

BiGuard SSL VPN Security Gateway

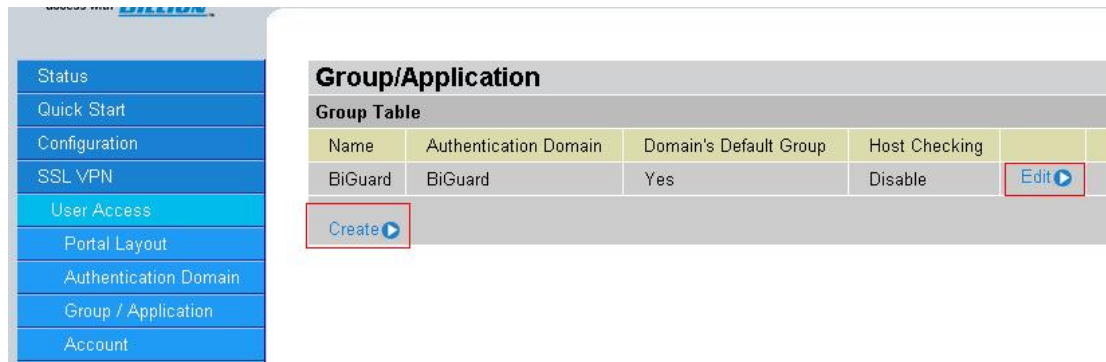
Password Policy Configuration Guide

1. Introduction

- Set the password policy for the Group to enable all the group users to follow the password policy to ensure the safety of the user accounts.
- In the Group setting screen, configure all the settings associated with the password policy and enable the function.

2. Settings

2-1 Input **admin** in the **User Name** filed to access Router. Select **SSL VPN >> User Access >> Group / Application**. Press **Edit** to access **Edit Group** configuration screen to edit the current group's password policy. User can also press **Create** to create a new group, and set the password policy for the new group.



2-2 Press **Create** to access **Add Group** configuration screen. Enter a group name, enable Password policy, and then press **Advanced Setting**.

Add Group	
General Settings	
Group Name	test
Domain	BiGuard
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Advanced Setting
Inactivity Timeout	5 Minutes
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Service	
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Advanced Setting <input type="checkbox"/> Standalone Application (Win32 Only)
Transport Extender Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable Advanced Setting
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network Extender IP Assignment	<input checked="" type="radio"/> Dynamic Assign <input type="radio"/> Fix IP 192.168.1.240
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom Welcome to SSL VPN St:

2-3 Then, you will access the **Password Policy** configuration screen where you can configure the password rules.

Password	
Parameters	
Group Name	BiGuard
Password Rules (Must Contain)	<input type="checkbox"/> Minimum 8 characters
	<input type="checkbox"/> Lowercase
	<input type="checkbox"/> Uppercase
	<input type="checkbox"/> Special Symbols
Default Password	
Retype Default Password	
Retry Password Count	0 Times
Retry Password Timeout	0 Minutes
Allow Password Change	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply Cancel

Password Rules: Minimum 8 characters (The password must contain 8 characters at least.)

Uppercase (The password must contain uppercase letters.)

Lowercase (The password must contain lowercase letters.)

Special Symbols (The password must contain special symbols.)

Default Password: Indicates the default password of the group


Retry Password Count: Specifies the number of times that you may attempt to enter the password to log on. If you fail to enter the password in the set number of times, you will be locked out of your account. For example, if you enter value 3 for **Retry Password Count** field, it indicates your will be locked out of your account if you fail to provide a correct password for more than 3 times.

Retry Password Timeout: Specifies the period of time that the account will be locked. If you set the timeout value to 5 in this field, it indicates you will be locked out of your account for 5 minutes, but you will be allowed to log on after 5 minutes are elapsed.

Allows Password Change: Allow the user to change the password on the **Portal** screen.

3. Check the Use group default password option to allow the new account to inherit the default password of the Group.

Note: that no entries are allowed for the password field after **Use group default password** is checked.

Add Account		
General Setting		
User Name	<input type="text" value="test"/>	<input checked="" type="checkbox"/> Active
Group 	<input type="text" value="BiGuard"/>	
Password	<input type="text"/>	
Retype Password	<input type="text"/>	<input checked="" type="checkbox"/> Use group default password
Force Login	Enable <input type="radio"/> Disable <input type="radio"/>	
Inactivity Timeout	<input type="text" value="5"/> Minutes	
Host Checking	<input checked="" type="checkbox"/> Active	Advanced Setting

3. Changing the User Password

3-1 When you log on to the Portal page, you will see the password button on the top right corner of the page if the Group allows user to change the password.



BiGuard S5 - SSL VPN Starter Pack



3-2 After the password button is pressed, a password parameter window will be popped up as illustrated below:

Enter the new password you prefer in the **Password** field, and type the new password again in **Retype Password** field. Click **Apply** to confirm.

Password	
Parameters	
User Name	admin
Password	••••••••
Retype Password	••••••••
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3-3 After the new password is set, a notification message will be displayed to inform you that the password has been changed successfully.

Note that next time when you need to log on to the **Portal** page, remember to enter the new password set above before you can log on to the page successfully.



###

© Billion Electric Co., Ltd. All rights reserved.

BiGuard User Registration: <http://www.biguard.com/>

Technology Support: support@billion.com

E-mail: sales@billion.com, marketing@billion.com

Billion Global Website: <http://www.billion.com/>