External Authentication with Windows 2008 Server with Terminal Server Web Gateway

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Andy Kemshall	akemshall@securenvoy.com	
Date	19th November 2009	

Windows 2008 Server with Terminal Server Web Gateway Integration Guide

This document describes how to integrate a Windows 2008 or 2008 R2 (32bit and 64bit) Terminal Server Web (TSWeb) Gateway installed with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Microsoft Windows 2008 Terminal Server provides Web based Secure Application Access to the internal corporate network.

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

> **Note**
>
> **This document relates only to TSWeb access. If you want to authenticate Remote Desktop Client connections as well you should 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 seemless login into the Windows 2008 Terminal Server 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 2008
Installed roles:
Microsoft Terminal Server
Microsoft Terminal Server Gateway

SecurEnvoy
SecurAccess Server software release v5.2.501
IIS Web Agent V5.2.501

> **Note**
>
> **You must use IIS Agent version 5.2.501 or higher**
> **You must use Security Server version 5.2.500 or higher**

© 2005 SecurEnvoy Ltd. All rights reserved

Contents

1.0 Pre Requisites 3
2.0 Configuration of Terminal Server 3
2.1 Configure IIS to protect Rpc and TS 3
2.2 TS RemoteApp Configuration 5
3.0 Configuration of SecurEnvoy Server 7
4.0 Test Logon 8

1.0 Pre Requisites

It is assumed that Terminal Server and Terminal Server Gateway 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 and TSWeb server.

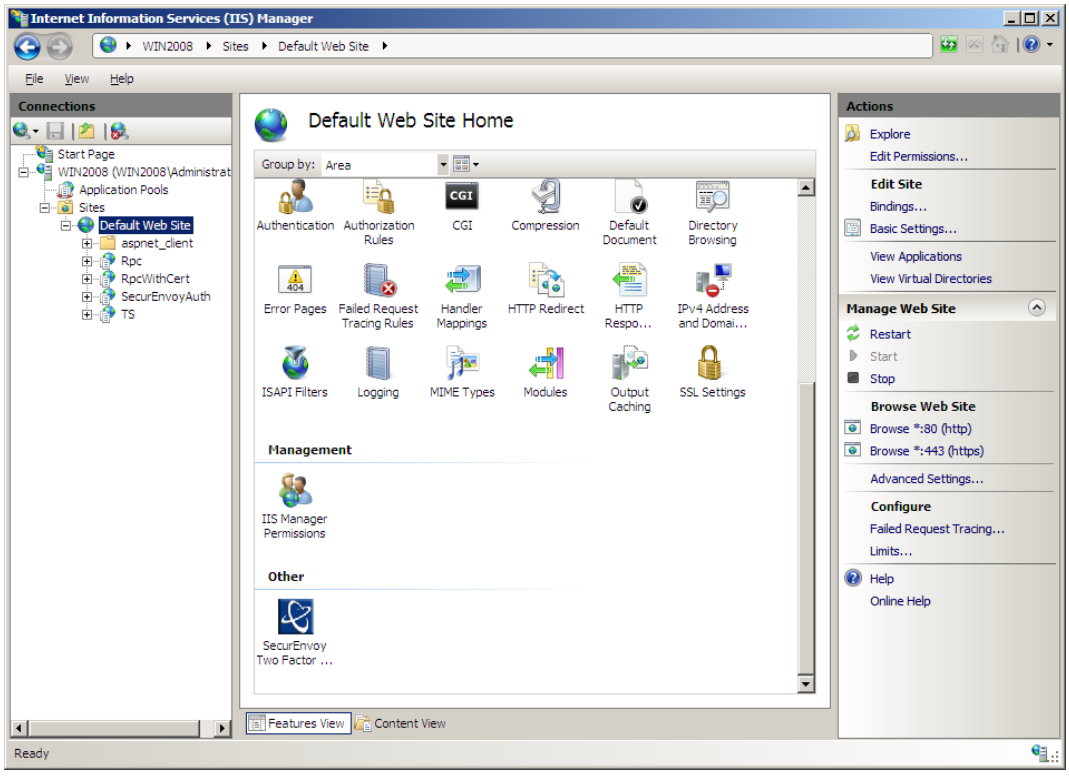
> **Note**
>
> **You must use SecurEnvoy IIS Agent version 5.2.501 or higher**
> **You must use SecurEnvoy Security Server version 5.2.500 or higher**

2.0 Configuration of Terminal Server

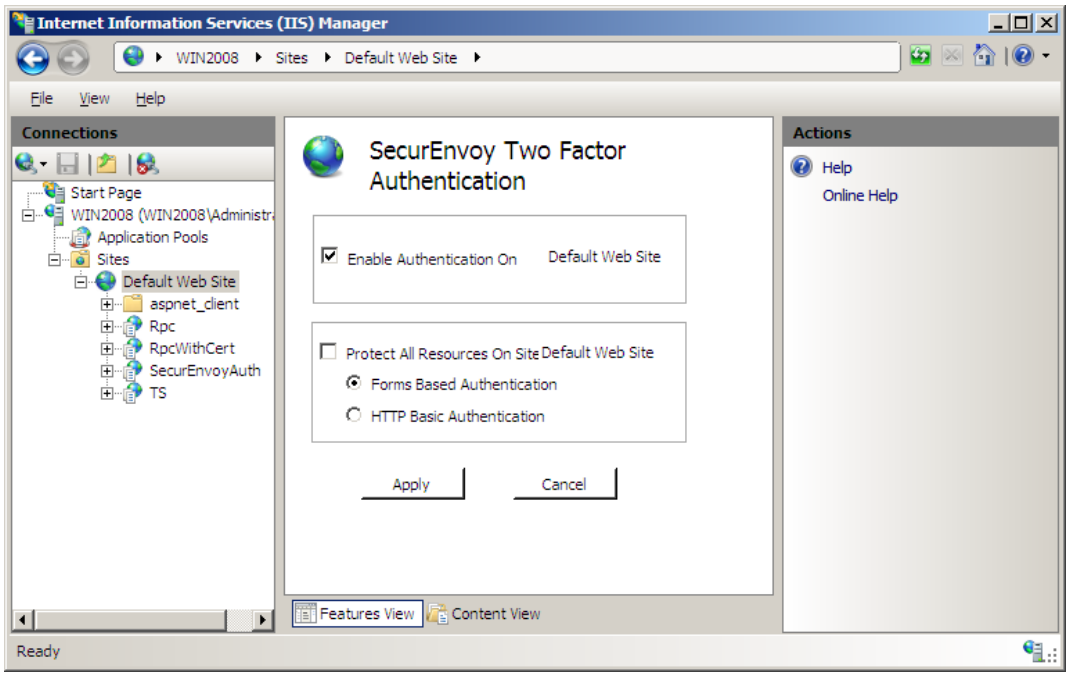
2.1 Configure IIS to protect Rpc and TS

a. Install SecurEnvoy IIS Web Agent v5.2.501 or higher on the TSWeb Access host
b. Start IIS Manager
c. Select Default web site under connections pane.
d. Select the SecurEnvoy Icon

© 2005 SecurEnvoy Ltd. All rights reserved

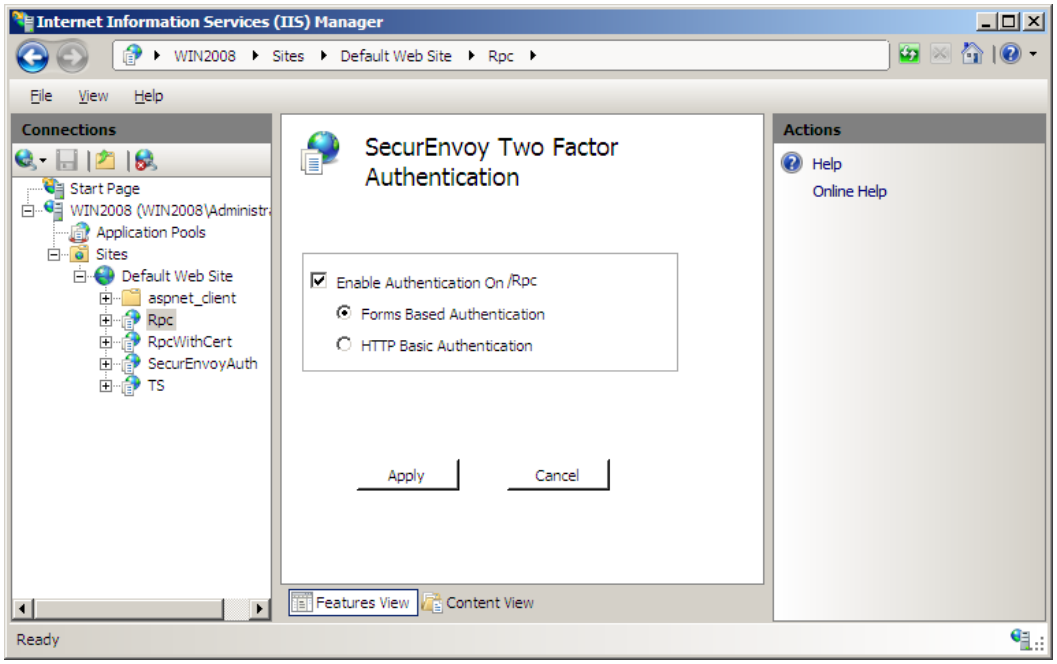


e. Select **Enable Authentication On Default Web Site.**

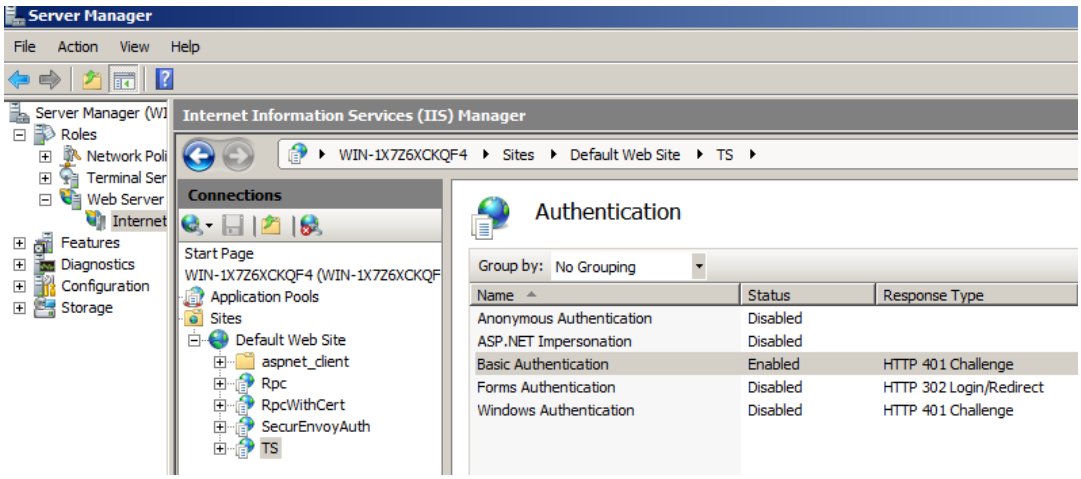


f. Apply changes
g. Select **Rpc** under **Default Web Site**
h. Select the SecurEnvoy Icon
i. Select the check box **Enable Authentication On /Rpc**

© 2005 SecurEnvoy Ltd. All rights reserved



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



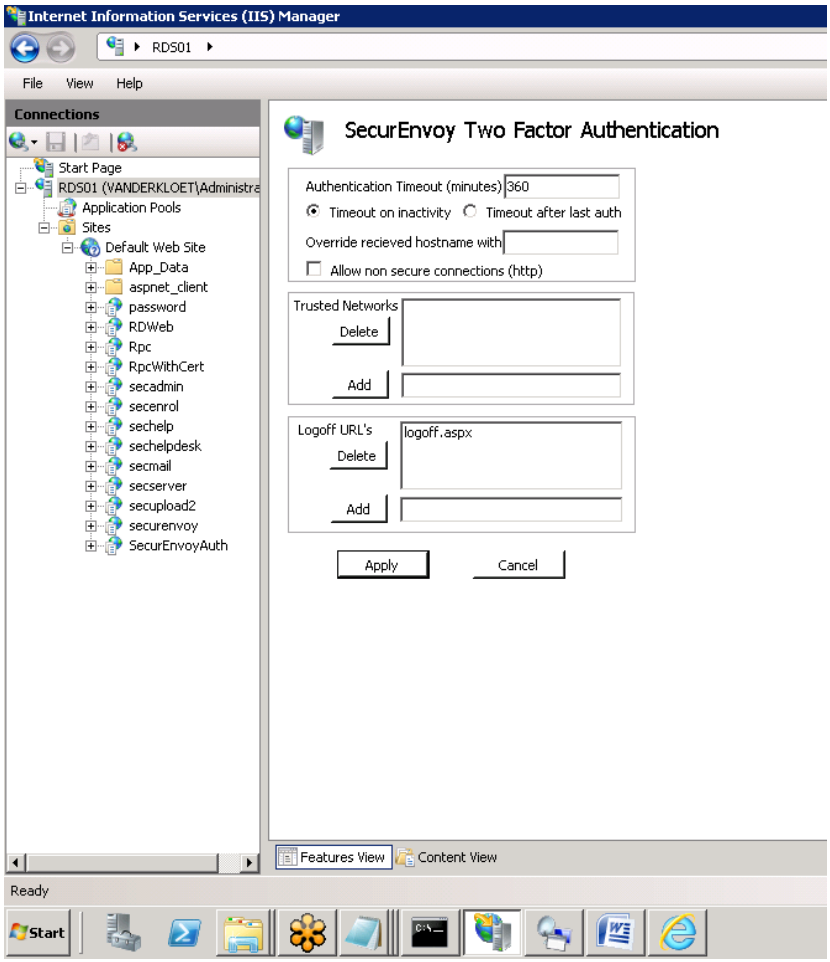
q. Check **SecurEnvoyAuth** is a member of the application pool **TSWebAcess** this should be the case if you protected **TS** last

Note

SecurEnvoyAuth MUST be a member of the TSWebAccess Application Pool

© 2005 SecurEnvoy Ltd. All rights reserved

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.aspx** (enter logoff.aspx right of the Add button and press Add)
Restart IIS when prompted.



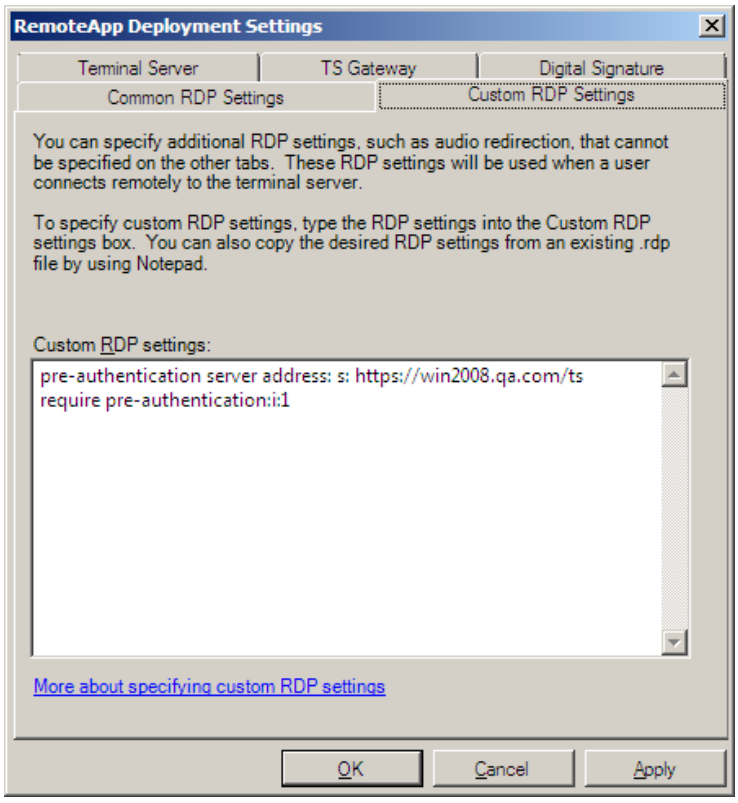
© 2005 SecurEnvoy Ltd. All rights reserved

2.2 TS RemoteApp Configuration

a. Click Start > Administrative Tools >Terminal Services >TS RemoteApp Manager.
b. In the Overview pane of TS RemoteApp Manager, next to RDP Settings, click Change.
c. 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>/ts
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**

3.0 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"**

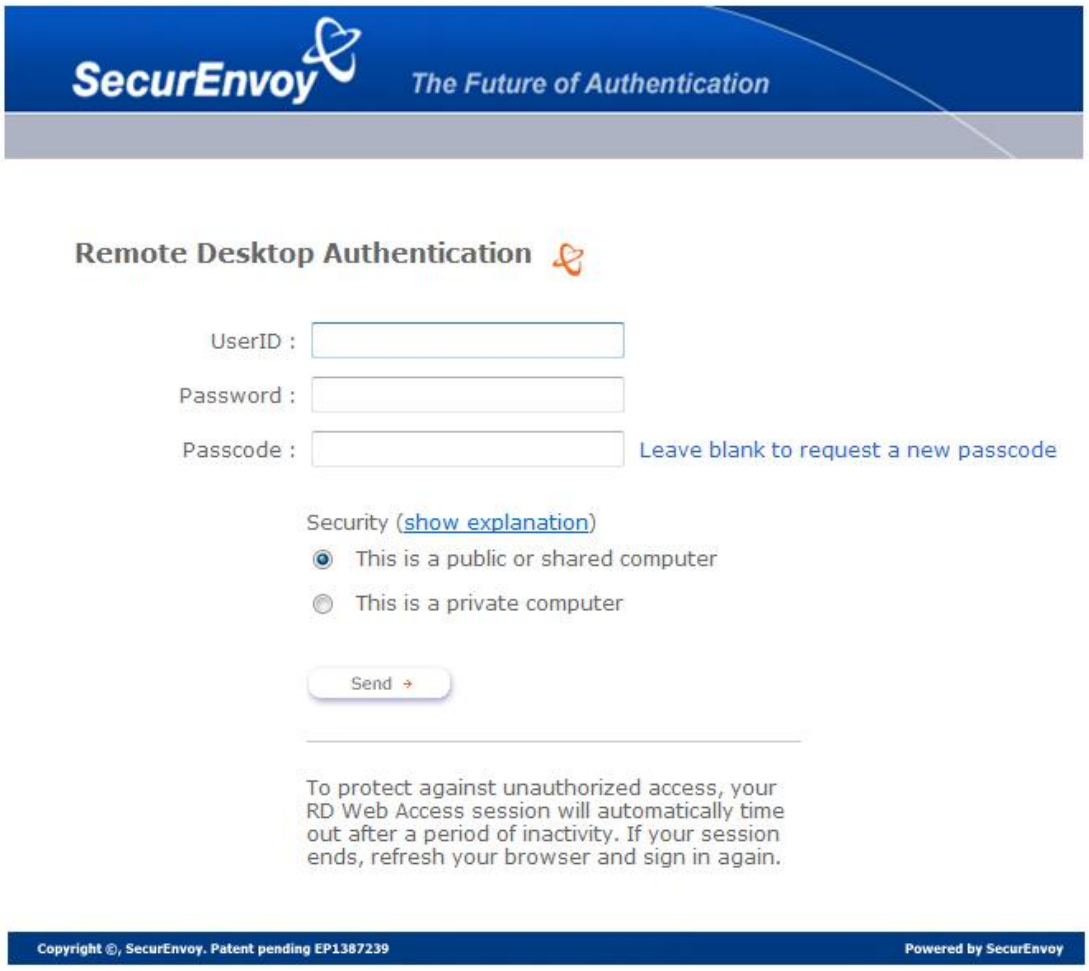
Select LDAP Password is the PIN under PIN Management (This is the default setting)

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

© 2005 SecurEnvoy Ltd. All rights reserved

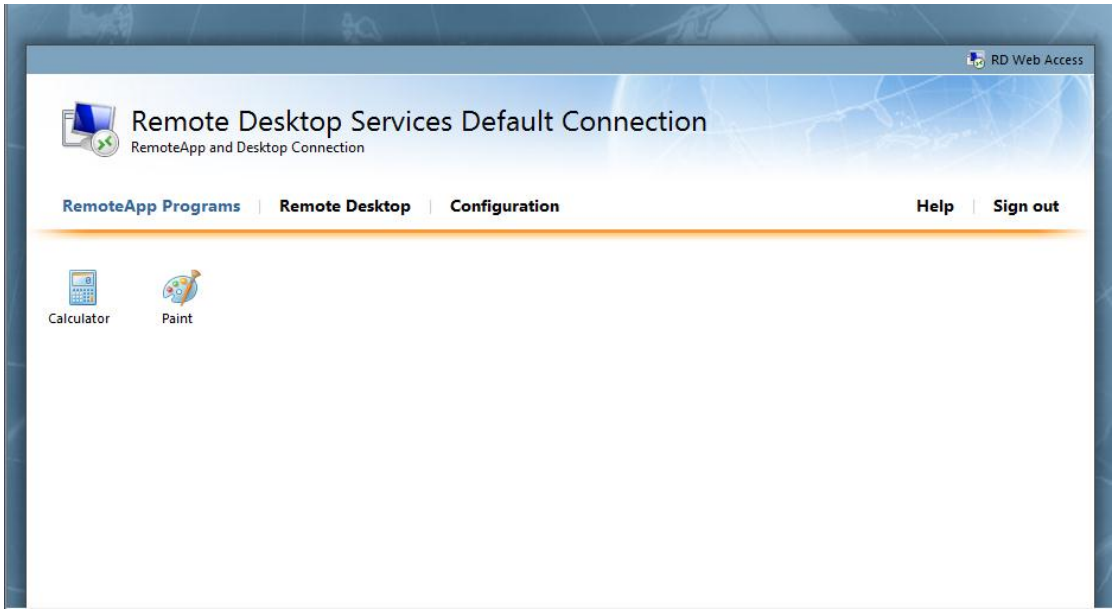
4.0 Test Logon

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



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

© 2005 SecurEnvoy Ltd. All rights reserved



Please note, you will be prompted for a domain login when you access any application.

© 2005 SecurEnvoy Ltd. All rights reserved