

---

## How to Configure Entrust IdentityGuard Authentication

<https://campus.barracuda.com/doc/41110961>The Barracuda SSL VPN can authenticate users with login information from Entrust IdentityGuard servers. When configured, the Java based RADIUS client sends authentication requests to the IdentityGuard server and allows access to the Barracuda SSL VPN unit based upon a success or failure message returned by the server. Specify the Barracuda SSL VPN as a RADIUS client on the IdentityGuard server, configure the RADIUS server settings on the Barracuda SSL VPN and set up a RADIUS authentication scheme for your users.

### Before you begin

---

You must have your IdentityGuard server configured to accept RADIUS requests from the Barracuda SSL VPN. To do this, specify the Barracuda SSL VPN IP address as a RADIUS client on the server.

### Step 1. Configure the RADIUS server

---

1. Open the **Management System > ACCESS CONTROL > Configuration** page.
2. Enter the following information in the RADIUS section:
  - **RADIUS Server** - Enter the hostname or IP address of the IdentityGuard server.
  - **Authentication Port** - Enter 1812.
  - **Shared Secret** - Enter the shared secret. This passphrase must be configured on the IdentityGuard server.
  - **Authentication Method** - Select **PAP**.
  - **Reject Challenge** - Disable in order to receive additional RADIUS prompts such as change PINs prompts.

**RADIUS**
Save Changes Help

RADIUS Server:

Backup RADIUS Servers:

Hostname	Hostnames

Host names of backup RADIUS Servers.

Authentication Port:  This is the port number stipulated for the RADIUS authentication process. It **MUST** be a valid integer port between 0 and 65535. Default (1812).

Accounting Port:  This is the port number stipulated for the RADIUS accounting process. It **MUST** be a valid integer port between 0 and 65535. Default (1813).

Shared Secret:  The RADIUS shared secret which has been set up on the RADIUS server.

Authentication Method:  If your server does not use a specific authentication method, this value is ignored. The only methods that are currently supported in this configuration are **PAP**, **CHAP**, **MSCHAP** and **MSCHAPv2**.

Time Out:  The timeout for a RADIUS message.

Authentication Retries:  The number of retries for a RADIUS message.

RADIUS Attributes:

Attribute	Attributes

The RADIUS attributes required to execute the request.

Username Case:   
 As Entered   
 Force Upper Case   
 Force Lower Case   
Setting that defines what case the username is sent to the RADIUS server. Options are to leave as entered, force to upper case or force to lower case.

Password Prompt Text:  Customize the RADIUS password prompt text.

Reject Challenge:  Yes  No Reject a challenge-response request from the RADIUS server. Default (true)

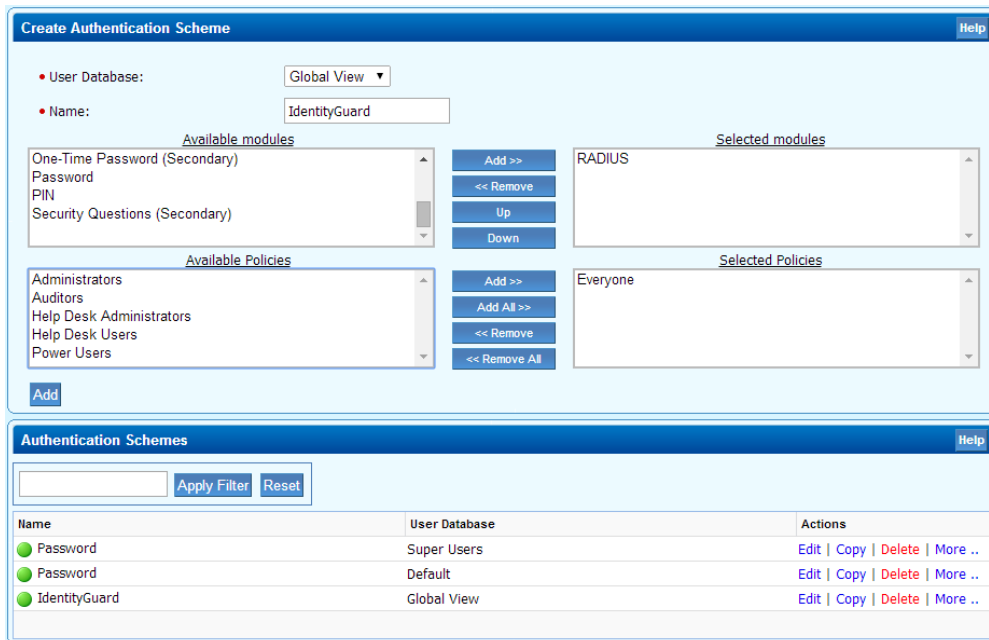
Challenge Image URL:  A URL for generated challenge images. Leave blank to disable.

Allow Untrusted Challenge Image URL:  Yes  No Allow Challenge Images to be server from untrusted servers.

3. Click **Save Changes**.

## Step 2. Create an authentication scheme

1. Go to the **Manage System > ACCESS CONTROL > Authentication Schemes** page.
2. Create an authentication scheme which contains the RADIUS module (select *RADIUS*, click **Add**). You may add more modules if you wish to have multi factor authentication.
3. Select a policy which will be able to use this authentication (e.g. *Everyone*) and click **Add**.

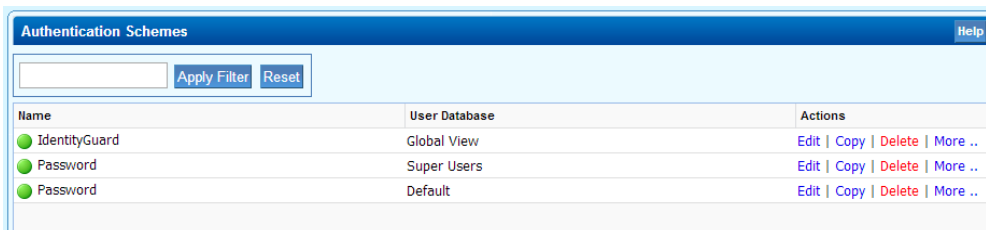


The screenshot shows two panels from the Barracuda SSL VPN management interface. The top panel, titled "Create Authentication Scheme", has a "Global View" dropdown for "User Database" and "IdentityGuard" entered in the "Name" field. It features two lists: "Available modules" (One-Time Password (Secondary), Password, PIN, Security Questions (Secondary)) and "Selected modules" (RADIUS). Below these are "Available Policies" (Administrators, Auditors, Help Desk Administrators, Help Desk Users, Power Users) and "Selected Policies" (Everyone). Buttons for "Add >>", "<< Remove", "Up", "Down", "Add All >>", "<< Remove", and "<< Remove All" are present. An "Add" button is at the bottom left. The bottom panel, titled "Authentication Schemes", has a search filter and "Apply Filter" and "Reset" buttons. It displays a table of existing schemes:

Name	User Database	Actions
● Password	Super Users	Edit   Copy   Delete   More ..
● Password	Default	Edit   Copy   Delete   More ..
● IdentityGuard	Global View	Edit   Copy   Delete   More ..

#### 4. Click **Add**.

The new scheme is now listed in the **Authentication Schemes** section, this may be set as the default module by clicking **More..** next to the entry and choosing **Increase Priority** until it appears at the top of the list.



The screenshot shows the "Authentication Schemes" panel with the "IdentityGuard" scheme now at the top of the list:

Name	User Database	Actions
● IdentityGuard	Global View	Edit   Copy   Delete   More ..
● Password	Super Users	Edit   Copy   Delete   More ..
● Password	Default	Edit   Copy   Delete   More ..

### Step 3. Test the IdentityGuard authentication

To log into the Barracuda SSL VPN using Entrust IdentityGuard authentication, create a user account to match the RADIUS login name. Alternatively, if you are using an Active Directory or LDAP server, ensure this account exists on the user database. To create a new user account,

1. Go to the **Manage System > ACCESS CONTROL > Accounts** page.
2. Enter a username and password and click **Add**.

To test the authentication, log in as the user:

1. Enter the username and click **Login**.

## Barracuda | **SSL VPN**



© 2003-2014 Barracuda Networks, Inc.

2. Enter the password and click **Login**.
3. Work out the passcode based on the grid.

You are now logged into the Barracuda SSL VPN.

## Figures

1. id\_guard01.png
2. id\_guard02.png
3. id\_guard03.png
4. id\_guard05.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.