** under **Default Web Site**
- h. Select the SecurEnvoy Icon
- i. Select the check box **Enable Authentication On /Rpc**



- j. Cancel IIS Restart
- k. Select **RDWeb** under **Default Web Site**
- l. Select the SecurEnvoy Icon
- m. Select the check box **Enable Authentication On /RDWeb**
- n. Apply and Restart IIS
- o. Navigate back to **Default Web Site > RDWeb** and select the Authentication icon
- p. Disable Basic Authentication
- q. Make sure that only **Anonymous Authentication** is Enabled

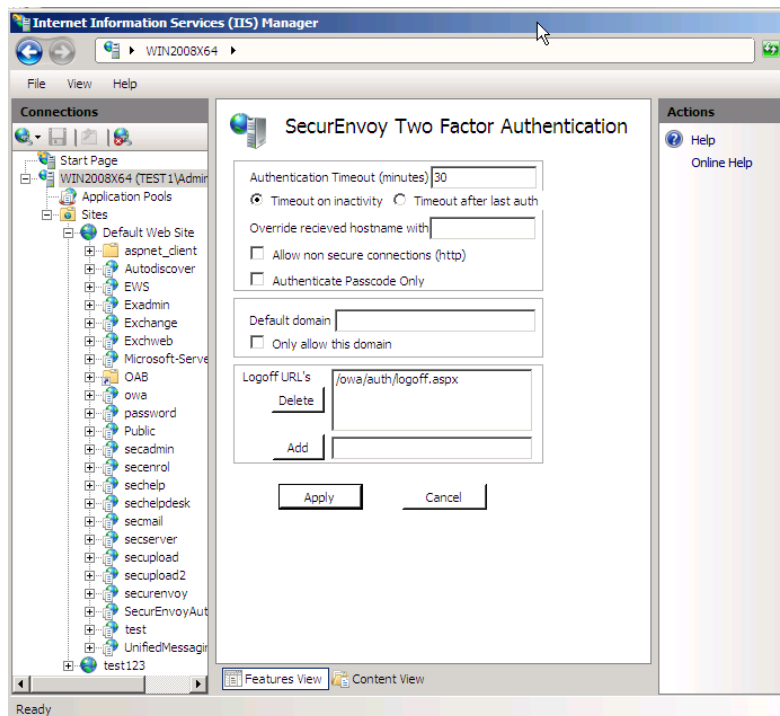


- r. Check **SecurEnvoyAuth** is a member of the application pool **RDWebAccess** this should be the case if you protected **RDWeb** last

**Note**

**SecurEnvoyAuth MUST be a member of the RDWebAccess Application Pool**

In the Navigation pane, select top level host name (the 2<sup>nd</sup> line down).  
 Scroll down the centre panel and press the "SecurEnvoy Two Factor" icon.  
 Setup your required inactivity timeout.  
 Add the logout URL **/owa/auth/logoff.aspx**  
 Restart IIS when prompted.

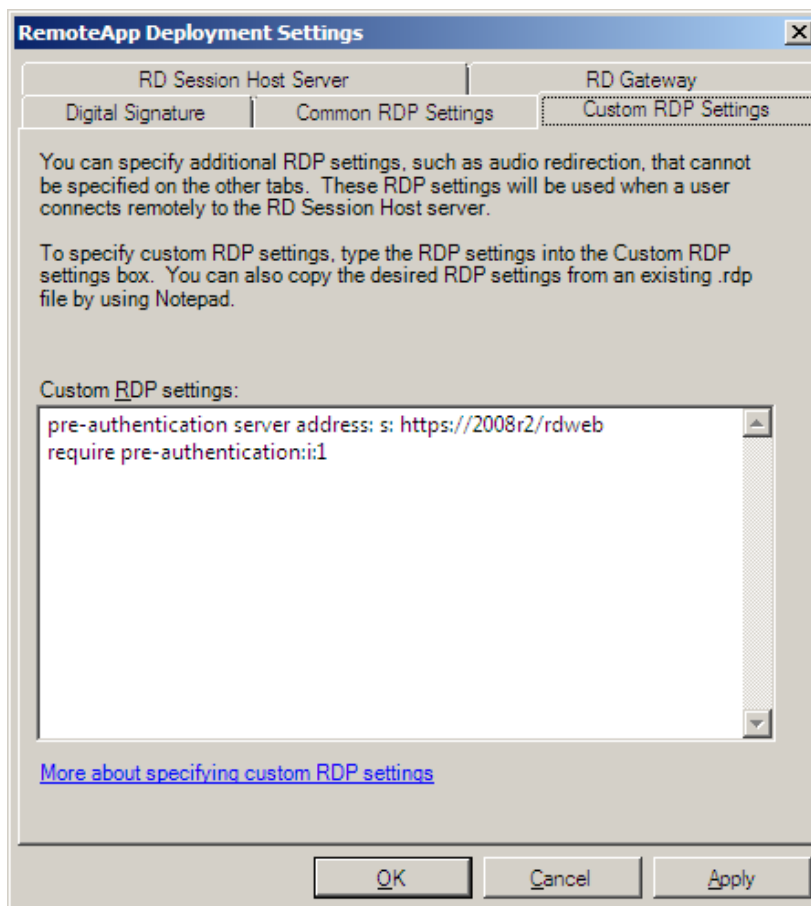


## 2.2 RemoteApp Manager Configuration

- Click Start > Administrative Tools > Remote Desktop Services > RemoteApp Manager.
- In the Overview pane of RemoteApp Manager, next to RDP Settings, click Change.
- On the Custom RDP Settings tab, type or copy the following RDP settings into the Custom RDP settings box:

```
pre-authentication server address: s: https://<hostname>/rdweb
require pre-authentication:i:1
```

**Note:** <hostname> should be replaced with the external name of the RDWeb server (i.e. The name that the browser will use).



e. When you have finished adding the settings, click **Apply**

## 2.3 Setting Up Single Sign-On

Change directory to C:\Program Files (x86)\SecurEnvoy\Microsoft IIS Agent\SAMPLES\RemoteDesktop2008R2

Copy passcodeok.htm, auth.htm and accessdenied.htm ..\..\WEBAUTHTEMPLATE\

copy logoff.aspx to \windows\Web\RDWeb\Pages\en-US\logoff.aspx

(See readme.txt for details)

## 3 Configuration of SecurEnvoy Server

For single-signon to work the SecurEnvoy server must be configured to use LDAP password as the PIN (This is the default)

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

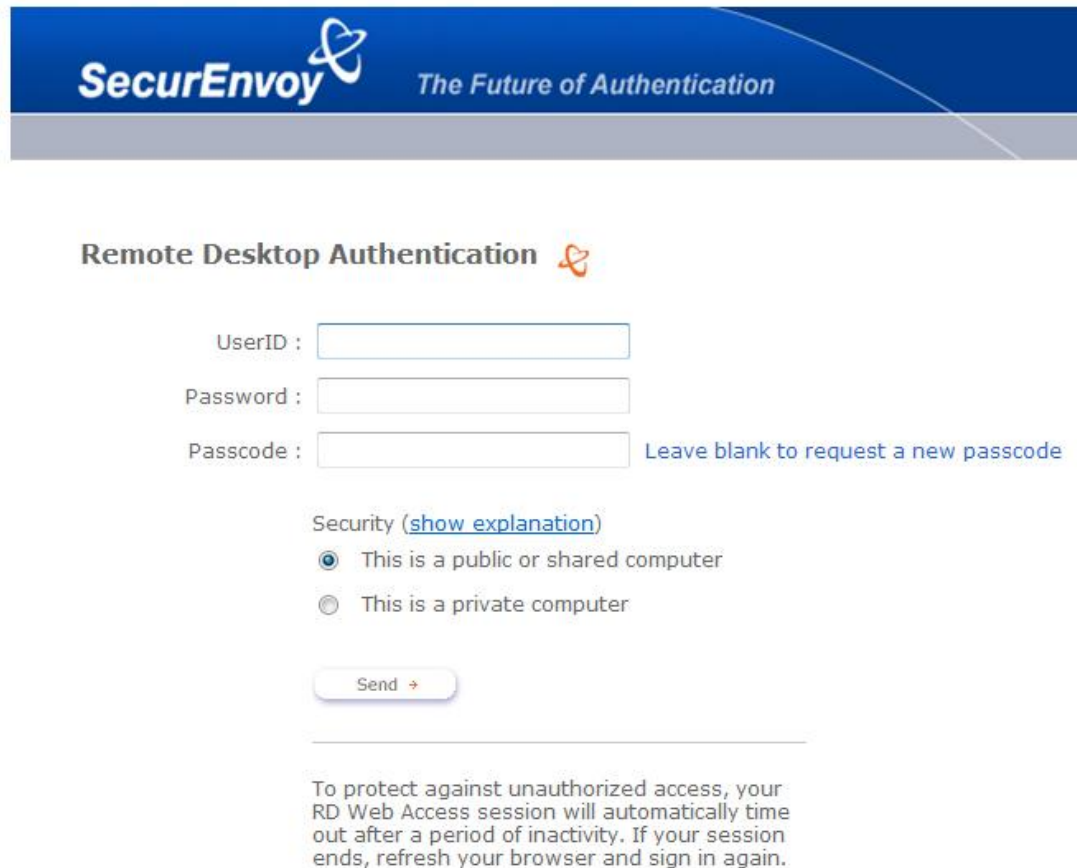
Click **"Config"**

Select LDAP Password is the PIN under PIN Management (This is the default setting)

Click **"Update"** to confirm the changes

## 4.0 Test Logon

Open a browser and navigate to *https://machine.domain.com/RDWeb*



The screenshot shows the SecurEnvoy Remote Desktop Authentication interface. At the top is a blue header with the SecurEnvoy logo and the tagline "The Future of Authentication". Below this is the title "Remote Desktop Authentication" with a small SecurEnvoy icon. The form contains three input fields: "UserID", "Password", and "Passcode". To the right of the "Passcode" field is the text "Leave blank to request a new passcode". Below the input fields is a "Security" section with a link "(show explanation)". There are two radio button options: "This is a public or shared computer" (which is selected) and "This is a private computer". A "Send" button with a right-pointing arrow is located below the radio buttons. At the bottom of the form, there is a disclaimer: "To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again." At the very bottom of the page, there is a dark blue footer with the text "Copyright ©, SecurEnvoy. Patent pending EP1387239" on the left and "Powered by SecurEnvoy" on the right.

- Enter Domain Username in the UserID field
- Enter Domain Password in the Password field.
- Enter SMS passcode (received upon mobile phone) in the Passcode field
- Select your Security Option
- Click "Send"
- Once logged on will be single signed onto the RDWeb access page



**Note**

**You will be prompted for a domain login when you access any application.**