External Authentication with Aventail SSL VPN

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	

The equipment used as the time of writing this integration guide is listed below:

Aventail

Aventail SSL VPN appliance
Software Revision Version 8.8.1

Microsoft

Windows 2003 server
IIS installed with SSL certificate
Access to Active Directory with an Administrator Account

SecurEnvoy

SecurAccess software release v4.1

1. Setting up SecurEnvoy

Install the SecurEnvoy server

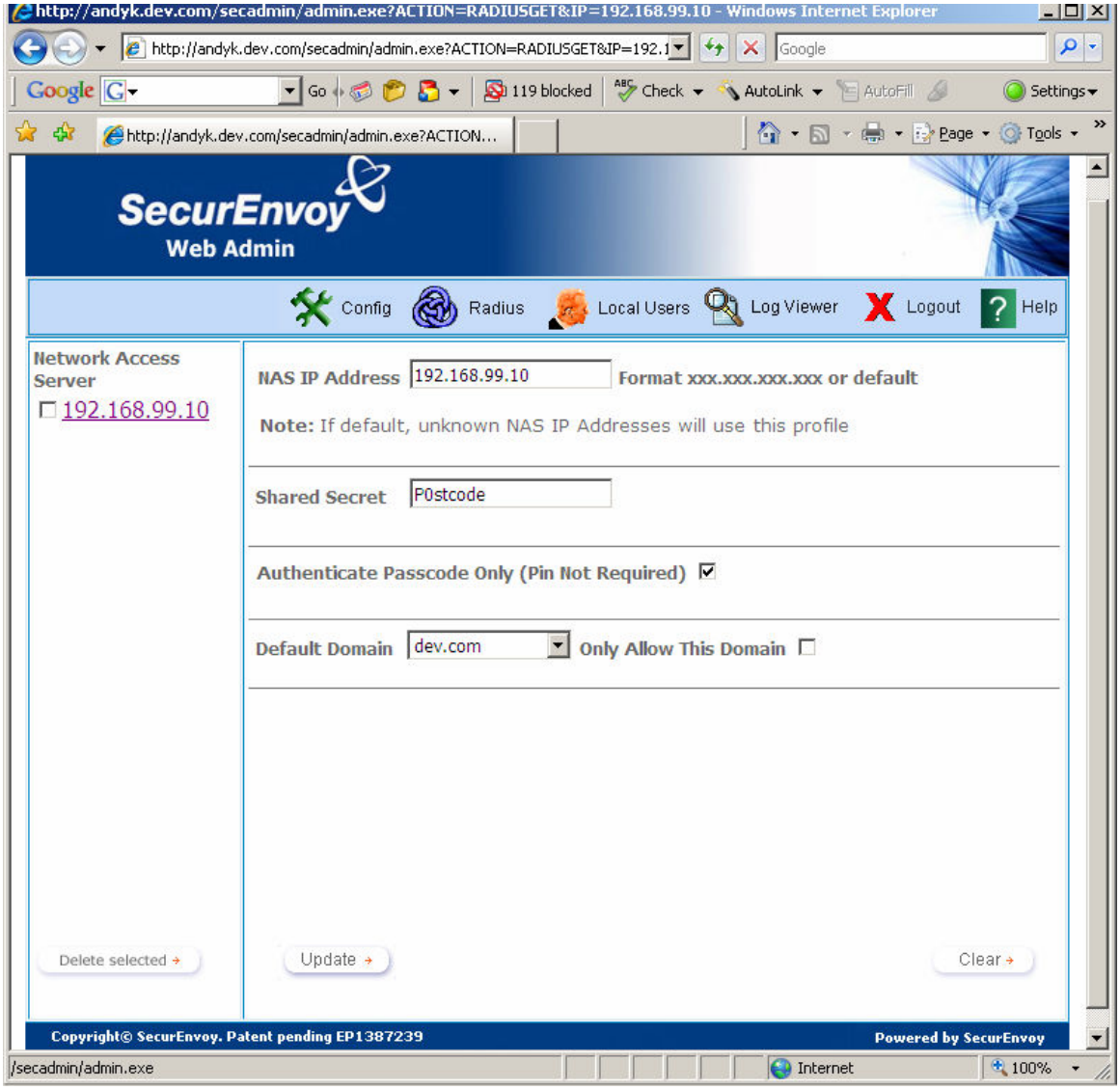
Use the default setting of Windows Password is the PIN in the GUI Config Menu

Step 1 Setup SecurEnvoy / Radius client

Step 2 Start the SecurEnvoy GUI and select the menu Radius

Step 3 Enter the IP Address of the Aventail SSL system

Step 4 Select the "Authenticate Passcode Only" check box



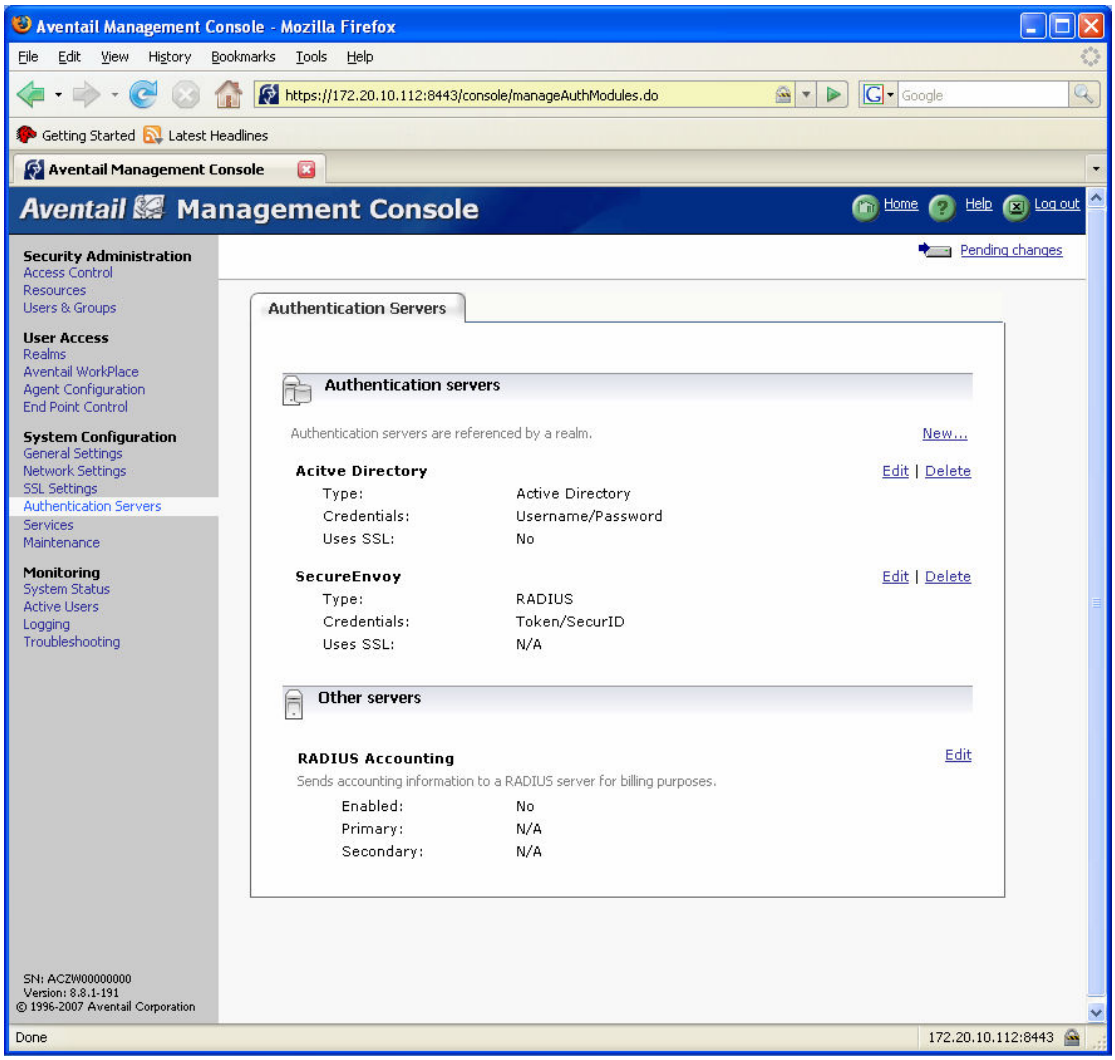
2. Setting up Aventail

Create the Authentication Servers

Step 1.1
Logon to console with administrator account

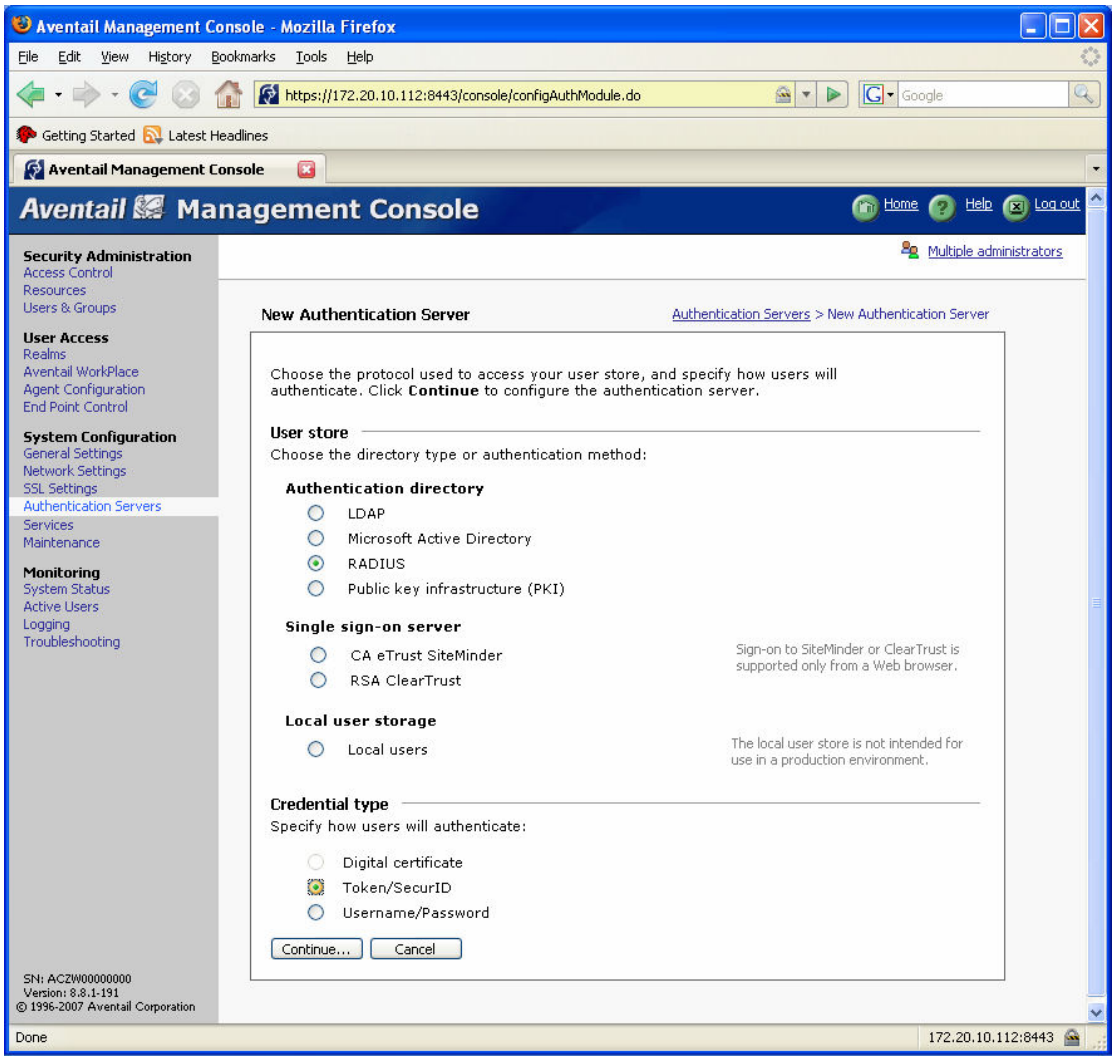
Select Authentication Servers

Create a new authentication server, select "new"



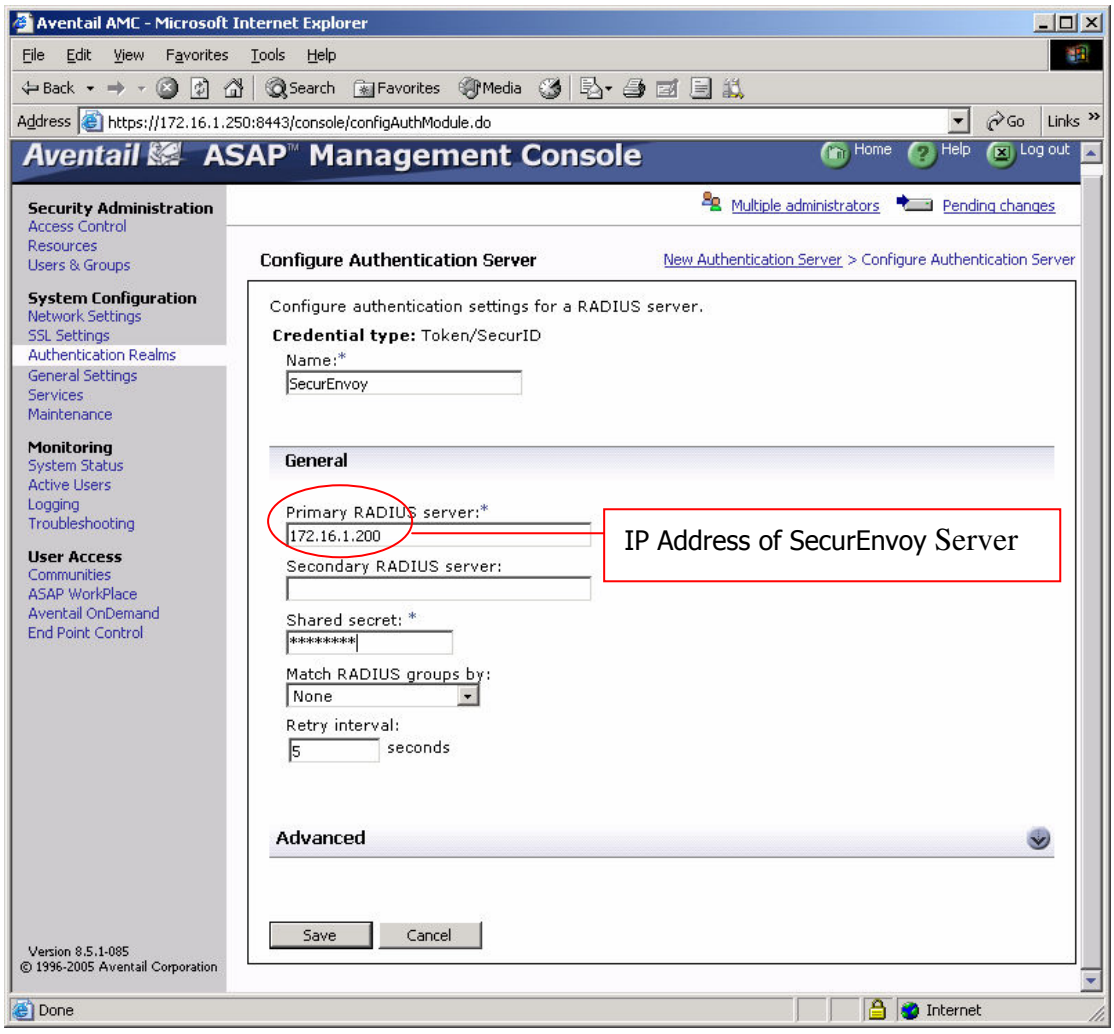
Step 1.2

Select “Radius” and “Token/SecurID”, then select “Continue”



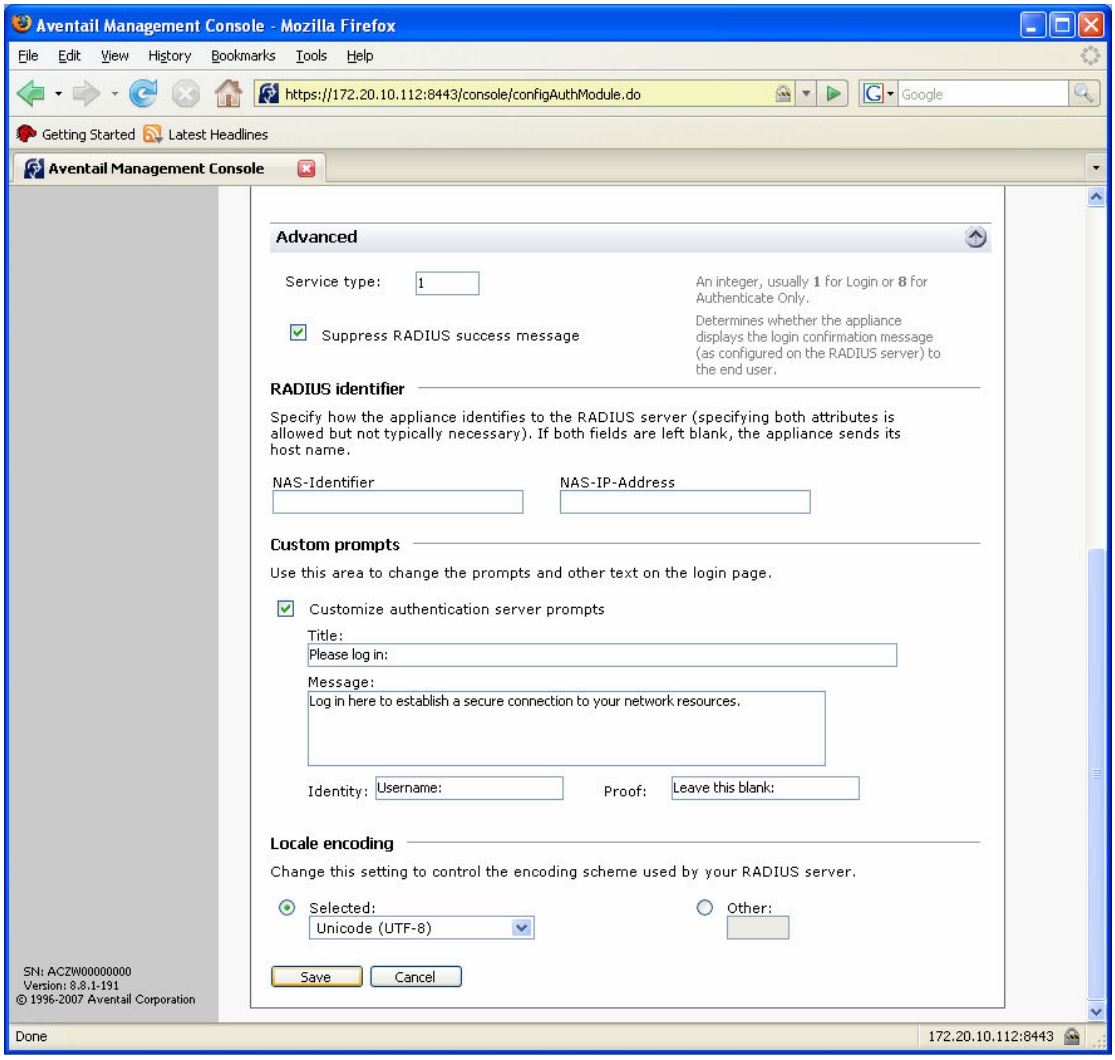
Step 1.3 Enter SecurEnvoy Radius Server details

The "Name:" field is used for Aventail internal reference only.
The shared secret entered must be the same as set later in this document.



Step 1.4
Change the end users logon prompt.

Select Advanced with the down arrow and select "suppress RADIUS success message", then select "Customize authentication server prompts" and change the "proof" field to read "Enter SMS Passcode:"



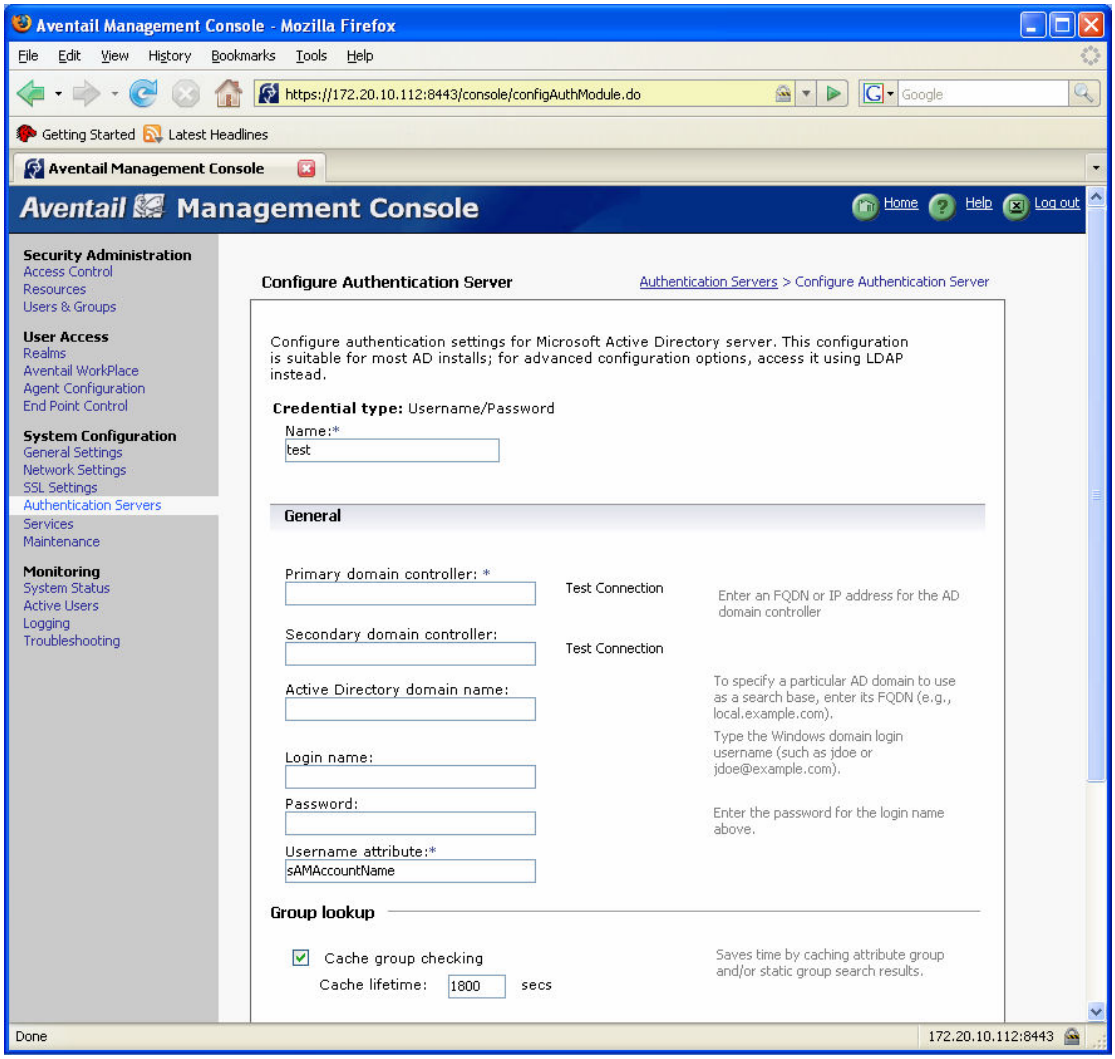
Select Save

Step 1.5
Create AD authentication server
Select "New" and then select "Microsoft Active Directory"

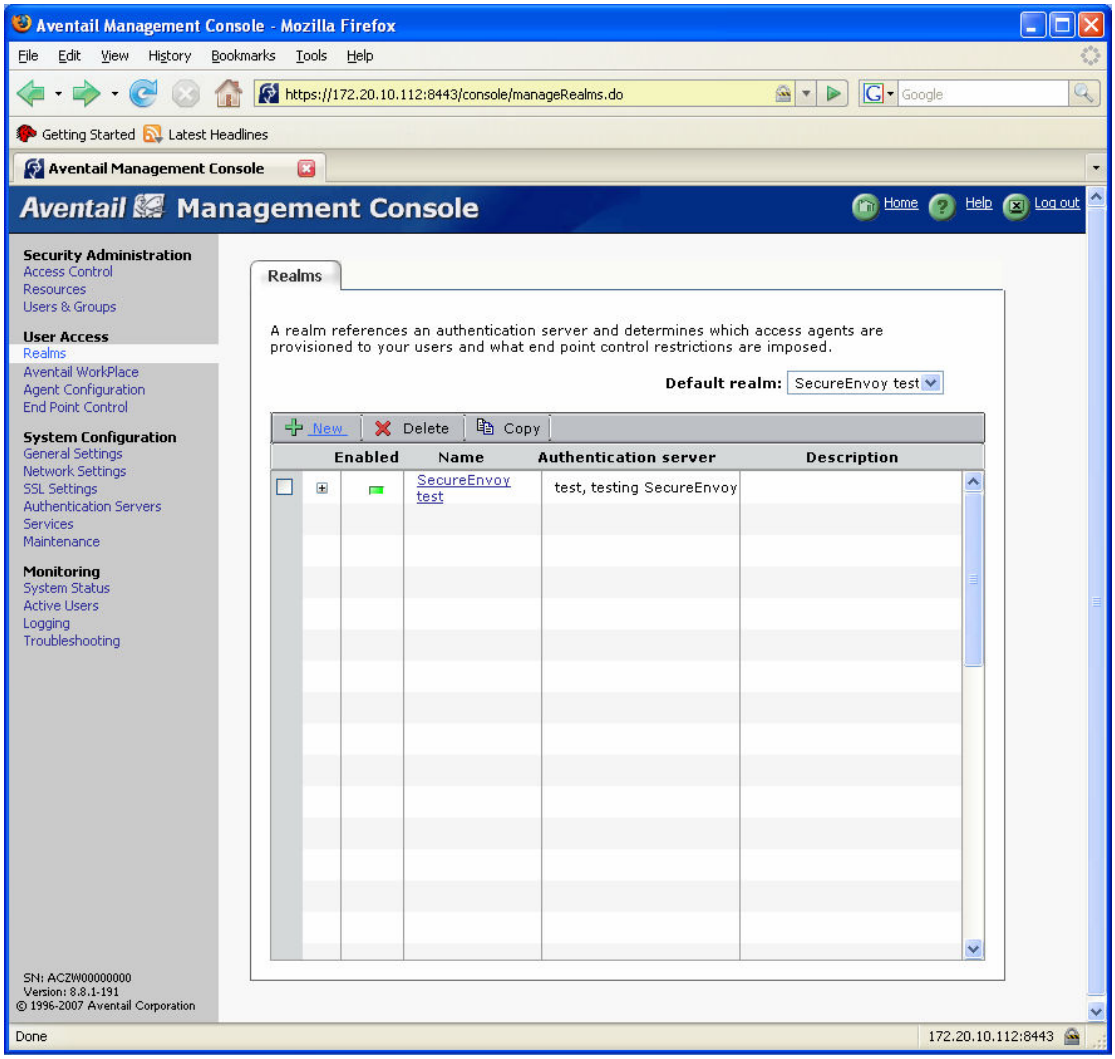
Step 1.6

Enter the IP address or FQDN of the primary and optionally a secondary AD server, the AD Domain name and username and password of an account with read privileges to all objects in the directory (the only account by default with these privileges is Administrator)

Select "Save"



Step 2 Create an authentication Realm, Select "Realms", then select "New"



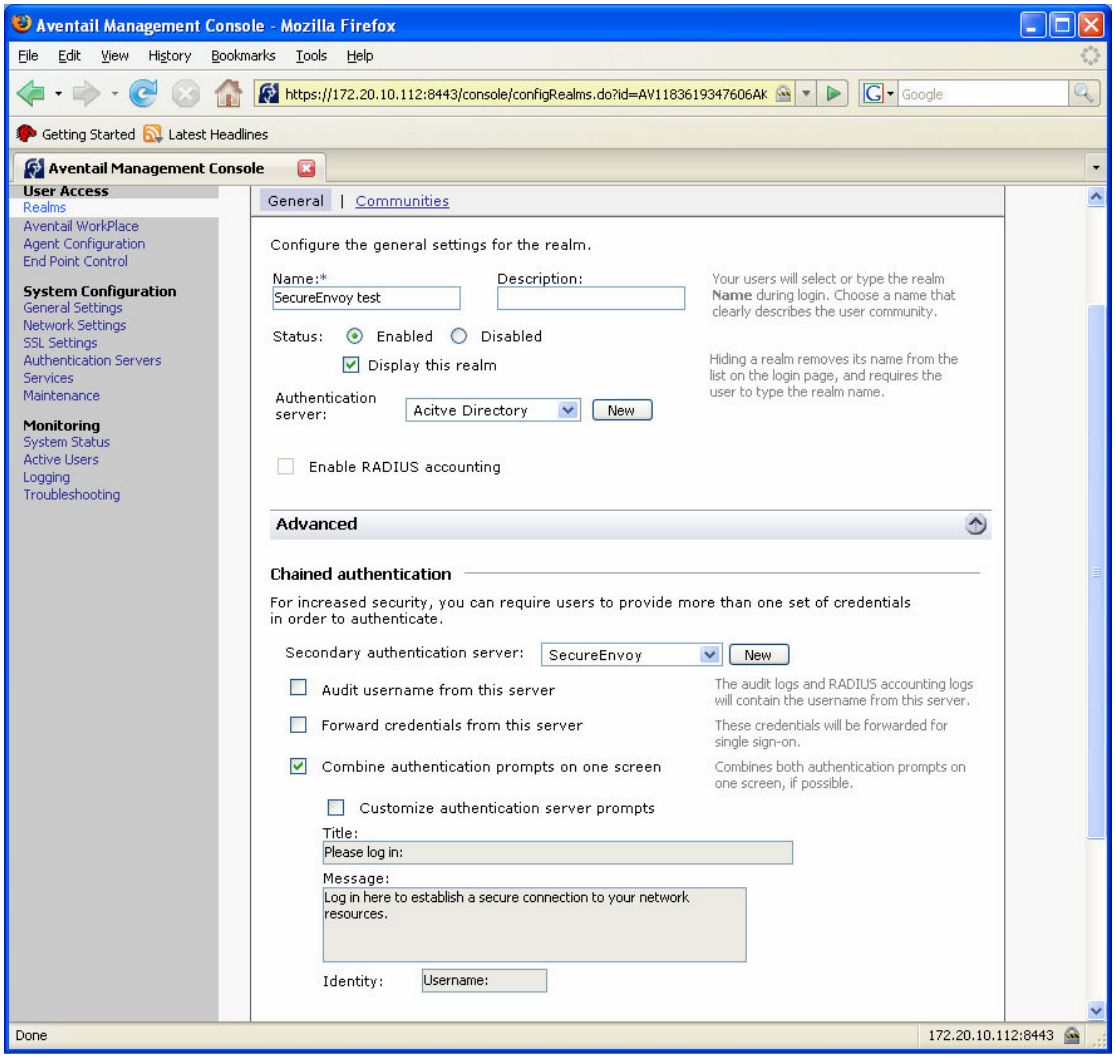
Type a name for the realm. Your users will select a realm name when logging in, so specify a realm name that clearly describes the user community.

Authentication Server: select the Active Directory server

Select "Advanced" to open the advanced configuration options,

Secondary authentication server: select SecureEnvoy
Select the "combine authentication prompts on one screen" check box

If is also recommended that communities are setup as per Aventail's documentation.



Step 3 Apply pending changes