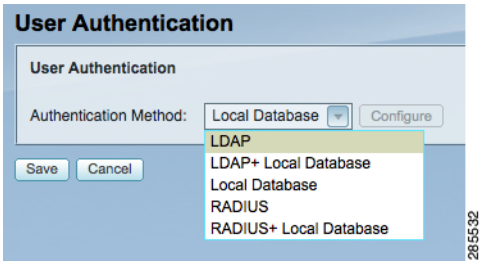
# Configuring the Cisco ISA500 for Active Directory/LDAP and RADIUS Authentication

This application note describes how to authenticate users on a Cisco ISA500 Series security appliance. It includes these sections:



User authentication is a way of identifying the user and verifying that the user is allowed to access restricted services. With authentication, a user can login to the network from any computer but can access only those resources for which they are authorized.

You can configure the ISA500 as a local authentication server, or choose from one or more authentication server types such as the Lightweight Directory Access Protocol (LDAP), or RADIUS servers as shown here.




## Configuring Active Directory/LDAP Authentication

The section describes how to configure the authentication using Active Directory through LDAP for the ISA500. It includes these sections:



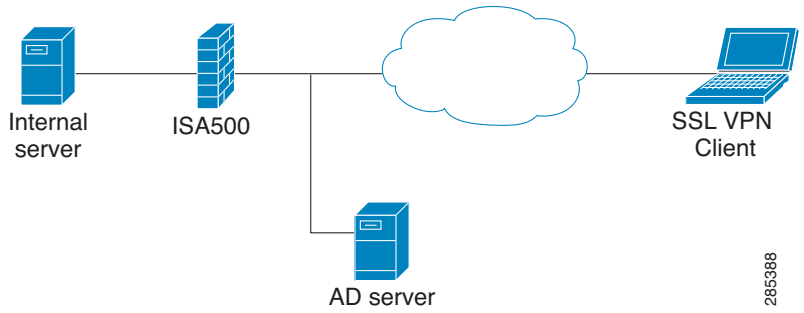
Before you begin, download and install the Cisco AnyConnect Client. This client is used to establish the SSL VPN tunnels and provides users with a secure VPN connection to the ISA500. For more information, see: http://www.cisco.com/en/US/products/ps8411/tsd_products_support_series_home.html

### Configuring an Active Directory Server

Active Directory (AD) is the Microsoft Windows-based application of an LDAP directory structure. Active Directory lets you expand the concept of domain hierarchy used in DNS to an organizational level and keeps information and settings in a central, easy-to-access database.

You can configure an Active Directory server so that SSL VPN Clients can authenticate to the ISA500 with their current network credentials. Figure 1 shows the ISA500 in an Active Directory topology.

**Figure 1** ISA500 in an Active Directory Topology




**NOTE** Before you begin, make sure that the Active Directory server is configured and is working properly.

Step 1. **Configure an SSL VPN Group Policy.**

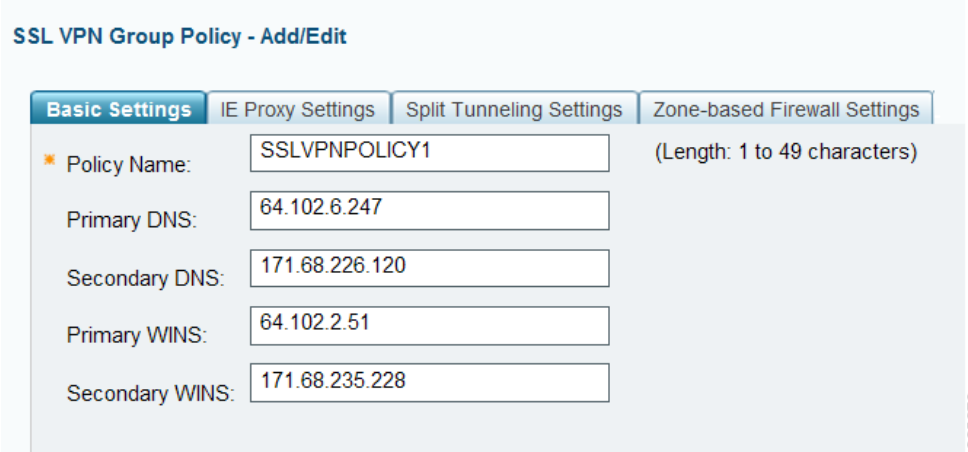
SSL VPN Policies give you control over which resources are accessed by certain SSL VPN groups and users. In this example, we created an SSL VPN Group policy “SSLVPNPOLICY1” and added a new group “ADGroup” that share this same policy.

a. Choose **VPN > SSL Remote User Access > SSL VPN Group Policies**.

b. Specify a name for the new policy. For example: SSLVPNPOLICY1.

c. Enter the **Primary** and **Secondary DNS** and **WINS IP** addresses.

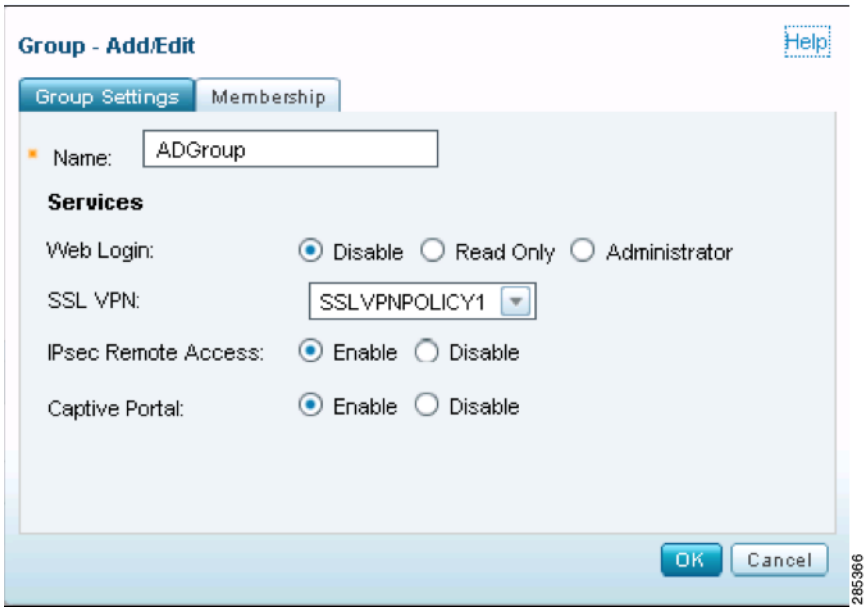
d. Click **OK** to save your settings.




**Step 2. Add a User Group.**

a. Choose **Users > Users and Groups**.

b. Click **Add**.



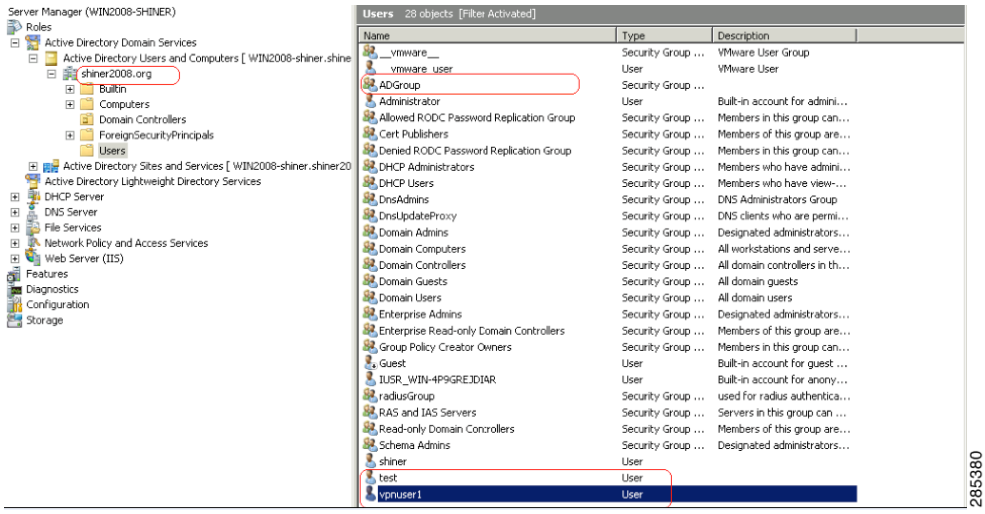

c. Enter a name for the user group. For example: ADGroup.

d. Choose the group policy you just created from the SSL VPN drop-down menu. For example: SSLVPNPOLICY1.

e. Click **OK** to save your settings.

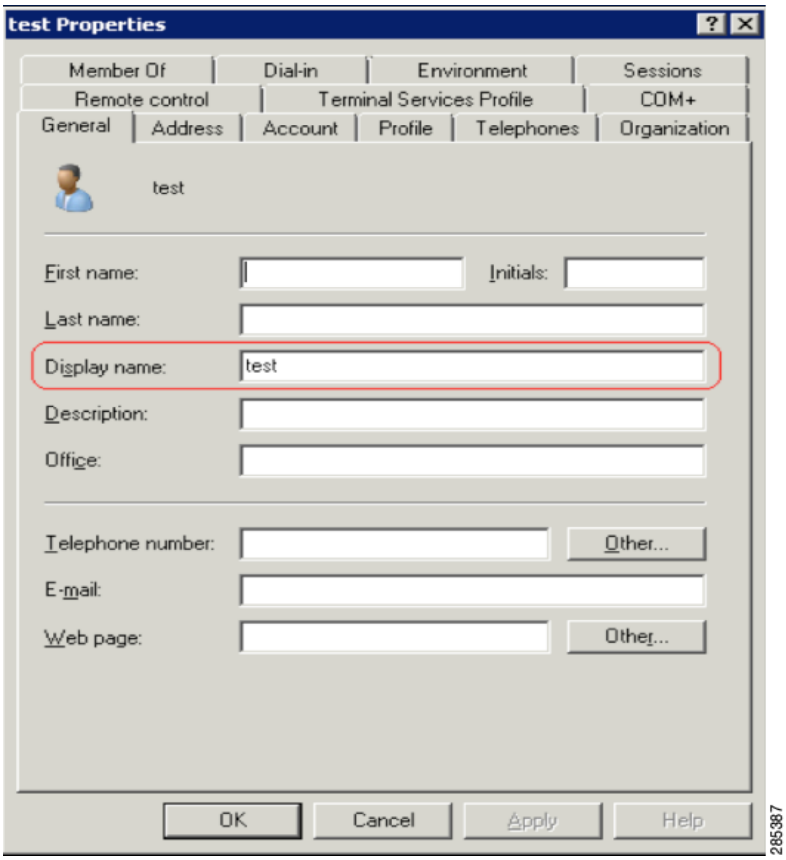
Step 3. Create an Active Directory domain.

In the following example the Active Directory domain is **shiner2008.org**.



Step 4. Create an account in the Windows Active Directory server.

In the following example, an account was created named **test** that was assigned LDAP read privileges.

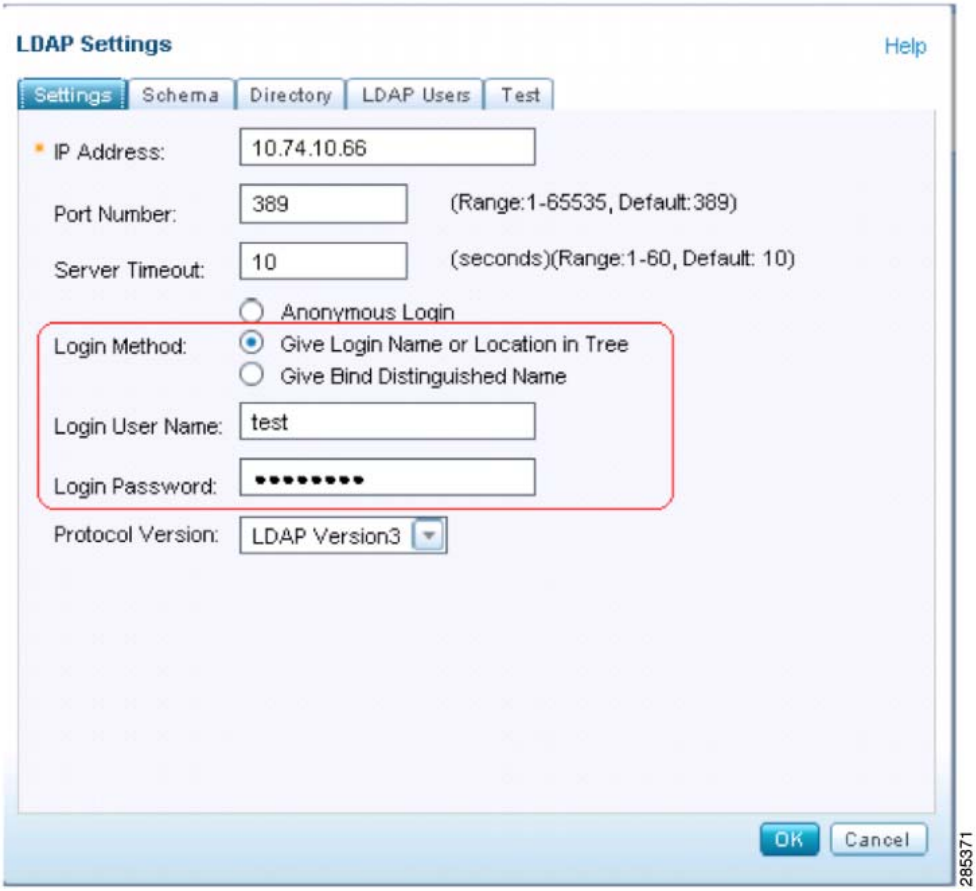



**Configuring LDAP authentication**

Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. LDAP is an open-standard protocol for using online directory services and operates with Internet transport protocols, such as TCP. You can use an LDAP server to authenticate your users with the ISA500.

a. Select **Users > Users Authentication.**

b. Choose **LDAP** from the drop-down menu and click **Configure**.



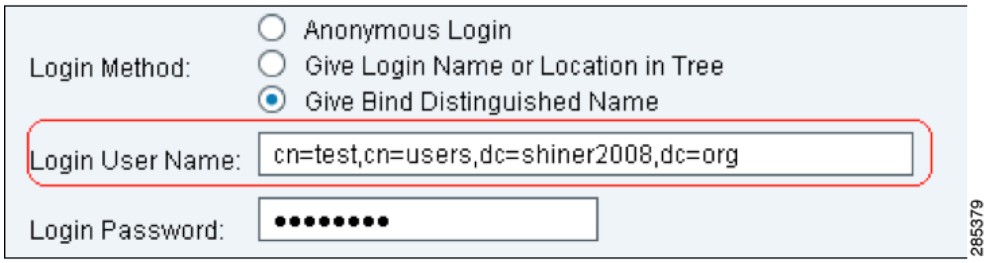

c. Specify the LDAP configuration settings

- **IP Address**: Enter the LDAP IP address of the Windows Active Directory server.
- **Port Number**: Enter the port number of the LDAP server. The default port number is TCP 389.
- **Login Method**:

  - If the LDAP server supports anonymous access, select the **Anonymous Login** option.

  - If you select **Give Login Name or Location in Tree**, enter the **Login User Name** and **Login Password**. The Login username must match the account name and have LDAP read privileges.

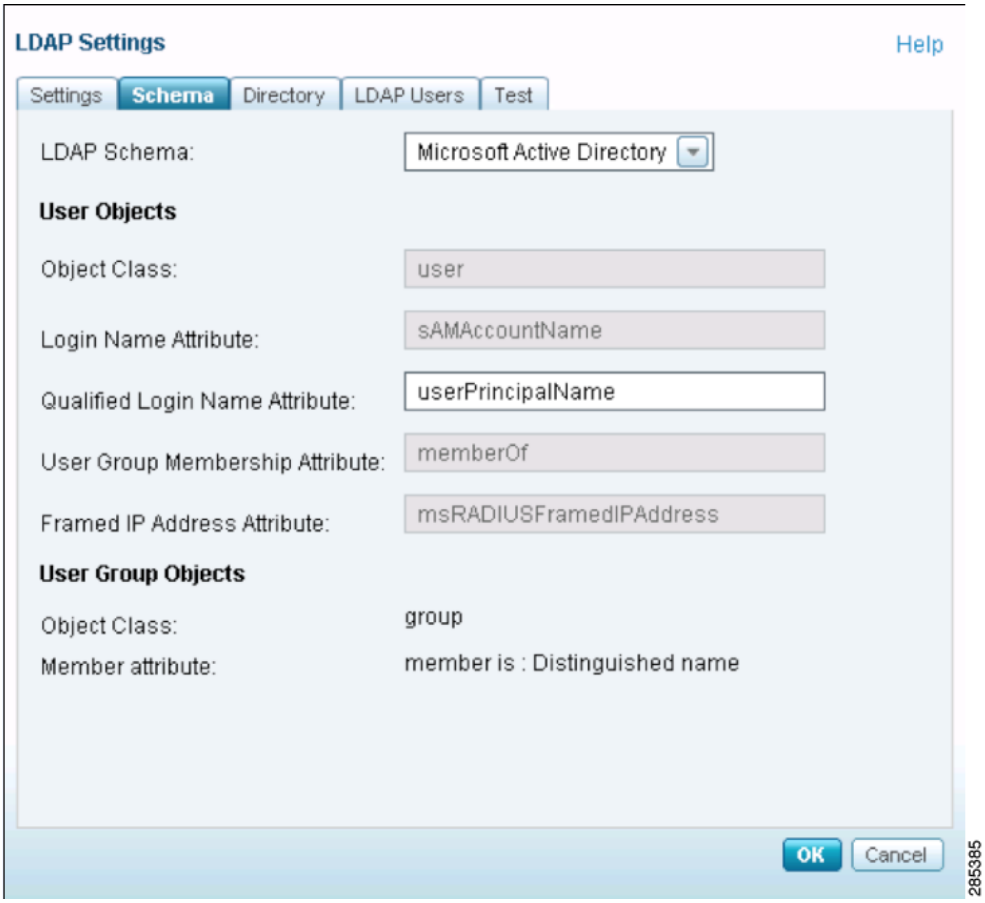
  - If you select **Give Bind Distinguished Name**, provide the full destination name explicitly to be used to bind to the LDAP server. In this example, the destination name is shown as: **cn=test,cn=users,dc=shiner2008,dc=org**.




- **Protocol version**: Choose the LDAP version from the drop-down list. Check your LDAP server for the version. Most LDAP servers, including Microsoft Active Directory, support LDAP version 3.

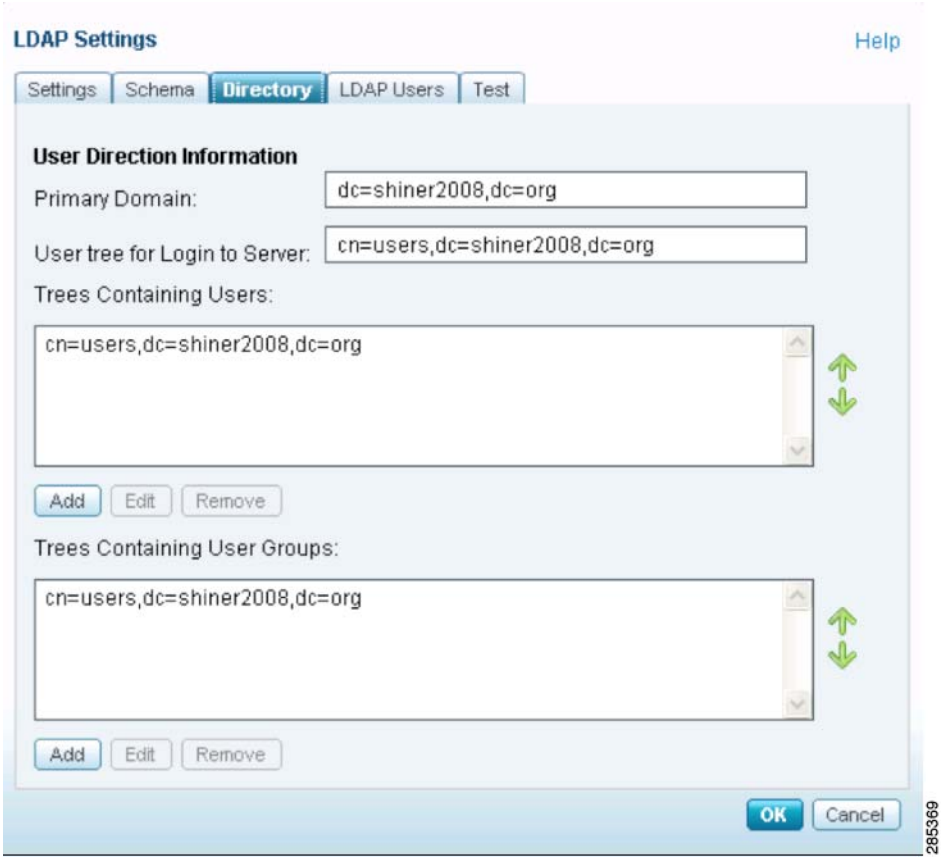
Step 5. Click the **Schema** tab.

The following example shows the Microsoft Active Directory Schema with the default values applied.



Step 6. Click **OK** to save your settings.

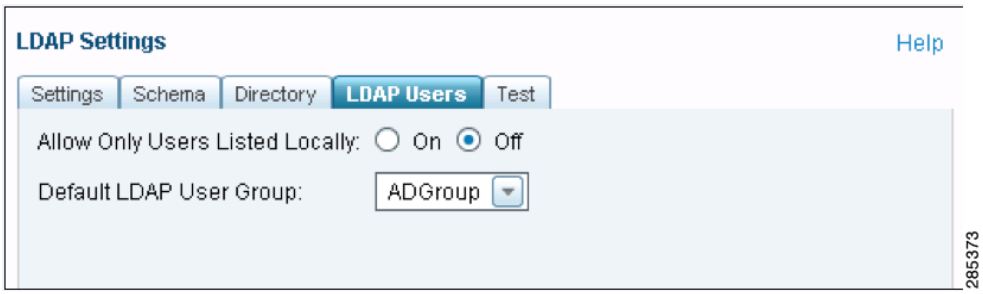
Step 7. Click the **Directory** tab.




Step 8. Enter the following information:

- **Primary Domain**: Input the user domain. All domain components use “dc=”. In this example the primary domain is: **dc=shiner2008,dc=org**
- **User tree for Login to Server**: Specify the user tree that is used to log into the LDAP server. You can only edit this option if you choose **Give Login Name** or **Location in Tree** in the Settings tab.

Step 9. Click the **LDAP Users** tab.



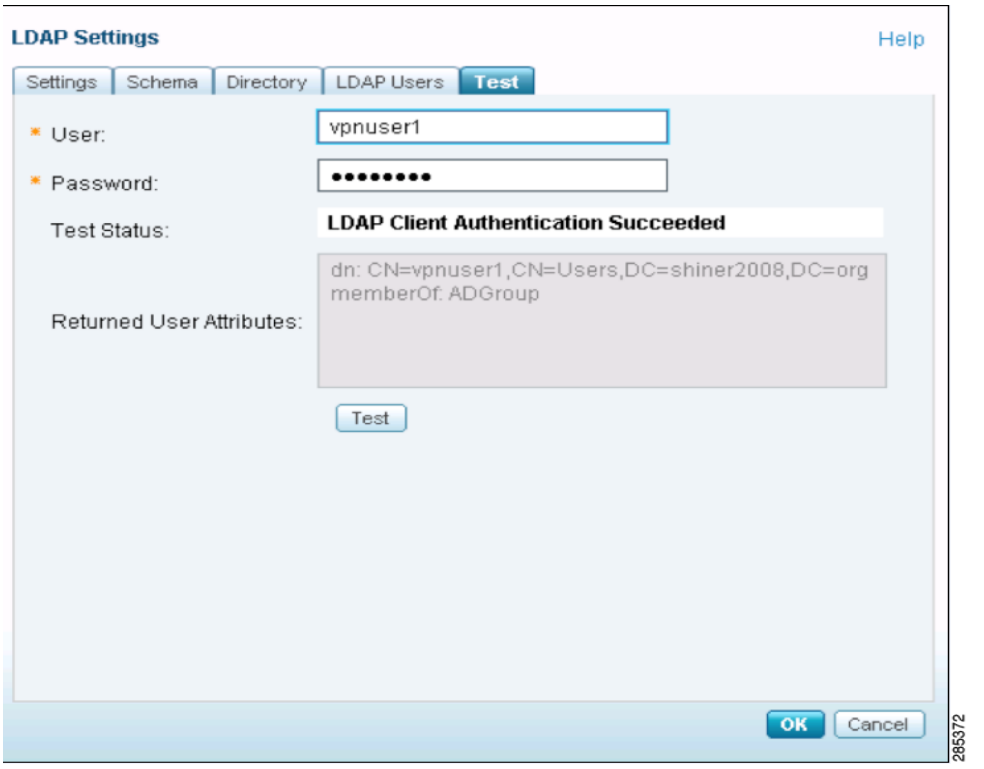

Step 10. Enter the following information:

- **Allow Only Users Listed Locally:** Click **On** to allow only the LDAP users who also are present in the local database to login. Choose **Users > Users and Groups** to view the local database configuration.
- **Default LDAP User Group:** Choose a local user group as the default group to which the LDAP users belong. If the group does not exist in the local database when retrieving the user group information from the LDAP server, the LDAP user is automatically set to the specified local user group.

Step 11. In the **Test** tab, enter the user's credentials in the **User** and **Password** fields.

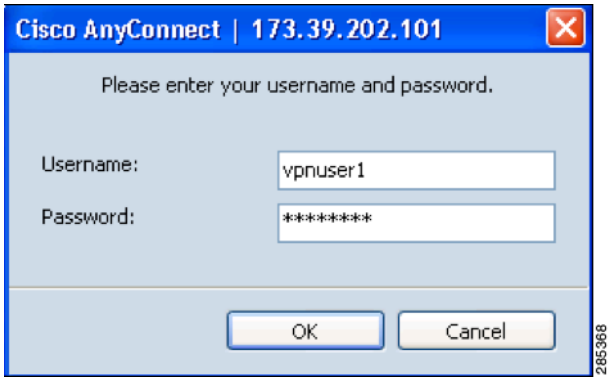
Step 12. Click **OK** to save your settings.

Step 13. To verify whether the LDAP user is valid, click **Test**.

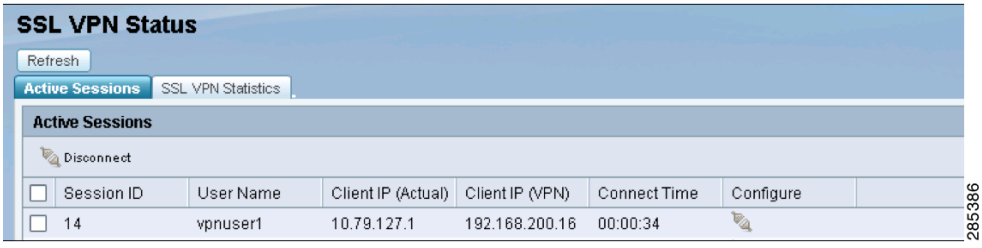


You can now use the Cisco AnyConnect VPN Client to establish SSL VPN tunnels.

For information about SSLVPN, refer to the application note, “Configuring SSLVPN on the Cisco ISA500 Security Appliance at: www.cisco.com/go/isa500resources.


After the tunnel is established, verify the connection from the **Status > VPN Status > SSL VPN Status** page. This example shows the session information for the VPN client.

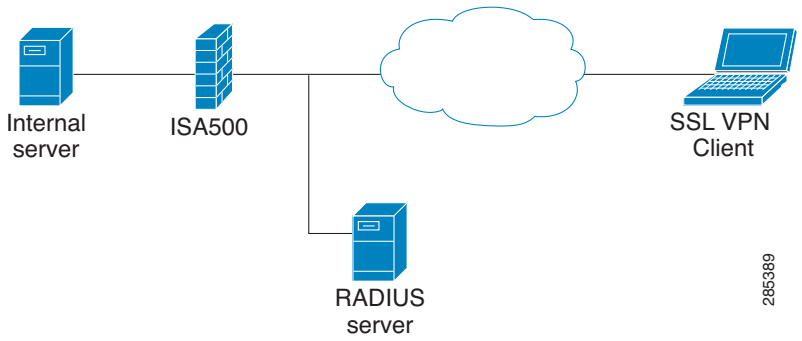


### Configuring RADIUS Server Authentication

RADIUS (Remote Authentication Dial-In User Service) authenticates local and remote users on a network. RADIUS is a client/server system that stores the authentication information for users, remote access servers, VPN gateways, and other resources in one central database. You can use a Cisco Secure Access Control Server (ACS) or FreeRADIUS as the RADIUS server. Figure 2 shows the ISA500 in a RADIUS server topology.

**NOTE** Before you begin, make sure that the RADIUS server is configured and is working properly.

**Figure 2** ISA500 in a RADIUS Server Topology

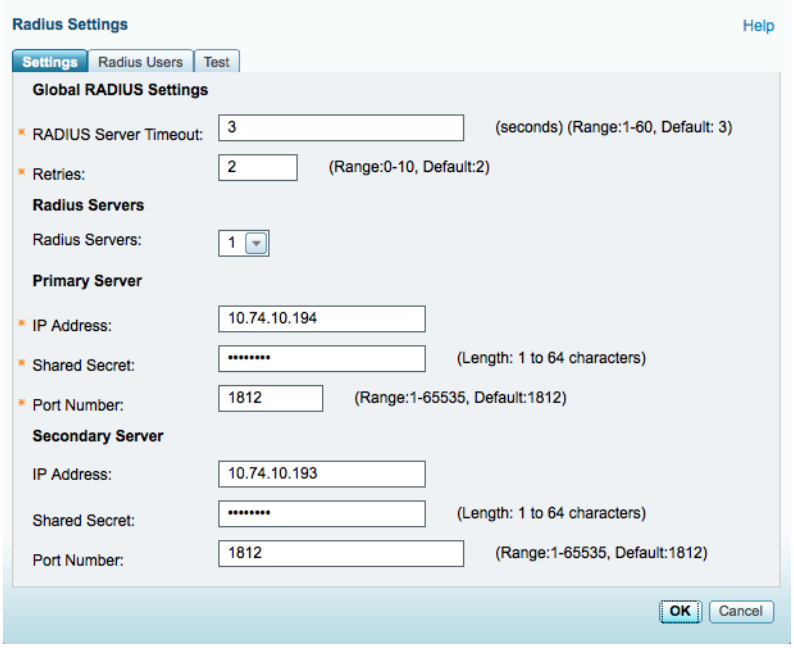



Step 1. Configure an SSL VPN Group Policy **SSLVPNPOLICY1** and add a new group **RADIUSGroup** that share this same policy. These steps are identical to the Active Directory server steps 1 and step 2 on page 10.

Step 2. Specify the user authentication method.

a. Select **Users > Users Authentication**.

b. Choose **RADIUS** from the drop-down menu and click **Configure**.

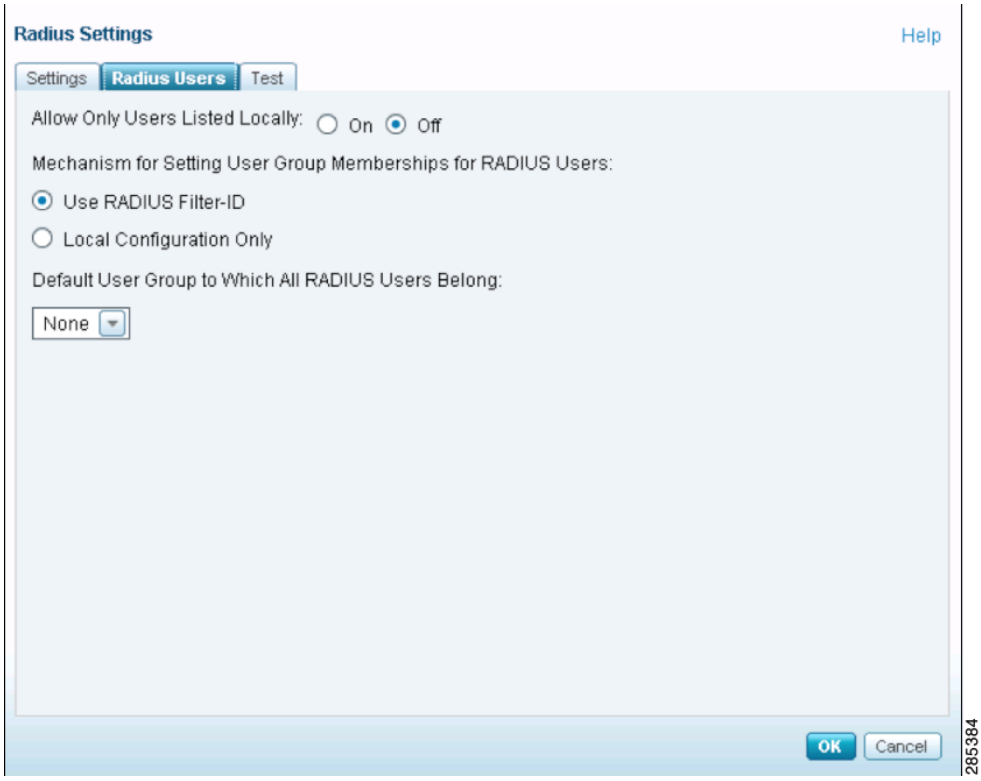



c. Specify the RADIUS configuration settings

- **RADIUS Server Timeout**: Enter the number of seconds that the connection is active before reauthentication is required. This value depends on your network connection. The default value is 3 seconds.
- **Retries**. Enter the number of times that the security appliance will try to resend the authentication message.
- **RADIUS Servers**: Choose the number of RADIUS user groups. You can have up to three groups (Group 1, Group 2, and Group 3).
- **Primary Server**: Enter the RADIUS server IP address, port number and shared secret information.
- **Secondary Server**: If applicable, enter the IP address, port number and shared secret information for the secondary RADIUS server.

d. Click **OK** to save your settings.

Step 3. Click the **RADIUS Users** tab and specify the user information.



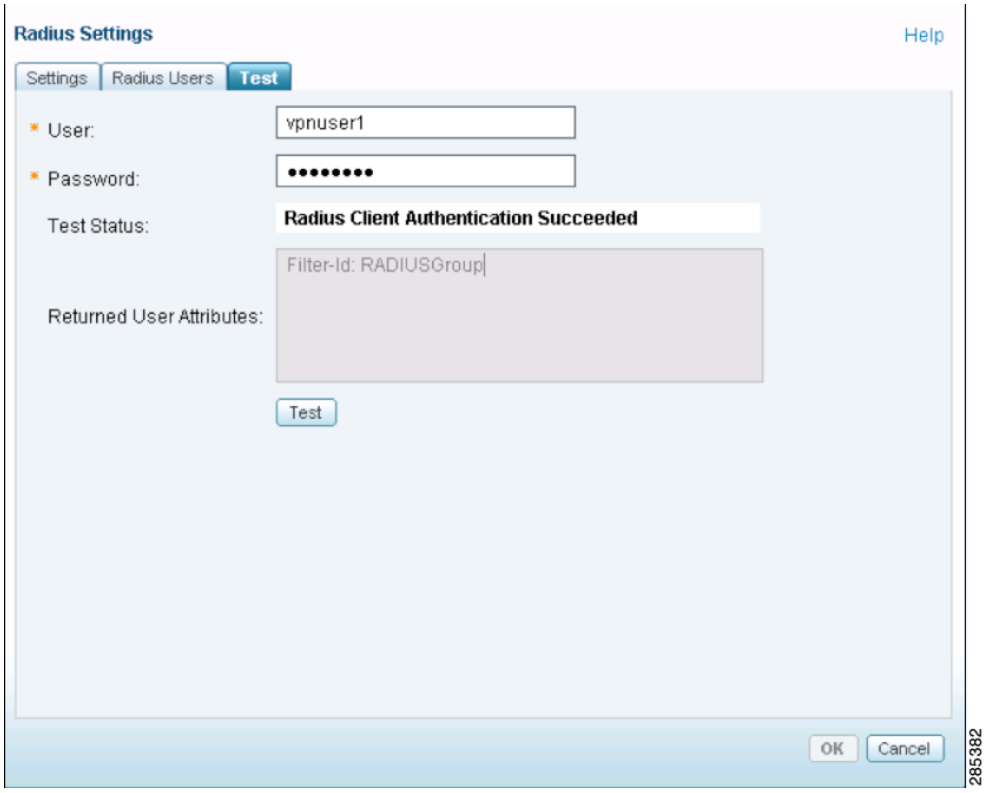

- **Allow Only Users Listed Locally:** Click **On** to allow only the RADIUS users (who also are present in the local database) to log in..
- **Mechanism for Setting User Group Memberships for RADIUS Users.** Choose one of the following:

  - **Use RADIUS Filter-ID:** Finds the user group information by using the Framed-Filter-ID attribute from the RADIUS server. The FreeRadius server uses attribute “Framed-Filter-Id”. For ACS Setup, see: http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html.

  - **Local Configuration Only**: Finds the user group information from the local database only. If the RADIUS server does not return a Filter-ID, choose this option. You will also need to add the users to the groups in the local database (See **Users > Users Authentication**).

- **Default User Group to Which All RADIUS Users Belong**: If the RADIUS server does not return the group name or if the group does not exist, you can add the user to this configured group. You can also choose **None** for security purposes.

Step 4. Click the **Test** tab and enter the user’s credentials in the **Username** and **Password** fields. Then click the **Test** button to verify whether the RADIUS user is valid.




Step 5. Click **OK** to save your settings.

You can now use Cisco AnyConnect to establish the SSL VPN tunnels.

## Troubleshooting

This section contains information that helps you resolve problems you might encounter when configuring the SSL VPN configuration. If Logging is enabled on the security appliance (**Device Management > Logs > Log Settings**), you can use the information in the syslogs for troubleshooting purposes.

- Why can't I authenticate 802.1x clients with an Active Directory server?

  Only a RADIUS server can be used for 802.1x authentication. An Active Directory server and the local user database is not supported. Web Login, SSL VPN, IPsec Remote Access, and Captive Portal can use either an external Active Directory or a RADIUS server or a local database.

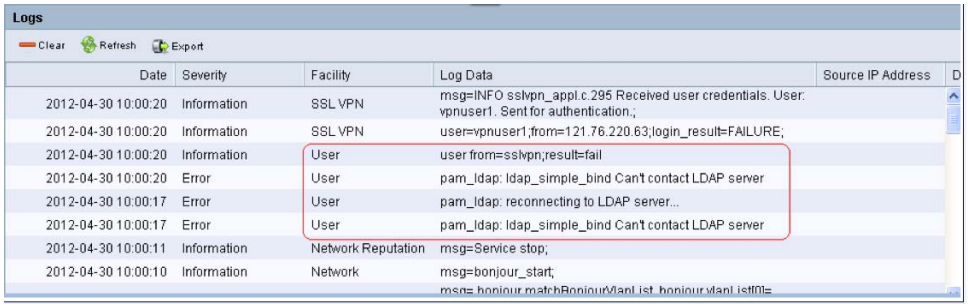
- Where should the Active Directory or RADIUS server be located, on the WAN side or the LAN side?

  Either side, as long the server is reachable from the ISA500.

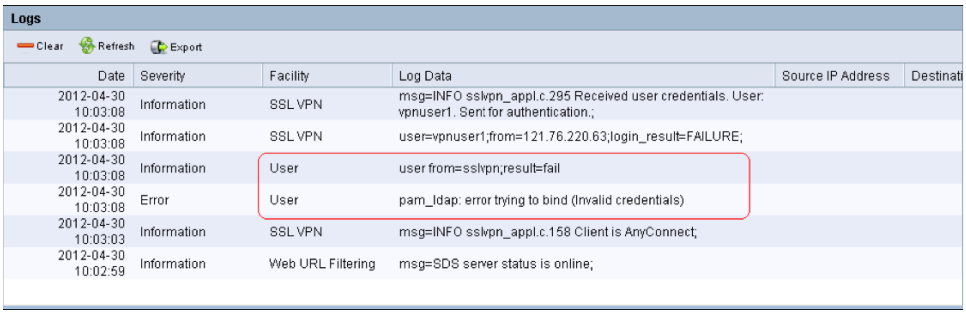
- Besides Microsoft Active Directory server, what else can I use as an LDAP server?

  The ISA500 supports three LDAP schemas; Microsoft Active Directory, RFC 2307 and RFC 2798. You can also use OpenLDAP (http://www.openldap.org/) or any other LDAP server which support these schemas.

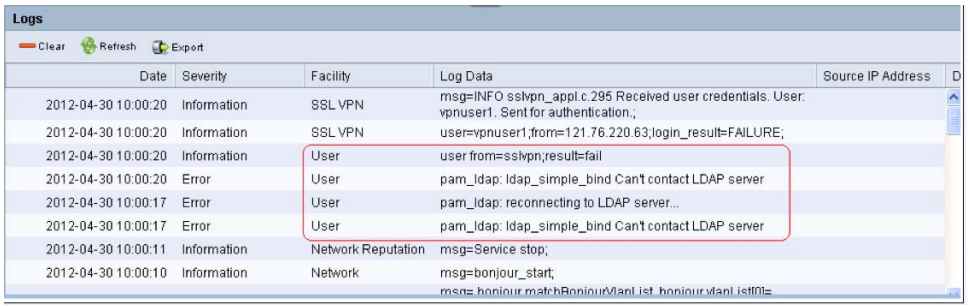
- Why is my AD/RADIUS server unreachable? When I check the user logs, it shows the following information:




Verify that the IP address and port number of the server is working properly. If you entered the wrong login username or password in the LDAP Setting page, the Logs page shows the following error:

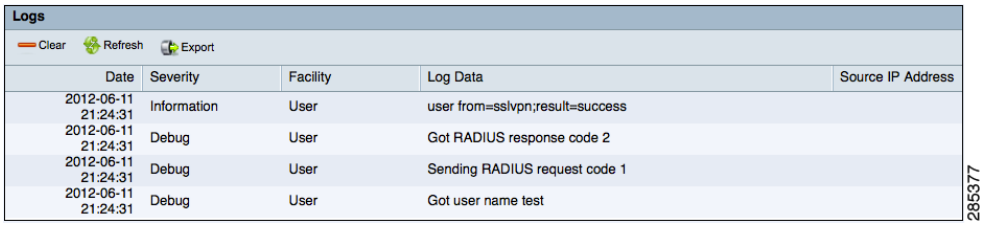



- What happens if I enter the wrong username and password for the SSL VPN client? The Logs page is showing the user as invalid.




To troubleshoot the problem, verify that the username and password for the SSL VPN client and Authentication server match.

For RADIUS authentication, you can also enable debug level logs to help troubleshoot. For instance, if you enter the wrong password for the SSL VPN client, the Log Data returns a response code. In the following example, the RADIUS response code 2 means Access-Accept. RADIUS response code 3 means Access-Reject.




- How can I verify that the LDAP or RADIUS settings are correct?

  a. Select **User > User Authentication**.

  b. Choose either LDAP or RADIUS. In the **Test** tab enter the user's credentials in the **Usename** and **Password** fields.

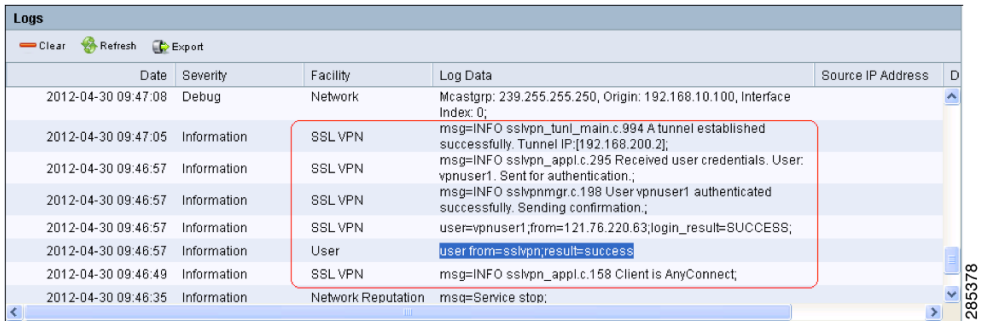
  c. Click **OK** to save your settings and then click **Test** to verify if the user is valid.

  If the authentication is successful but SSLVPN does not establish the tunnel, it may mean that the AD/RADIUS server returned the wrong group name.

  Check the AD/RADIUS server to verify that it returned the correct group name for the authenticated user, or specify a valid default user group to which all RADIUS users belong. See page 12 for more information.

- How do I know that the authentication was successful?

  When an VPN tunnel is established and user authentication is successful, the Logs page returns a success message. In the following example, the highlighted log shows "users from=sslvpn". It might also show "users from=captive portal", or "users from=weblogin", depending on which module initiates the authentication.



## For More Information

| Product Resources | Location |
|---|---|
| Product Documentation | www.cisco.com/go/isa500resources |
| Cisco Small Business Support Community | www.cisco.com/go/smallbizsupport |
| Cisco Small Business Support and Resources | www.cisco.com/go/smallbizhelp |
| Phone Support Contacts | www.cisco.com/go/sbsc |
| Firmware Downloads | www.cisco.com/go/isa500software |
| Cisco Partner Central for Small Business (Partner Login Required) | www.cisco.com/web/partners/sell/smb |
| Cisco Small Business Home | www.cisco.com/smb |