

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

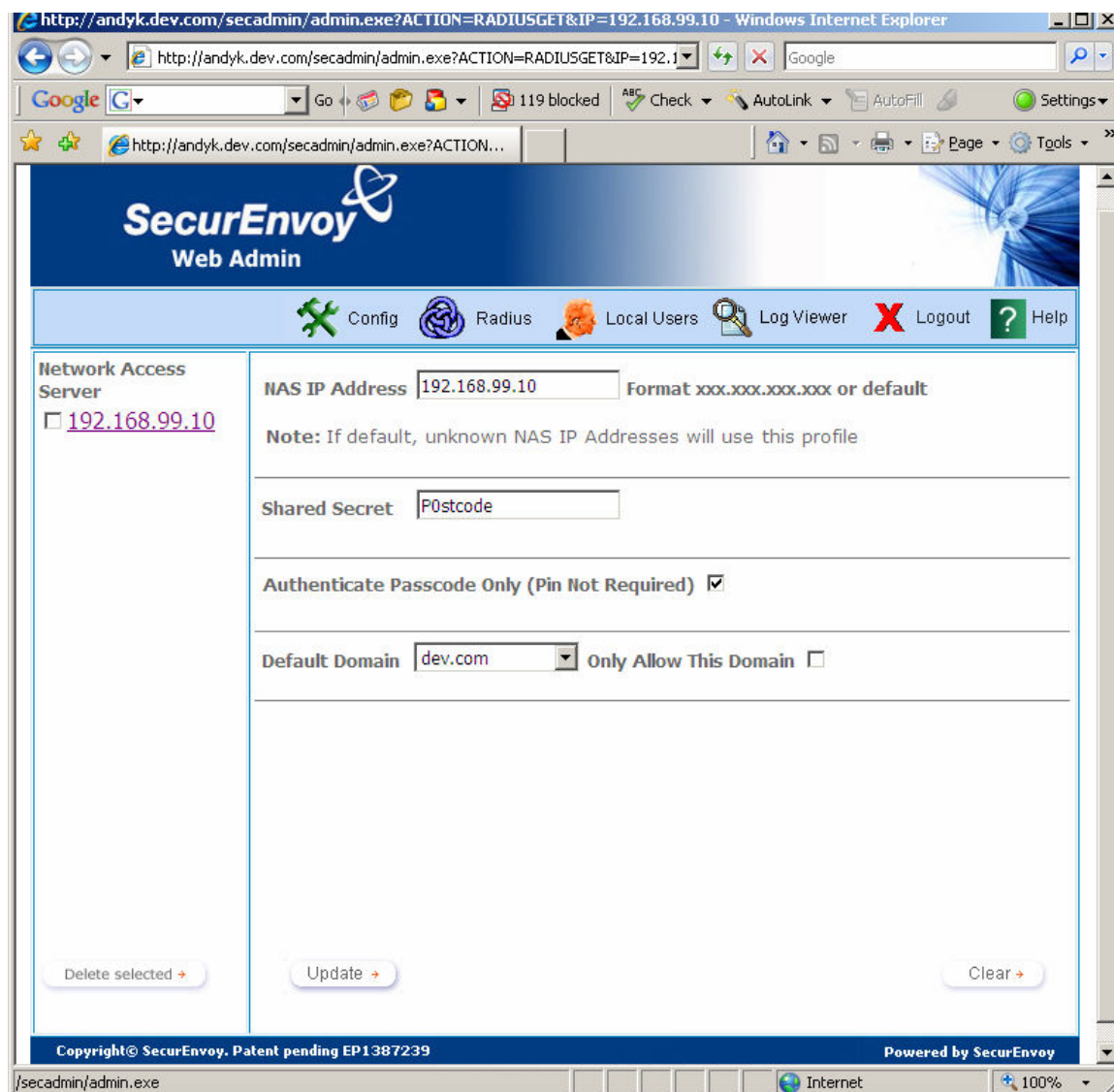
Use the default setting of Windows Password is the PIN in the GUI Config Menu

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 Aventaill SSL system

Step 4 Select the "Authenticate Passcode Only" check box



The screenshot shows the SecurEnvoy Web Admin interface in a Windows Internet Explorer browser. The page title is "SecurEnvoy Web Admin". The navigation menu includes "Config", "Radius", "Local Users", "Log Viewer", "Logout", and "Help". The "Radius" section is active, showing the configuration for a Network Access Server. The "NAS IP Address" field is set to "192.168.99.10" with a note: "Note: If default, unknown NAS IP Addresses will use this profile". The "Shared Secret" field is set to "P0stcode". The "Authenticate Passcode Only (Pin Not Required)" checkbox is checked. The "Default Domain" is set to "dev.com" and the "Only Allow This Domain" checkbox is unchecked. At the bottom of the form, there are buttons for "Delete selected", "Update", and "Clear". The footer of the page contains "Copyright© SecurEnvoy. Patent pending EP1387239" and "Powered by SecurEnvoy".

2. Setting up Aventail

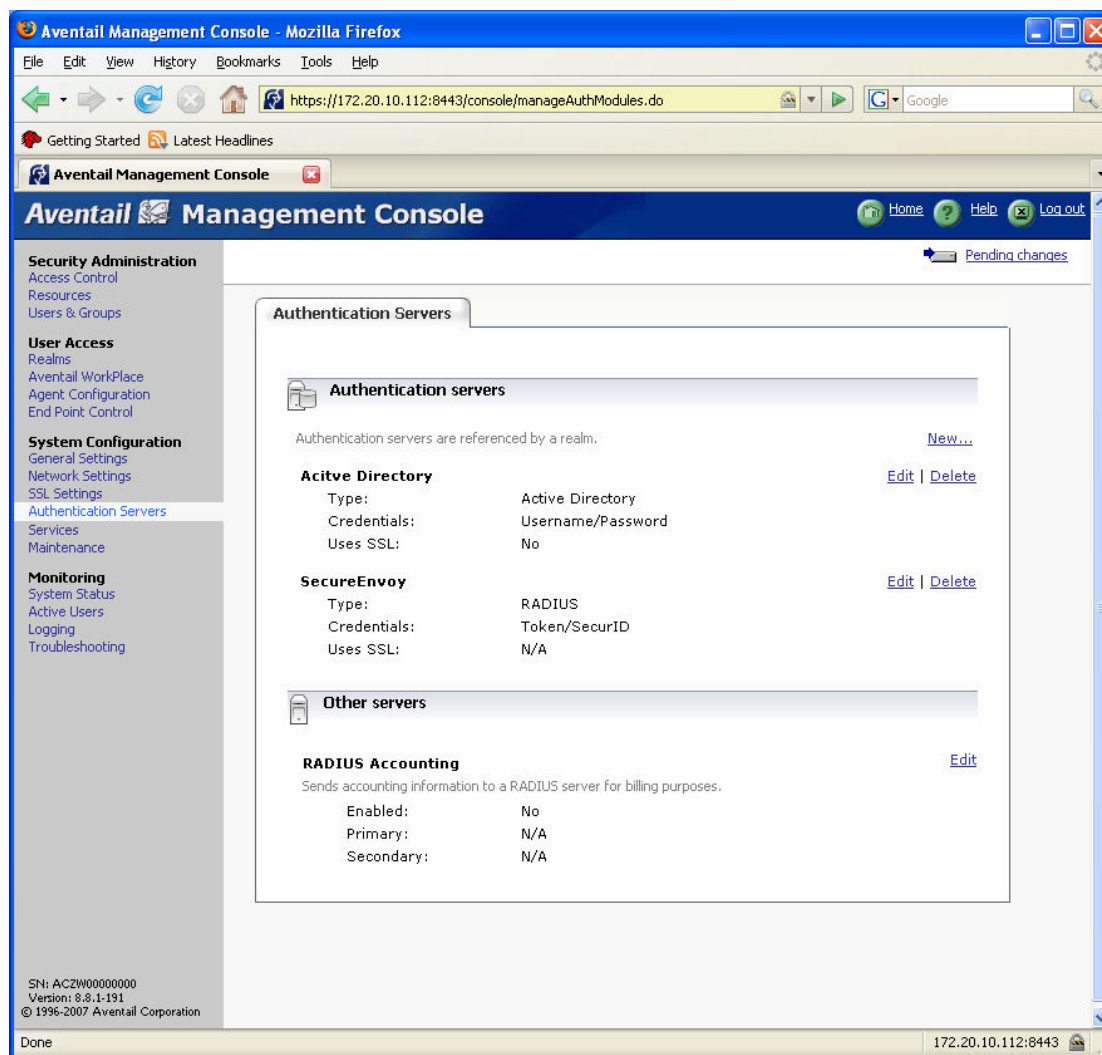
Create the Authentication Servers

Step 1.1

Logon to console with administrator account

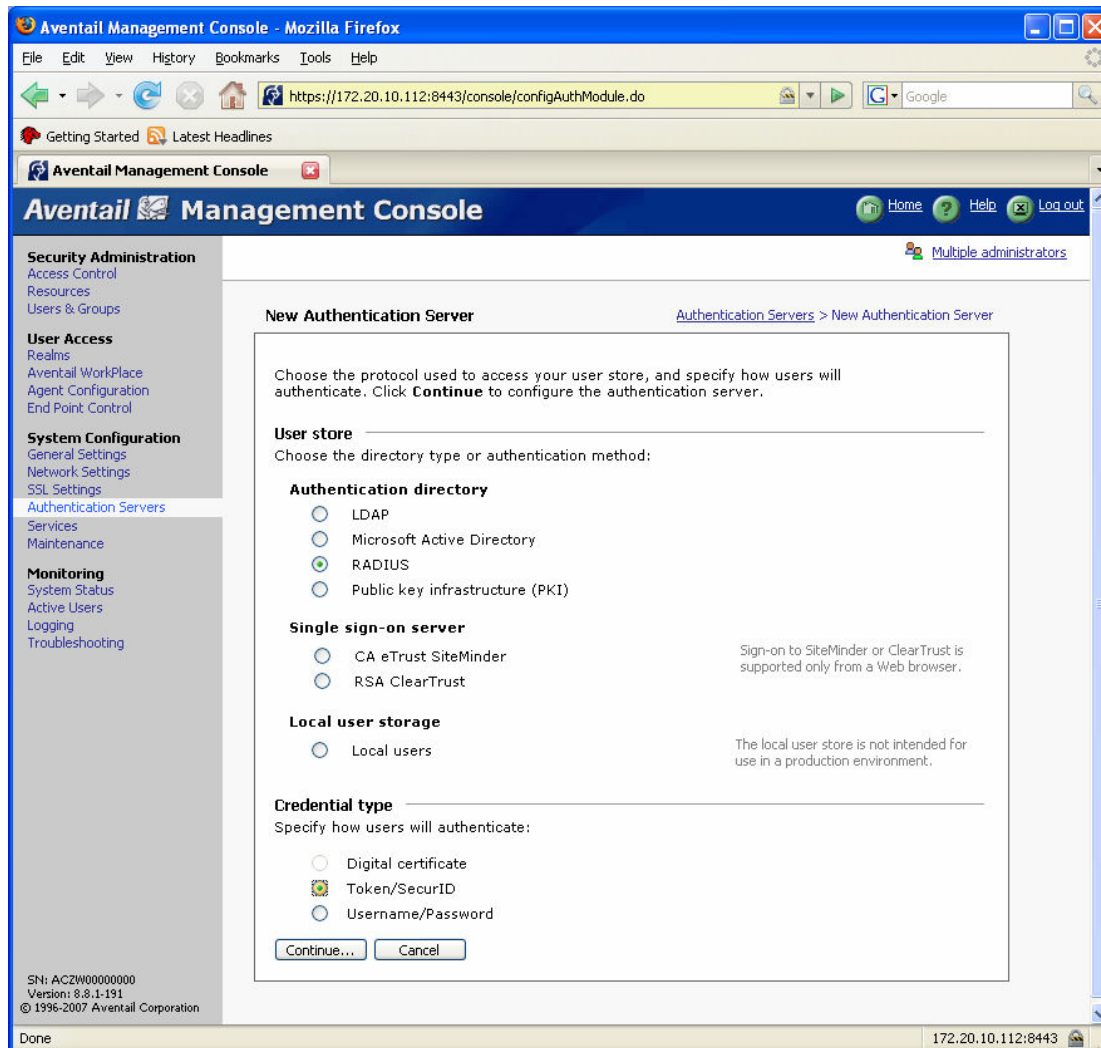
Select Authentication Servers

Create a new authentication server, select "new"



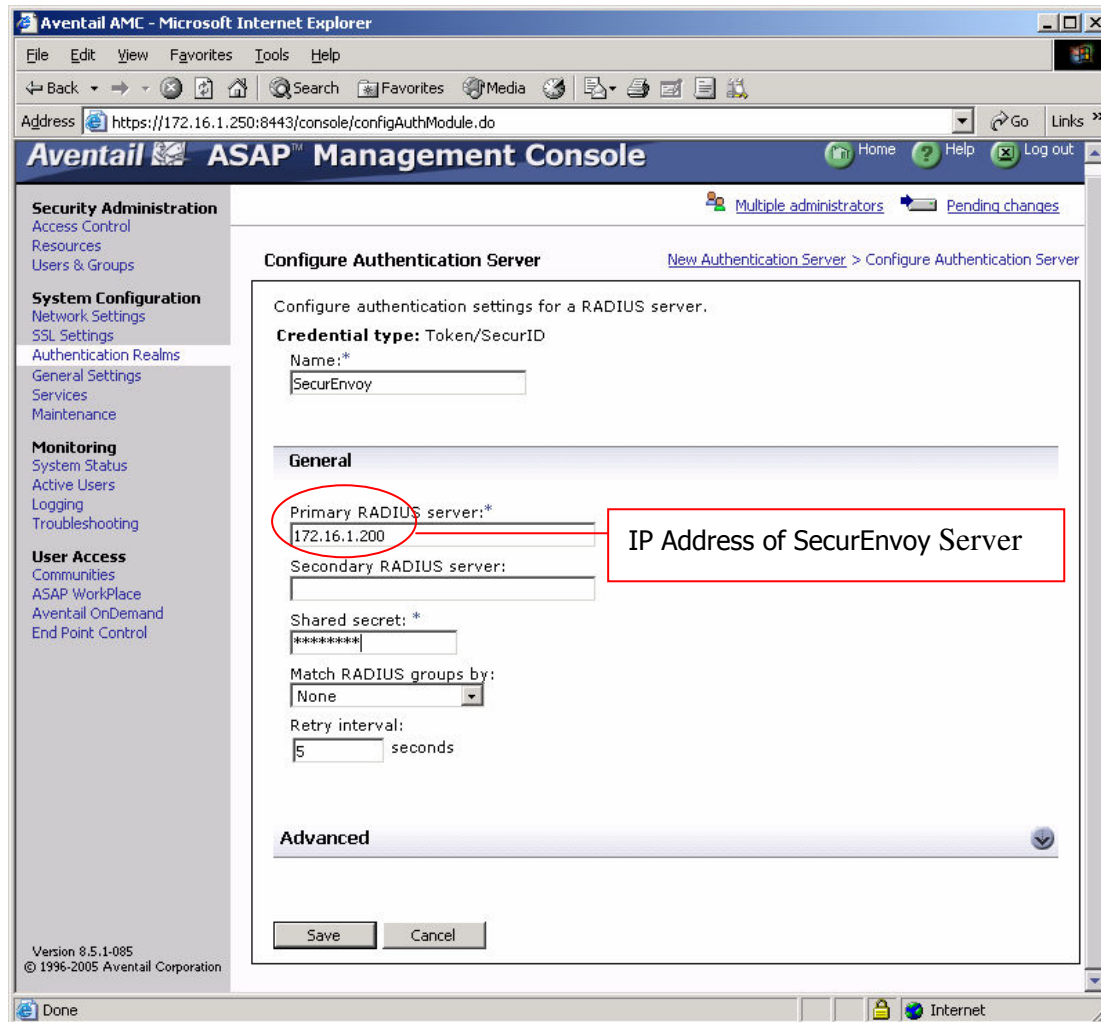
Step 1.2

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.



The screenshot shows the 'Configure Authentication Server' page in the Aventail ASAP Management Console. The page is titled 'Configure Authentication Server' and includes a breadcrumb trail: 'New Authentication Server > Configure Authentication Server'. The main content area is titled 'Configure authentication settings for a RADIUS server.' and shows the following fields:

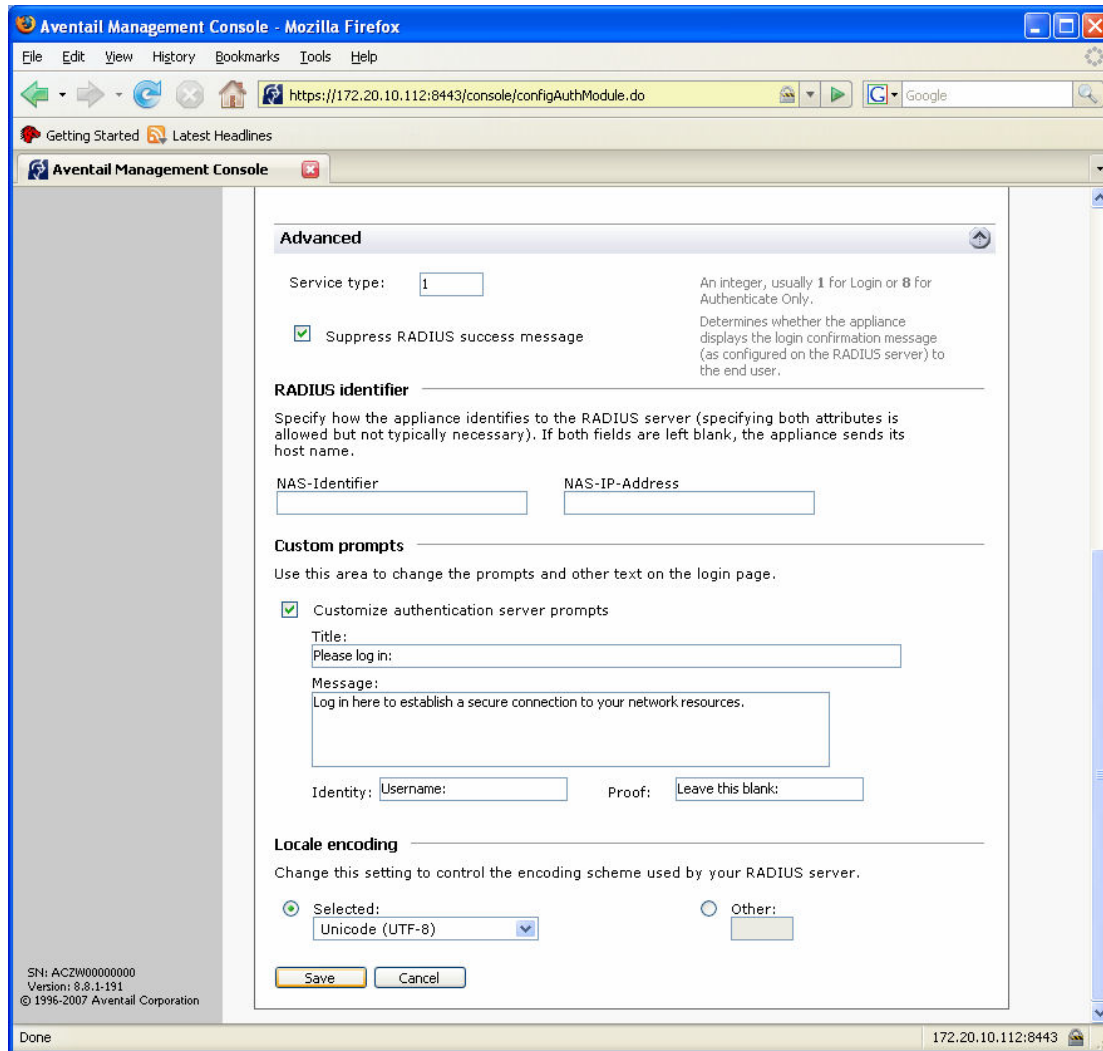
- Credential type:** Token/SecurID
- Name:*** SecurEnvoy
- General** section:
 - Primary RADIUS server:*** 172.16.1.200 (This field is circled in red and labeled 'IP Address of SecurEnvoy Server')
 - Secondary RADIUS server:** (empty)
 - Shared secret: *** (masked with asterisks)
 - Match RADIUS groups by:** None
 - Retry interval:** 5 seconds
- Advanced** section (collapsed)

At the bottom of the form are 'Save' and 'Cancel' buttons. The left sidebar contains navigation links for Security Administration, System Configuration, Monitoring, and User Access. The bottom of the window shows the version '8.5.1-085' and copyright '© 1996-2005 Aventail Corporation'.

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:"



The screenshot shows the 'Aventail Management Console' configuration page in Mozilla Firefox. The browser address bar shows the URL: `https://172.20.10.112:8443/console/configAuthModule.do`. The page title is 'Aventail Management Console'. The 'Advanced' section is expanded, showing the following configuration options:

- Service type:** 1 (An integer, usually 1 for Login or 8 for Authenticate Only.)
- Suppress RADIUS success message** (Determines whether the appliance displays the login confirmation message (as configured on the RADIUS server) to the end user.)
- RADIUS identifier**
Specify how the appliance identifies to the RADIUS server (specifying both attributes is allowed but not typically necessary). If both fields are left blank, the appliance sends its host name.
NAS-Identifier: NAS-IP-Address:
- Custom prompts**
Use this area to change the prompts and other text on the login page.
 Customize authentication server prompts
Title:
Message:
Identity: Username: Proof:
Locale encoding
Change this setting to control the encoding scheme used by your RADIUS server.
 Selected: Unicode (UTF-8) **Other:**

At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted. In the bottom left corner, the console version information is displayed: SN: AC2W00000000, Version: 8.8.1.131, © 1996-2007 Aventail Corporation. The browser status bar at the bottom shows 'Done' and the IP address '172.20.10.112:8443'.

Select Save

Step 1.5

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

Step 1.6

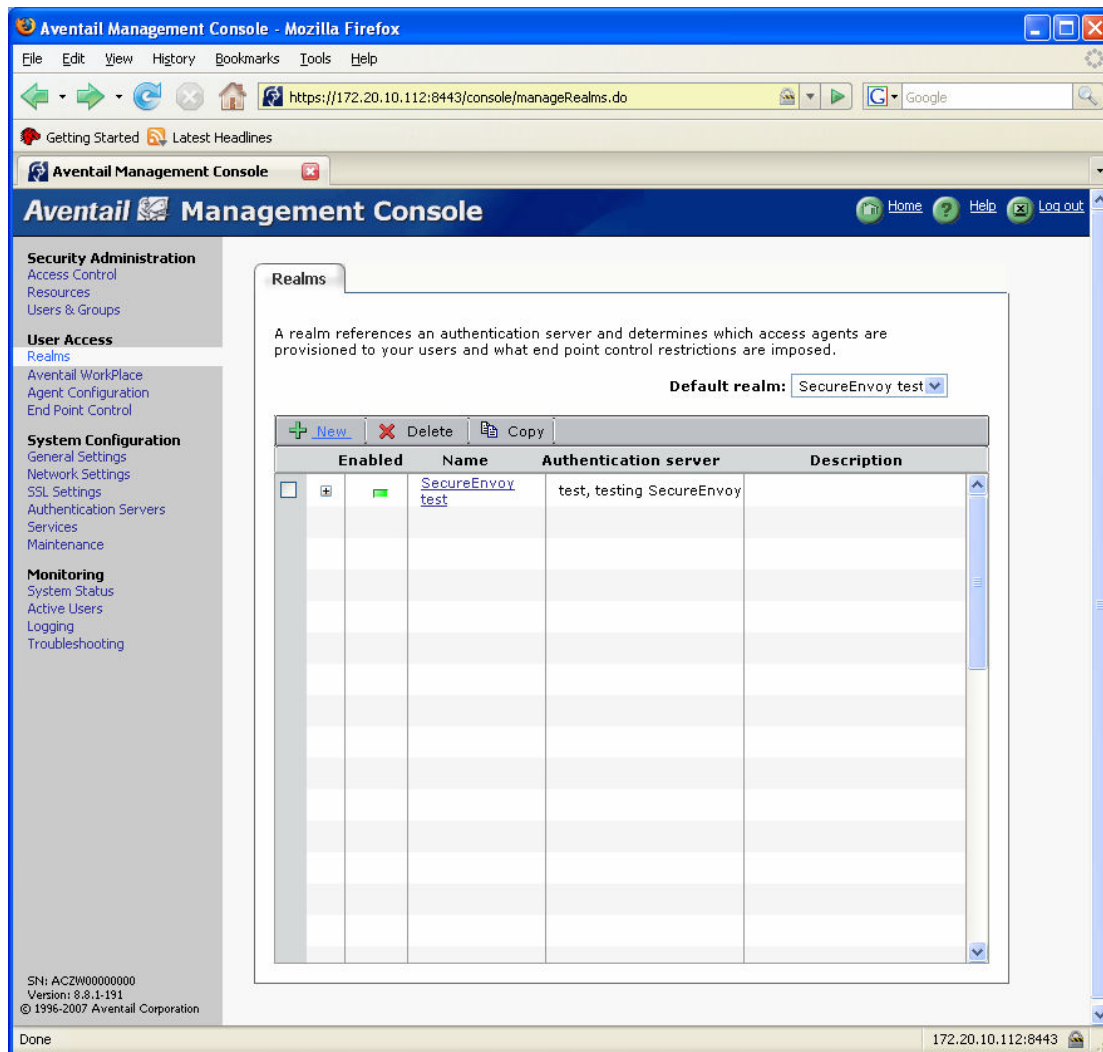
Enter the IP address or FQDN of the primary and optionally a secondary AD server, the AD Domain name and username and password of an account with read privileges to all objects in the directory (the only account by default with these privileges is Administrator)

Select "Save"

The screenshot displays the Aventail Management Console interface in a Mozilla Firefox browser window. The browser's address bar shows the URL `https://172.20.10.112:8443/console/configAuthModule.do`. The console's navigation menu on the left includes sections for Security Administration, User Access, System Configuration, and Monitoring. The main content area is titled "Configure Authentication Server" and contains the following configuration fields:

- Credential type:** Username/Password
- Name:***
- General** section:
 - Primary domain controller: *** **Test Connection** (Enter an FQDN or IP address for the AD domain controller)
 - Secondary domain controller:** **Test Connection**
 - Active Directory domain name:** (To specify a particular AD domain to use as a search base, enter its FQDN (e.g., local.example.com).)
 - Login name:** (Type the Windows domain login username (such as jdoe or jdoe@example.com).)
 - Password:** (Enter the password for the login name above.)
 - Username attribute:***
- Group lookup** section:
 - Cache group checking** (Saves time by caching attribute group and/or static group search results.)
 - Cache lifetime:** **secs**

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.

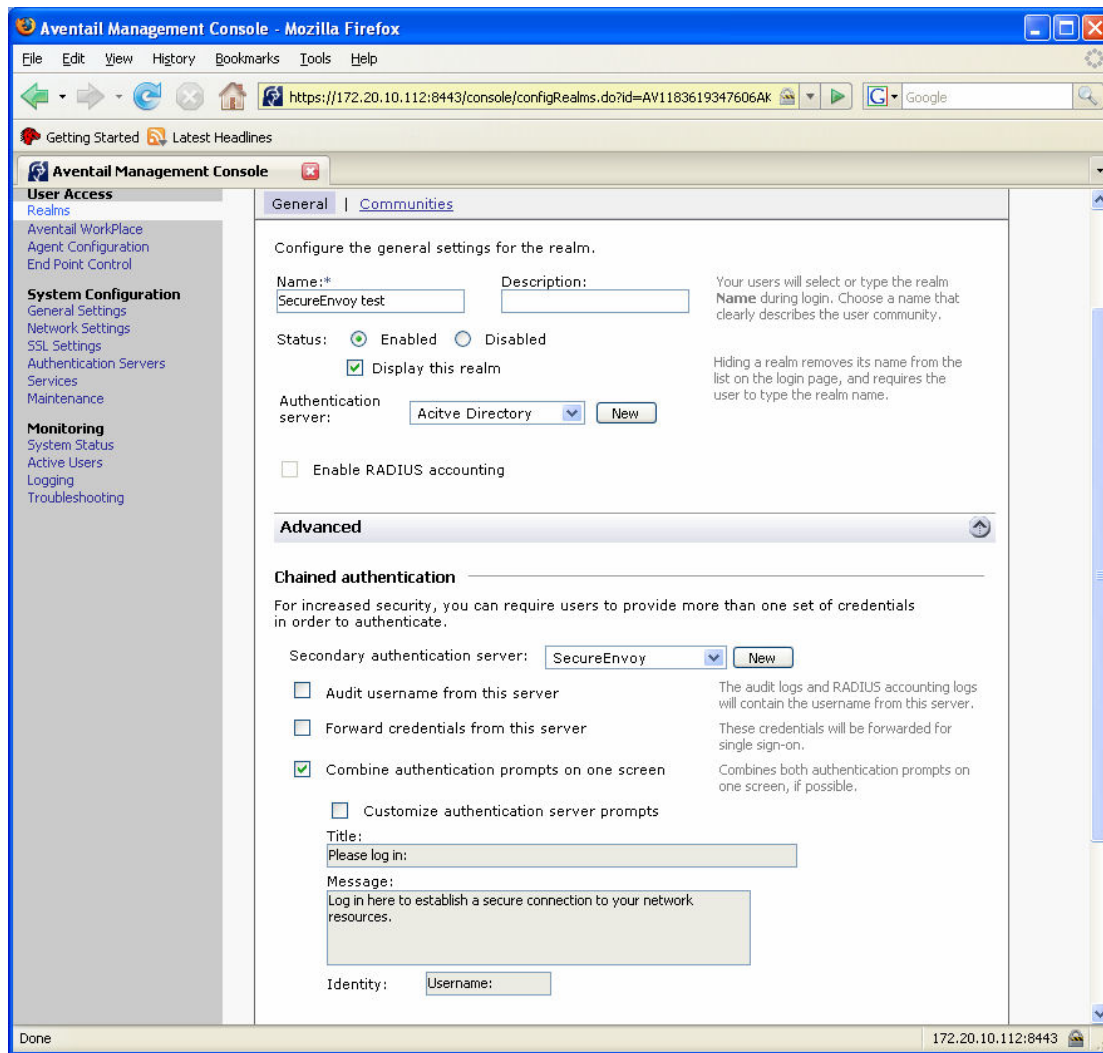
Authentication Server: select the Active Directory server

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