

## *How to enable AD authentication on SA500 series routers*

### Pre-requisites:

This guide assumes Active directory is already configured and users and groups are able to log in to domain from client computers. The SA500 series device is configured to allow VPN connections and is accessible from the local network.

### Configuration:

#### NOTE:

If port 443 is being forwarded and only one public IP is available for use on the WAN, see <THIS> document for implementation of workaround.

### Step 1

Log into SA with administrator privileges and navigate to "Administration"

The screenshot shows the Cisco Security Appliance Configuration Utility (SA) interface. The top navigation bar includes "Getting Started", "Status", "Networking", "Firewall", "IPS", "ProtectLink", "VPN", "Administration" (highlighted with a red circle 1), and "Network Management". The left sidebar shows a tree view with "Users" expanded, and "Domains" selected (highlighted with a red circle 2). The main content area displays the "Domains" configuration page, which includes a "List of Domains" table and "Add" and "Delete" buttons. A callout box with a red circle 3 points to the "Add" button, containing the following instructions:

1. Select "Administration"
2. Expand "Users" then select "Domains"
3. Click "Add"

<input type="checkbox"/>	Domain Name	Authentication Type	Portal Layout Name	User Type	Edit
<input type="checkbox"/>	SSLVPN*	Local User Database	SSLVPN		

Step 2

Specify your domain information and take note of field number 5

Step 3

Select "Users" from the menu tree; now we need to tell the SA router which users will be connecting to the SSL portal to be authenticated against Active Directory.

Click "Apply" to save user information and verify new user is able to log into the SSL portal.

Step 4

Once the user attempts to log into the SA portal page you should see a logged event under "Security" in Active Directory. If successful the logged event would look like this:

*Log Name: Security*  
*Source: Microsoft-Windows-Security-Auditing*  
*Date: 2/10/2010 8:50:42 AM*  
*Event ID: 4768*  
*Task Category: Kerberos Authentication Service*  
*Level: Information*

*Keywords:* Audit Success

*User:* N/A

*Computer:* ATHENSDC.ATHENS.STORAGE.LOCAL

*Description:*

A Kerberos authentication ticket (TGT) was requested.

*Account Information:*

*Account Name:* a.gallego

*Supplied Realm Name:* ATHENS.STORAGE.LOCAL 

*User ID:* NSS\a.gallego

*Service Information:*

*Service Name:* krbtgt

*Service ID:* NSS\krbtgt

*Network Information:*

*Client Address:* ::ffff:192.168.50.254 

*Client Port:* 34458