

# External Authentication with Microsoft ISA Server 2006

## 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	

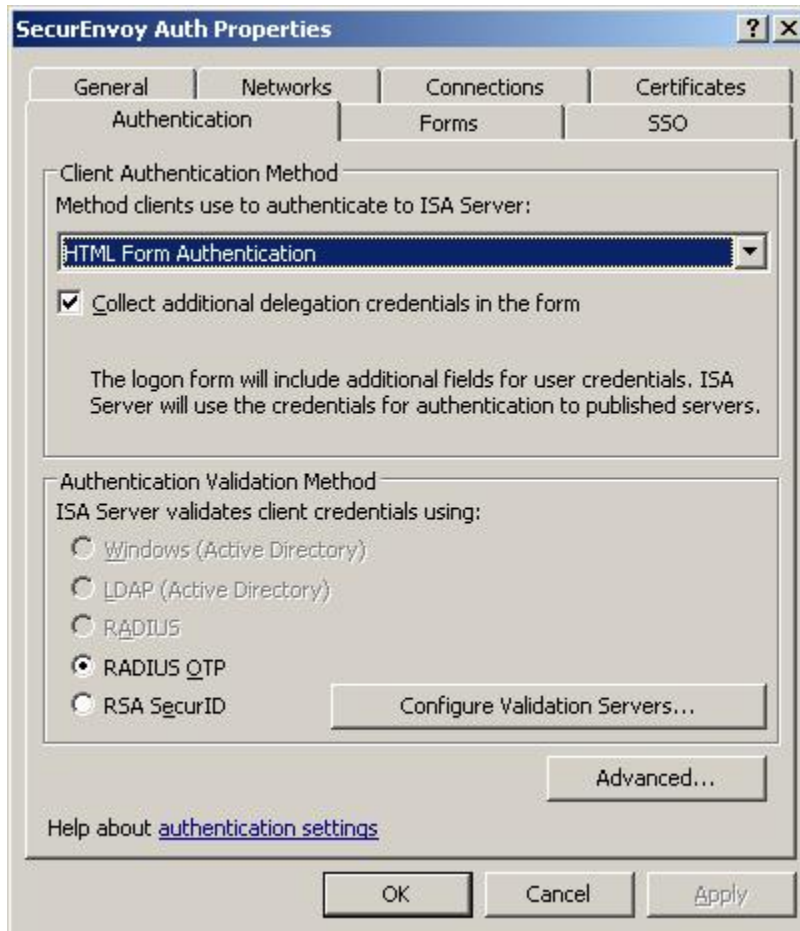
## 1. Setting up SecurEnvoy Authentication for Web applications

If you want to use Real Time Passcodes jump to Appendix 2

Create (or edit and existing) Listener and select the Authentication tab

In the Client Authentication Methods area, select **HTML Form Authentication**

In the Authentication Validation Method area, select **RADIUS OTP**



Press the "**Configure Validation Servers Button**"

Setup your SecurEnvoy Server settings

Then press **OK**

**Edit RADIUS Server** [?] [X]

Type the RADIUS server name or IP address and define how ISA Server will communicate with this server.

Server name:

Server description:

 By default, the shared secret is empty. For security reasons, we strongly recommend that you create a shared secret. Be sure to configure the shared secret on the RADIUS server as well.

Shared secret:

Authentication port:

 The port number used for RADIUS accounting will be the authentication port number plus one.

Time-out (seconds):

Always use message authenticator

Next press the "Advanced" button and check "Require all users to authenticate"

**Advanced Authentication Options** [?] [X]

Client Certificate Trust List | Client Certificate Restrictions

Authentication Preferences

Client Configuration Settings

**Require all users to authenticate:**

Require SSL client certificate

SSL client certificate timeout (seconds):

Allow client authentication over HTTP

Client Credentials Caching

Validate credentials for every HTTP request

Validate credentials every (seconds):

Authentication Domain

The default Windows domain used for Basic authentication is the Active Directory domain the ISA Server computer is active in. If a domain other than the default local domain should be used for authentication, enter the NetBIOS domain name of that domain.

Domain name:

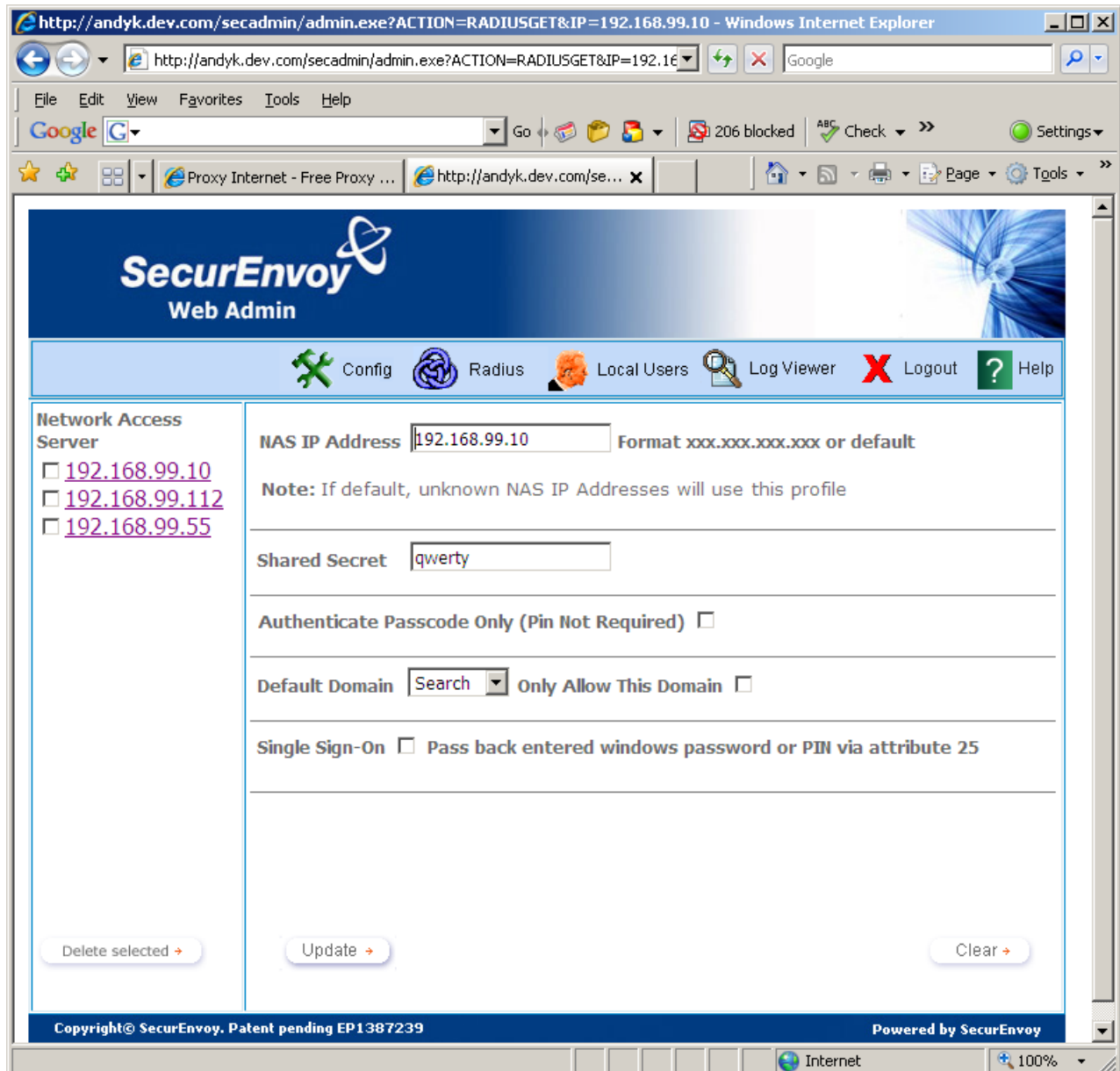
Help about [authentication preferences](#)

## 1.1 Setup SecurEnvoy Radius Settings

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

Click the **“Radius”** Button

Enter IP address and Shared secret for each Microsoft ISA 2006 server that wishes to use **SecurEnvoy** Two-Factor authentication.



## 2.0 IPSec VPN Authentications

Reuse the SecurEnvoy Radius server(s) defined in section 1 as the authentication method for IPSEC

## Appendix 1 Reducing multiply passwords in web logons

If you are only authenticating web based services than the Microsoft password is being checked by ISA and thus you should select "Authenticate Passcode Only" in the Radius setting of SecurEnvoy (see section 1.1).

If you plan to authenticate both IPsec and web applications then you can use customised templates with web applications to simply the login.

Customized Templates can only be used if you use SecurEnvoy's default setting of the windows password as the PIN and do not need support for mobile devices. In this operation the default Microsoft supplied templates require end users to enter their windows password and windows password and passcode which effectively results in the user entering their password in twice. These templates use Javascript to automatically enter the 2<sup>nd</sup> password.

### Step 1 Install the SecurEnvoy templates on to the ISA server

Download ISA 2006 templates from the following location:

[http://www.securenvoy.com//ftp/thirdparty/MicrosoftISA2006/SecurEnvoy\\_ISA2006Templates.zip](http://www.securenvoy.com//ftp/thirdparty/MicrosoftISA2006/SecurEnvoy_ISA2006Templates.zip)

Copy SecurEnvoy\_ISA C:\Program Files\Microsoft ISA Server\CookieAuthTemplates

Copy SecurEnvoy\_Exchange C:\Program Files\Microsoft ISA Server\CookieAuthTemplates

**Restart the Microsoft Firewall service to load templates into memory**

### Step 2 Define custom templates

Open the Firewall Policy that requires these templates

Select the **LISTENER** Settings tab, **PROPERTIES**

Check "Use customized HTML forms instead of the default"

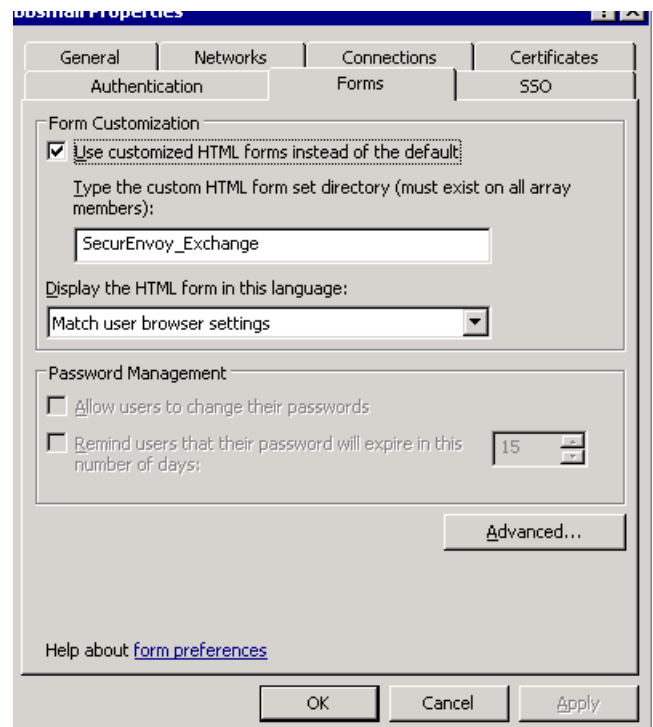
For Outlook Web Access enter SecurEnvoy\_Exchange

For other web applications enter SecurEnvoy\_ISA

**Restart the Microsoft Firewall service to load changes**

### Step 3 Radius settings

Un-Check "Authenticate Passcode Only" in the Radius setting of SecurEnvoy for this Isa Server



## **Appendix 2 Real Time Passcode Support**

To use real time passcodes you must install the ISA 2006 Real Time Agent.

This can be downloaded from the following location:

<http://www.securevoy.com//ftp/thirdparty/MicrosoftISA2006/ISA2006RealTimeAgent.zip>

Follow the ISA Agent Installation Guide contained in this zip file for installation and configuration details