Software Update License, and Service License Expiration Date.

Device License: The device license activates the device and authorizes the number of lines, number of branches, and mobile users.

Multi-Function License: The function license activates multi-function authorization, including the VPN, audit (including behavior audit and content audit), data center USB Key check, and SSL monitoring functions.

Security License: The antivirus SN authorizes the upgrade of the virus definition library of the antivirus module.

Application Signature Database: This license activates the update validity period of embedded libraries, including the URL Database, application identification library, and audit rule library.

Software Update License: This license upgrades the software of the device.

Third-Party URL Database License: This license activates the update validity period of the URL Database from third parties.

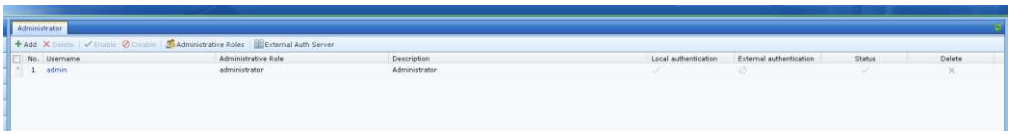
Sangfor URL Database: This license activates the update validity period of the URL Database from Sangfor.

Click **Edit** and enter the license to activate the authorization of the corresponding function.

3.11.5.2 Administrators

On the **Administrator** page, you can set a user account for managing the device

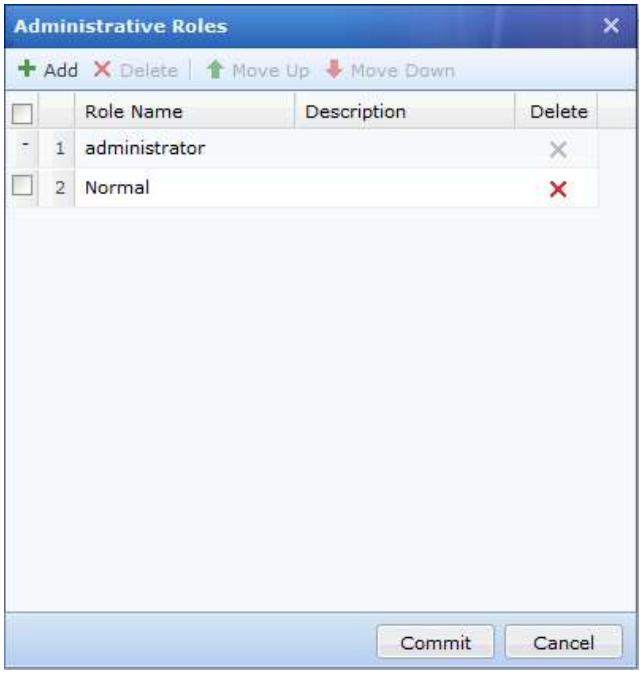
on the console. Navigate to **System** > **General** > **Administrators**. The **Administrators** pane is displayed on the right, as shown in the following figure.



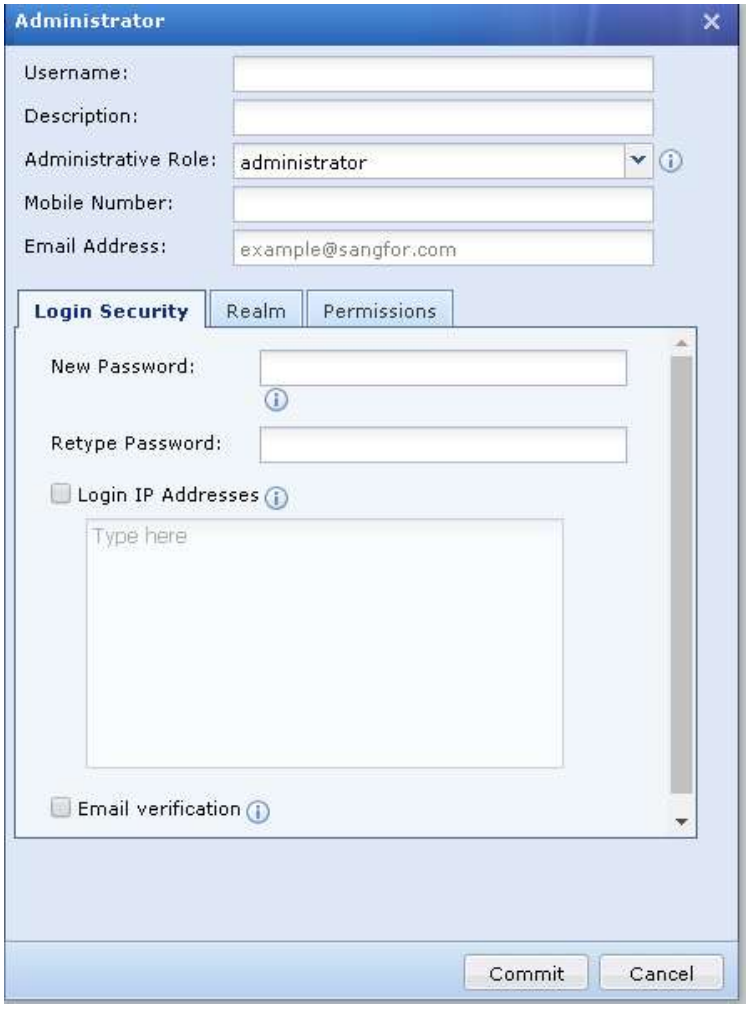
Click **Add** to add an administrator account, **Delete** to delete an administrator account, **Enable** to enable an administrator account, **Disable** to disable an administrator account, or **Administrative Role** to define the permission of an administrator account. When multiple administrators are required for hierarchical management, you need to define the permission level of each administrator. In the administrator account list, administrator accounts are displayed in descending order of permission level. If two administrators share the same jurisdiction scope, the administrator with a higher permission level can modify the policy created by the administrator with a lower permission level. The policy created by the administrator with a higher permission level takes precedence over that created by the administrator with a lower permission level. The role of the **administrator** is embedded. An account with the **administrator** role can manage the entire organization structure and add and delete administrator accounts.

Example 1: Add a console administrator.

1. Add a role. Different roles have different priorities. The administrator accounts are displayed in descending order of priority. An administrator with a lower priority cannot modify objects created or modified by an administrator with a higher priority. Click **Administrative Role**. The **Administrative Role** dialog box is displayed. Click **Add**, enter the username and description of the role to be added, and click **Commit**.



2. Create an administrator account. Click **Add**. The **Administrator Roles** dialog box for creating an administrator account is displayed. Set related parameters on the **Login Security** tab.

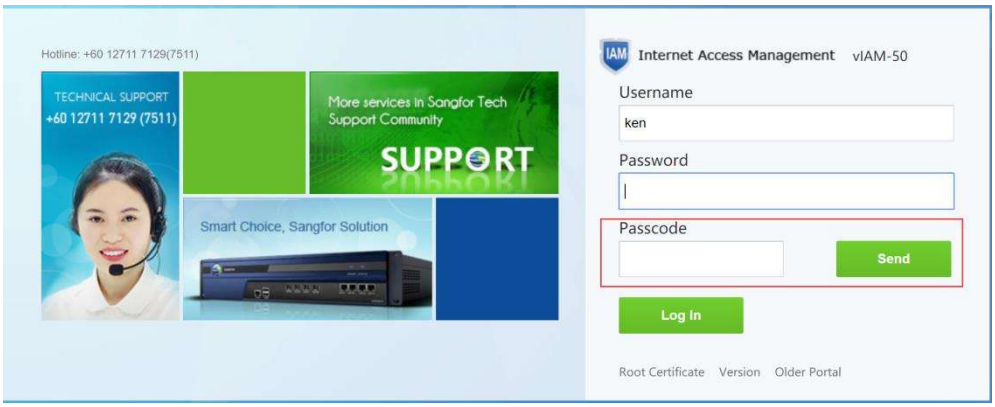


Username: Enter the account username for logging in to the console.

Administrator Role: Select the role defined in step 1.

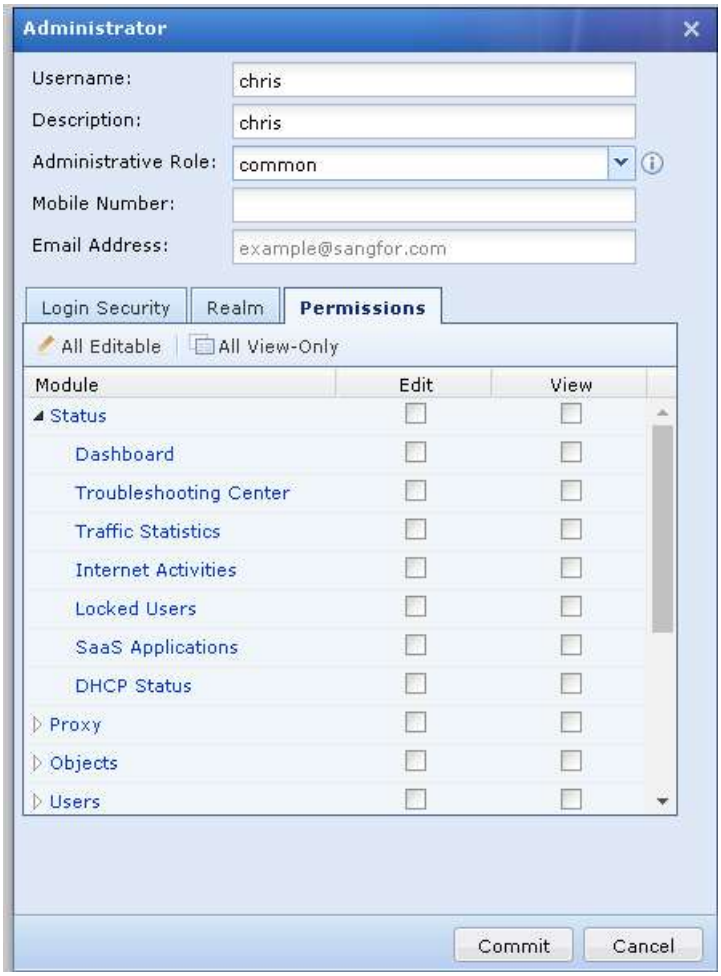
Login Security: Enter the account's password for logging in to the console in **New Password** and **Retype Password**. You can also set the IP address used by the administrator account to log in to the console. You can set a single IP address or an IP address segment. Set one IP address in each row and can set a maximum of 32 rows.

Mail Verification: By enabling it, entering users who need mail verification on the gateway console will automatically pop up the verification code acquisition and input box.



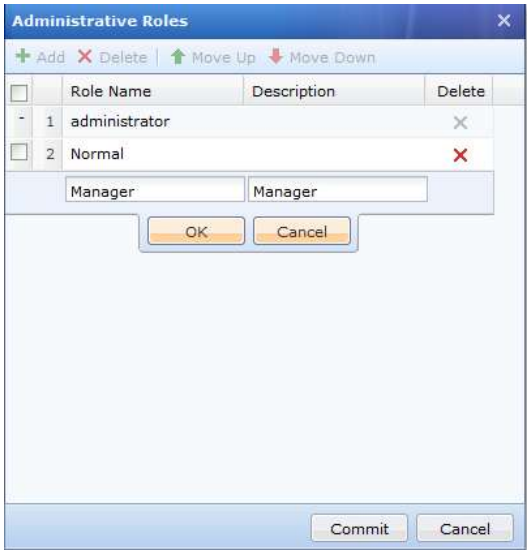
3. On the **Realm** page, set the permission for the added administrator account to manage a user group. Click **Select** and select a group in the displayed organization structure.

4. In **Permission**, set whether the administrator account can view or edit other modules on the console.

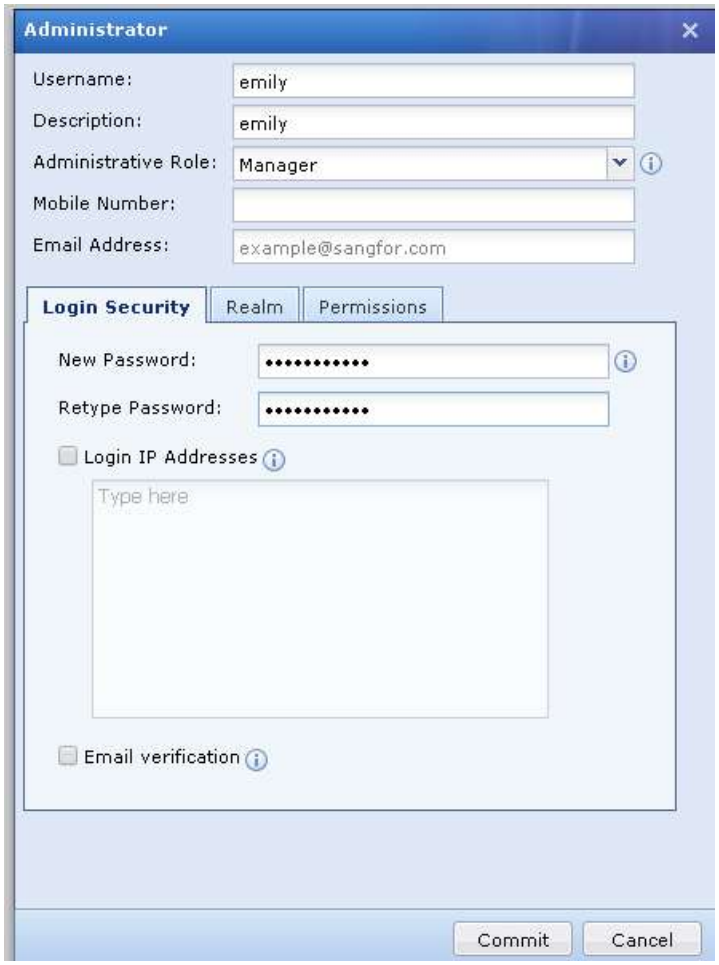


Example 2: Create an administrator role **Manager,** and an administrator account **emily**. Set the password to **@1234abcd**. Grant permission to manage the Director Group and view and edit the **Users** and **Object** pages. Assign the role **Manager** to the administrator account.

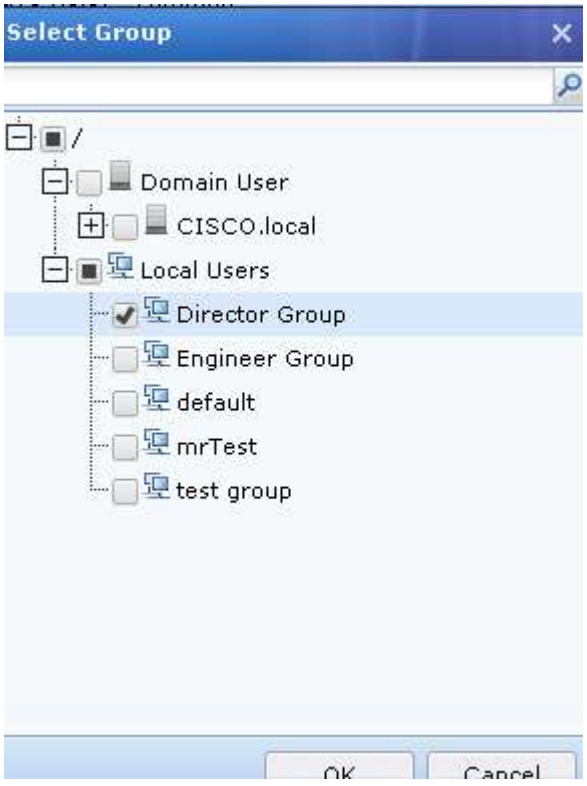
1. Add a role. On the **Administrator** page, click **Administrative Roles**. In the **Administrative Roles** dialog box, click **Add**, enter the role name **Manager** and description of the role, and click **OK.**



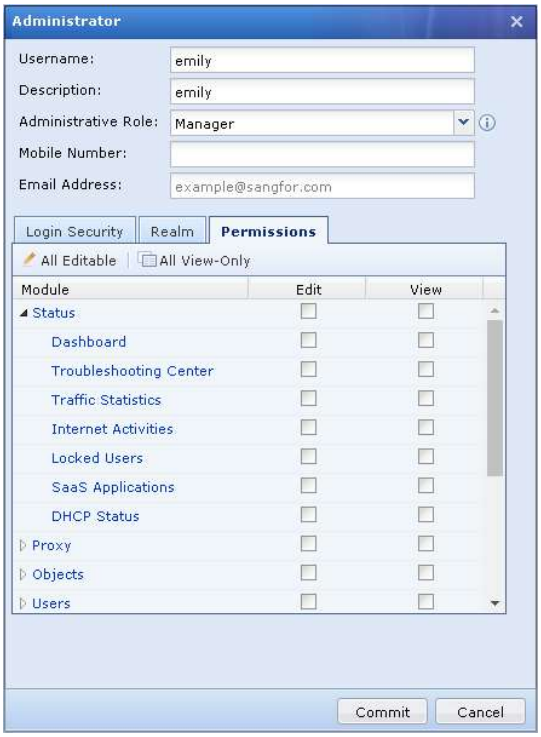
2. Create an administrator account. On the **Administrator** page, click **Add**. In the **Administrator** dialog box, enter the username **emily** and description of the account, and select the role **Manager**. On the **Login Security** page, enter the password **@1234abcd** and confirm the password.



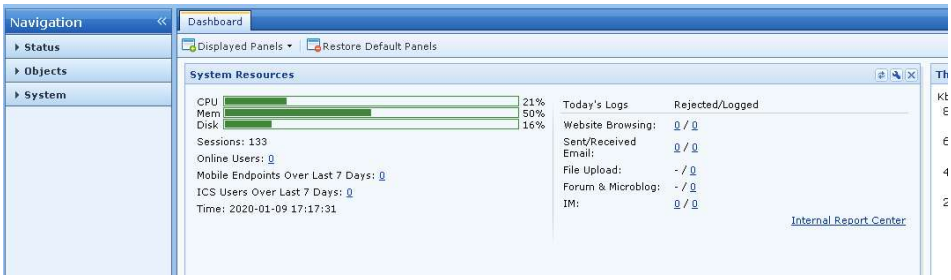
3. On the **Realm** page, click **Select**, select **Director Group** in the displayed organization structure, and click **Commit**.



4. On the **Permission** page, grant permission for viewing and editing the **Users** and **Object** pages and click **Commit**. The administrator account **emily** is created and associated with the role **Manager** successfully.

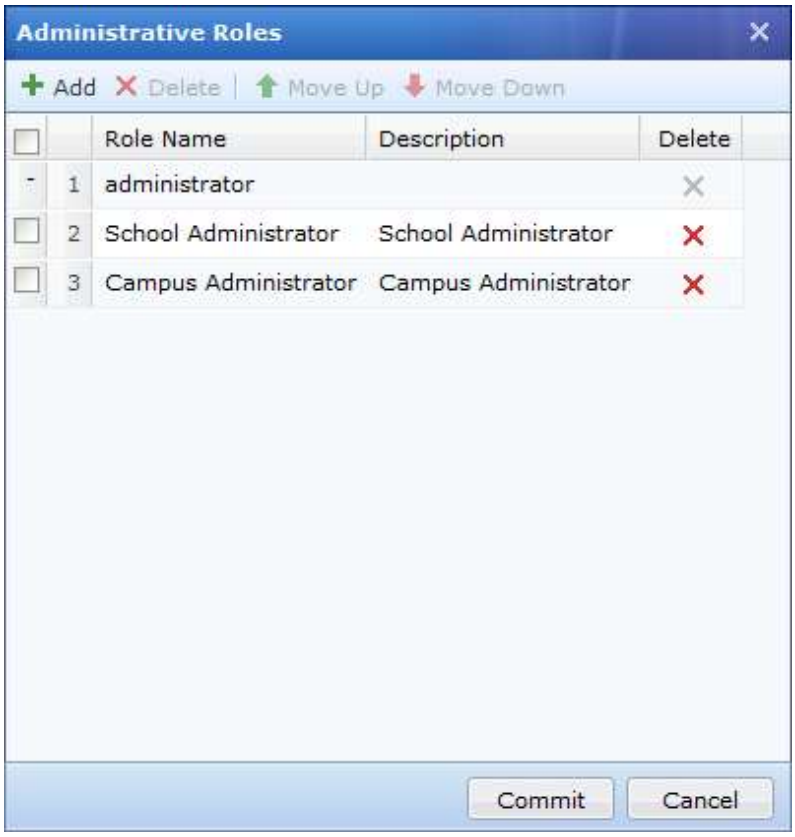


5. Log in to the console with the account **emily**. You can view online users in the **Network department** group and mail approval information, manage the **Director Group** group and Internet access policies, Objects, and set user authentication.

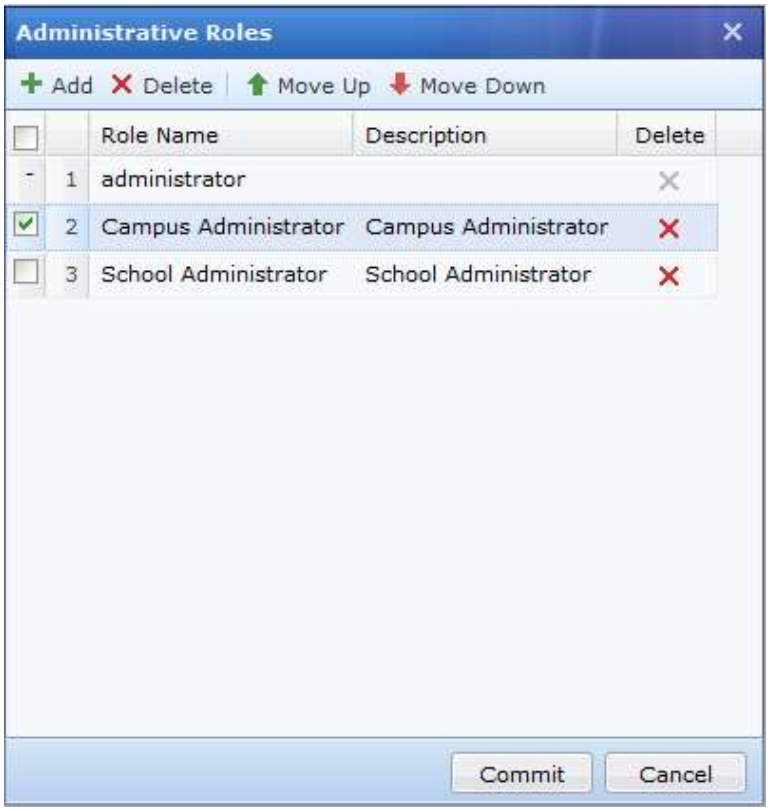


Example 3: Add two administrator roles, **Campus administrator** and **School administrator**, and two administrator accounts **test1** and **test2**. Associate **test1** to the **Campus administrator** role, which can manage all students. Log in as **test1** and define a policy to prevent all students from playing games in class. Associate **test2** to the **School administrator** role, which can manage the computer school students. Log in as test2 and define a policy to prevent computer school students from accessing Facebook in class.

1. Add two administrator roles: Campus administrator and School administrator.

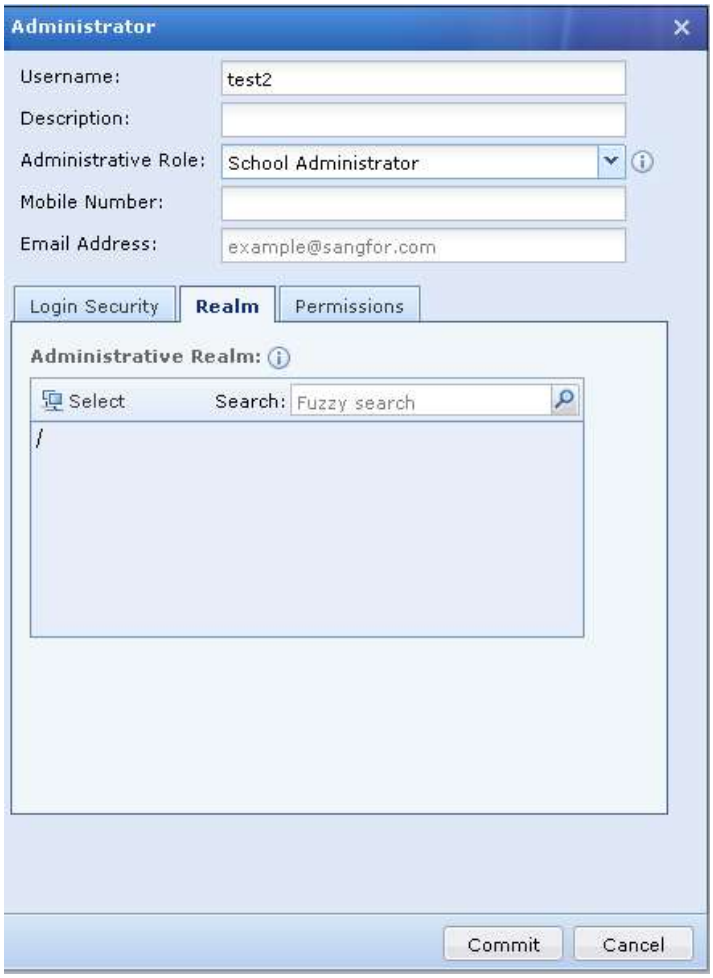


In the Administrative Roles list, roles are displayed in descending order of permission level. As shown in the following figure, the permission level of the **Campus administrator** role is higher than that of the **School administrator** role.

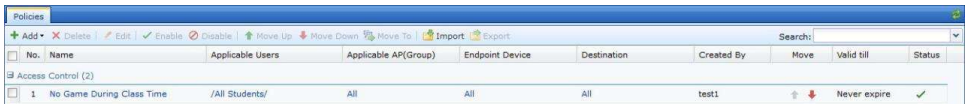


2. Create two administrator accounts **test1** and **test2**. Associate **test1** to the **Campus administrator** role, which can manage all students. Associate **test2** to the **School administrator** role, which can manage the computer school students.


Administrator
Username:
test1
Description:
Administrative Role:
Campus Administrator
Mobile Number:
Email Address:
example@sangfor.com
Login Security
Realm
Permissions
Administrative Realm:
Select
Search:
Fuzzy search
/All Student/
Commit
Cancel



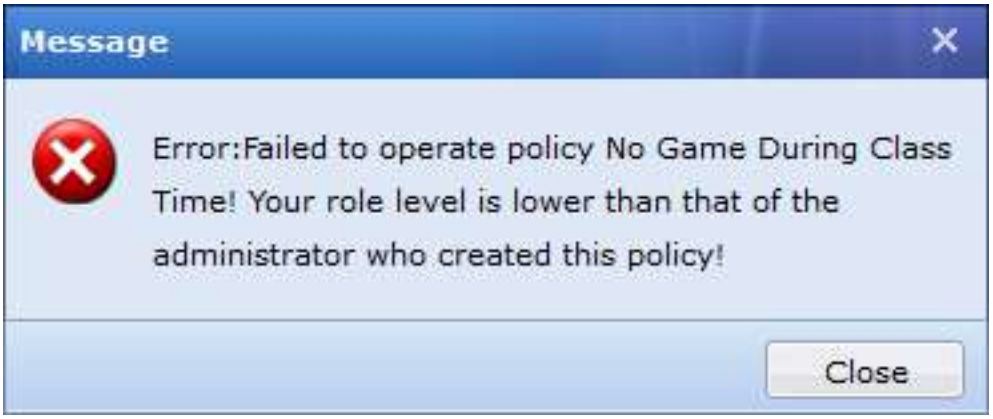
3. Log in to the console with the administrator account **test1** and define the **No Game During Class Time** policy, which applies to the **All-students** user group. For details about defining a policy, choose **Access Mgt** > **Policies**. See the following figure.



4. Log in to the console with the administrator account **test2** and define a No **Facebook policy during Class Time**, which applies to the **IT school** in **All students** user groups. For details about defining a policy, choose **Access Mgt** > **Policies**. See the following figure.

The priority of a policy depends on the permission level of the role that creates this policy. The policy created by the campus administrator takes precedence over that created by the school administrator. If the campus administrator **test1** selects **Give view privilege to administrator in lower-level role**, the school administrator **test2** cannot modify the policy defined by **test1**. Only the school

administrator has permission to view the policy. See the following figure.



An administrator cannot modify the Internet Access Policy defined by another administrator of the same permission level if their jurisdiction scopes are different. For example, **test2** and **test3** are associated with the **Campus administrator** role, but **test2** is authorized to manage the computer school, and **test3** is authorized to manage the management school. The two administrators cannot modify the Internet Access Policy defined by the peer.

NOTE

1. The role determines the level of an administrator. In the Administrative Roles list, roles are displayed in descending order of priority.

2. A higher-level administrator can set whether to allow a lower-level administrator to view the defined policy or allow an administrator of the same level to view and edit the defined policy.

3. By default, a lower-level administrator cannot modify the Internet Access Policy defined by a higher-level administrator.

4. If administrator A selects **Give view privilege to administrator in lower-level role** for the defined Internet Access Policy, administrator B of the same level can edit this policy only if they share the same jurisdiction scope of B covers that of A.

5. If administrator A selects **Give view privilege to administrator in lower-level role** for the defined Internet Access Policy, higher-level administrator C can edit this policy only if they share the same jurisdiction scope or C covers that of A.

6. An Internet Access Policy's priority depends on the administrator level that creates it. A policy created by a higher-level administrator has a higher priority. The priorities of policies created by the same level of administrators can be adjusted.

7. After an administrator is deleted, the user groups and users created by this administrator are unaffected. Therefore, the priority of the Internet Access Policy created by this administrator remains unchanged, and the created administrator becomes the admin.

8. By default, the **Administrator** role exists with the highest permission and cannot be deleted. Therefore, only an administrator of the **Administrator** role can create roles and administrator accounts.

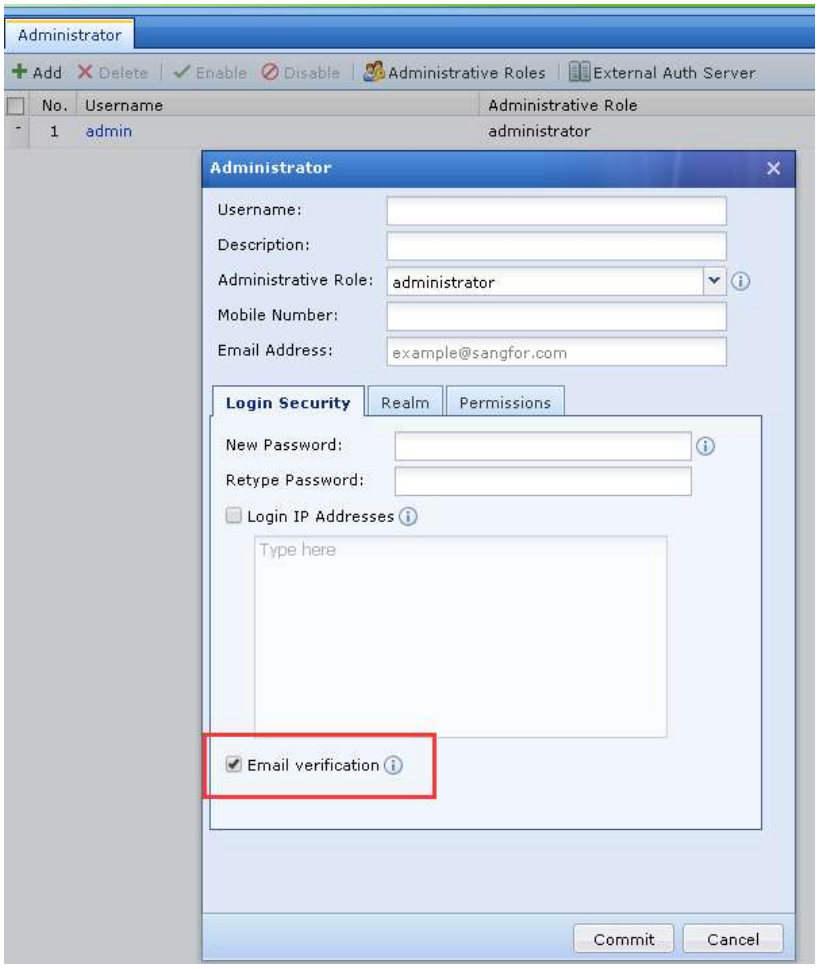
9. To delete an administrator role, delete the administrator of this role and the Internet Access Policy created by this role, and then delete this administrator role.

3.11.5.2.1 Email Verification

The dual-factor verification is added to the admin account. By default, this function is disabled. To use this function, select **Email verification** in the corresponding admin account.

NOTE

Enabling this function for the admin account is not recommended.



Configure **Email Notification**: