External Authentication with Windows 2012 R2 Server with Remote Desktop Web Gateway

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	

Windows 2012 R2 Server with Remote Desktop Web Gateway Integration Guide

This document describes how to integrate a Windows 2012 R2 Remote Desktop Web (RDWeb) Gateway installed with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Microsoft Windows 2012 R2 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 Microsoft Server 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 2012 R2 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 2012 R2
Installed roles:
Remote Desktop Services

SecurEnvoy
SecurAccess Server software release v7.2.504
Microsoft Server Agent V7.2

© 2014 SecurEnvoy Ltd. All rights reserved

Index

1.0 Prerequisites 3
1.1 Configure the Microsoft Server Agent 4
1.2 Configure the Microsoft Server Agent for the Default website (optional) 5
1.3 Configure the Microsoft Server Agent for RDWeb (optional) 6
2.0 Configure logout URL (optional) 7
2.1 Configure RDWeb Access Template (optional) 7
3.0 Test the Two Factor Authentication 8
4.0 Notes 10

1.0 Prerequisites

It is assumed that Remote Desktop Services 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 writes privileges to the Active Directory. If firewalls are between the SecurEnvoy Security server, Active Directory servers, and Remote Desktop Services, additional open ports will be required.

Microsoft Server Agent has been installed as per the SecurEnvoy Microsoft Server Agent Installation and Admin Guide:
https://www.securenvoy.com/integrationguides/iis%20agent%20installation%20guide.pdf

Note

You must use SecurEnvoy Microsoft Server Agent 7.2 or higher
You must use SecurEnvoy Security Server version 7.2.504 or higher
You Must use Remote Desktop Client 8.1 or higher

The following table shows what token types are supported.

Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓
One Swipe	✓

© 2014 SecurEnvoy Ltd. All rights reserved

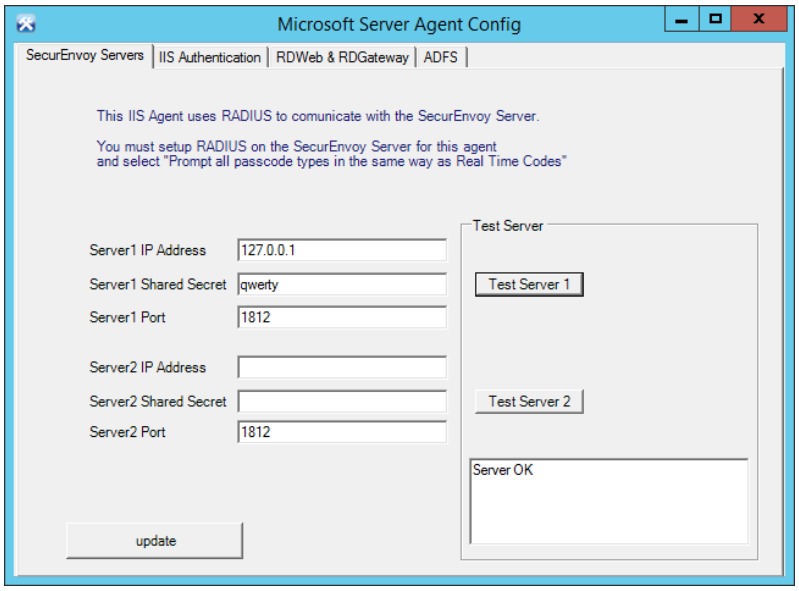
1.1 Configure the Microsoft Server Agent

Select the SecurEnvoy Servers tab.

Configure your SecurEnvoy Server 1 IP address and Shared Secret.

Once complete, press the Test Server 1.

If result returns 'OK', click 'update'.



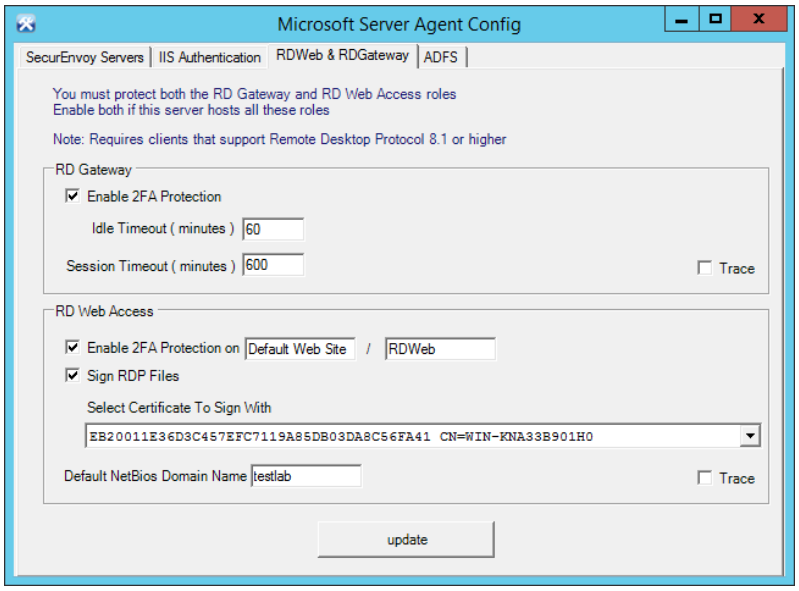
Select the RDWeb & RDGateway tab.

For RD Gateway protection from a direct connection, check the check box for 'Enable 2FA Protection'

RD Web Access protection, check the check box for 'Enable 2FA Protection on Default Web Site / RDWeb.

To enable RDP file signing, check the check box for 'Sign RDP Files' and select the certificate assigned to your RD Gateway.

Enter your Default NetBios Domain Name



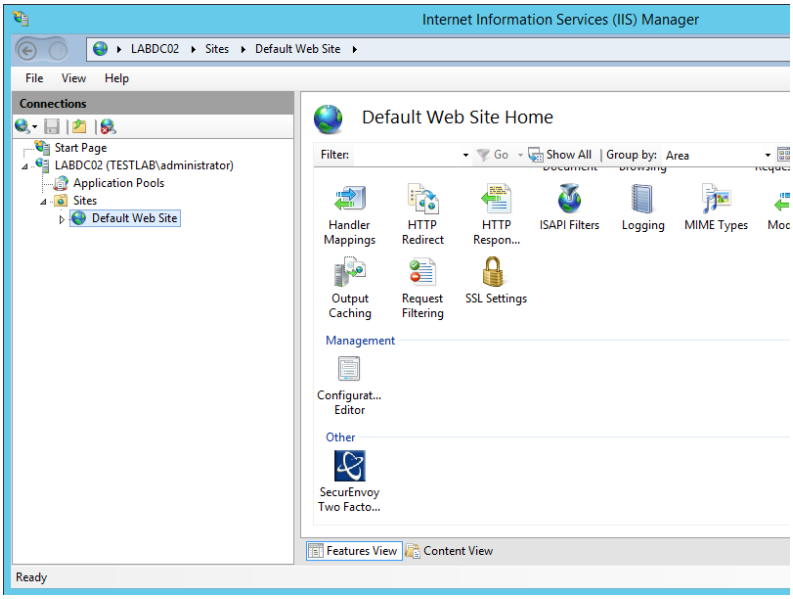
© 2014 SecurEnvoy Ltd. All rights reserved

1.2 Configure the Microsoft Server Agent for the Default website (optional)

> ***Note***
>
> **This section of the guide is for manual configuration of the RD Web Access and is not required, if you have used the Microsoft Server agent in section 1.1.**

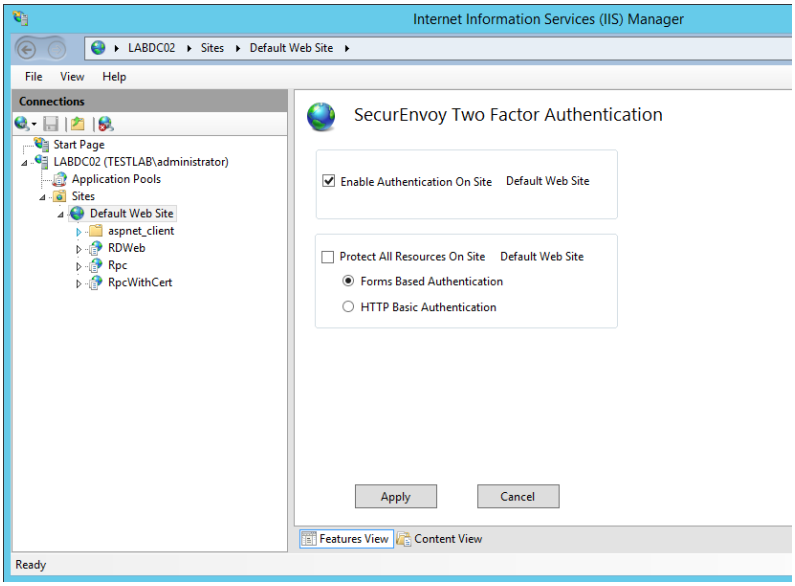
Launch the IIS management interface, either from "Start", "Administration Tools" or from the Server Manager

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.



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

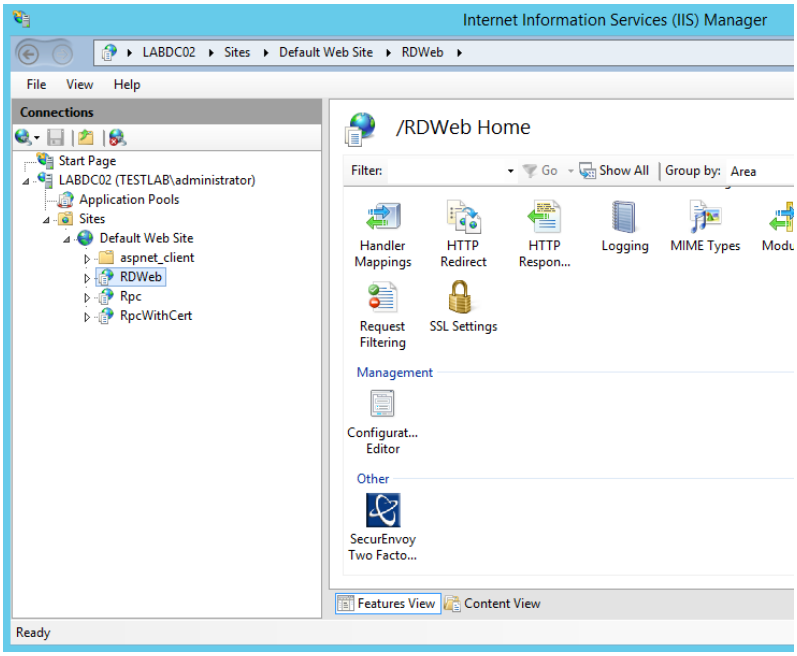
Click "Apply" when complete.



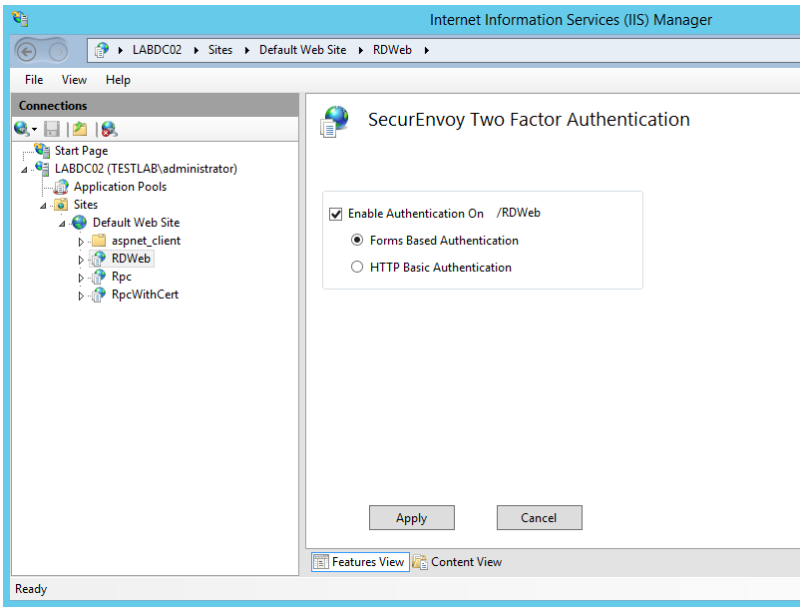
© 2014 SecurEnvoy Ltd. All rights reserved

1.3 Configure the Microsoft Server Agent for RDWeb (optional)

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



Select the tick box "Enable Authentication On /RDWeb"
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 "RDWebAccess". This must be maintained for correct operation.

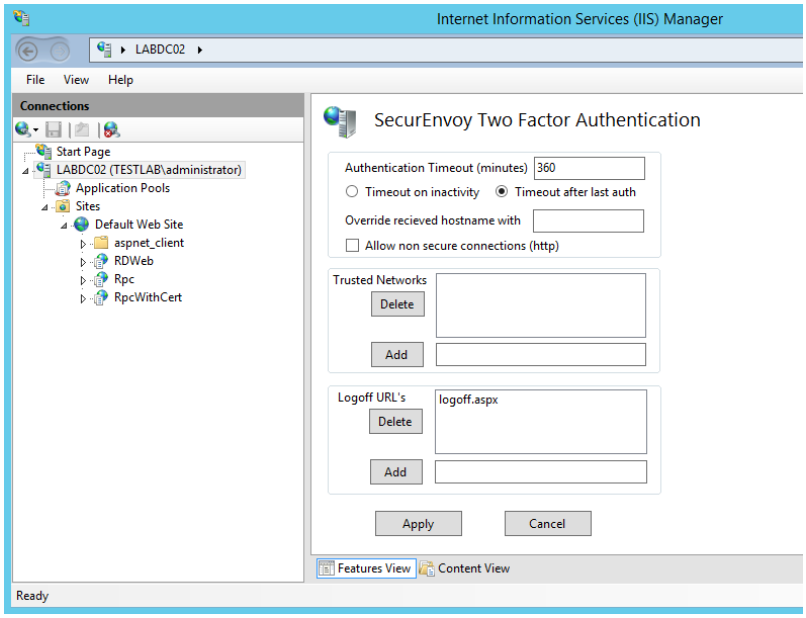
© 2014 SecurEnvoy Ltd. All rights reserved

2.0 Configure logout URL (optional)

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**

Restart IIS when prompted.



2.1 Configure RDWeb Access Template (optional)

Copy the contents of RDWeb2012R2 (C:\Program Files (x86)\SecurEnvoy\ Microsoft Server Agent \SAMPLES) to

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

© 2014 SecurEnvoy Ltd. All rights reserved

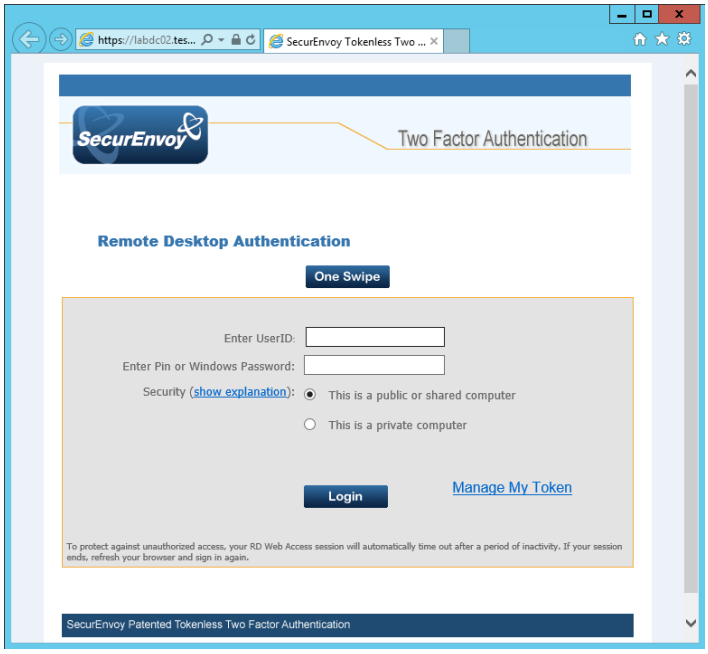
3.0 Test the Two Factor Authentication

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/rdweb (Don't forget the https)

User logon screen is shown.

Enter your UsedID and Password:

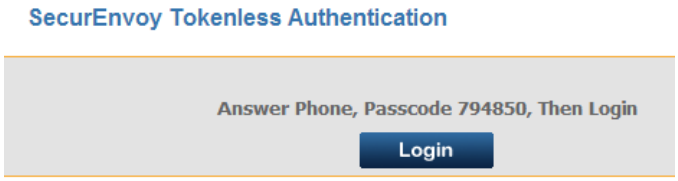


User is then presented with their two factor authentication type:

- Pre load, Realtime and Soft tokens:



- VOICE tokens:

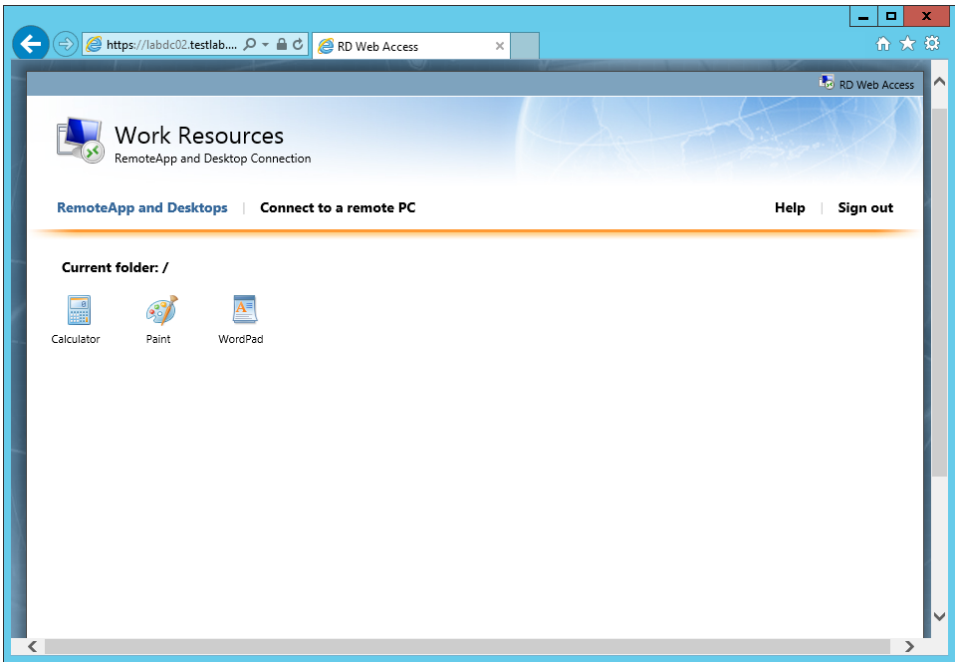


- One Swipe:



© 2014 SecurEnvoy Ltd. All rights reserved

User authenticates successfully and is presented with RDWeb 2012 R2:



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 OWA without specifying the domain name:
domain\UserID

© 2014 SecurEnvoy Ltd. All rights reserved

4.0 Notes

© 2014 SecurEnvoy Ltd. All rights reserved