Standard Development Model Specification

mSOLUTION Consultants Limited

Date : 2014/02/18
Prepared by : Man NG
Version : SDM_v0.2.0 - AccessControl
Remarks :

Revision History

Revision	Changes	Date
1	Initial Draft (API Specification)	2014/02/06
2	Add function: addUser, verifyPermission, changePassword, enableUser, disableUser	2014/02/18
3	Add function: addPermission, deletePermission, editPermission, showAllPermission, showAllPermissionOfUser, permissionGrantToUser, permissionDeniedToUser, permissionRemoveFromUser	2014/02/25
4	Add function: addGroup, deleteGroup, editGroup, showAllGgroup, showAllGroupUser, addGoupUser, removeGroupUser, showAllPermissionOfGroup, permissionGrantToGroup, permissionRemoveFromGroup	2014/02/28
5	Add function: showUserDetail, showAllUserList, showPermisisonOfGroup	2014/03/15

API Specification

SDMAccessControl API

Description : User access control. Such as login process, verify user login status, login timeout control, protect content access control by php web.

System Requirement:
PHP 5.3.0 or upper with PDO support

Installation:
Server:
MySQL script : run Install/AccessControl/defaultDB.sql

Config:
SDM/Modules/AccessControl/config.php
SDMAccessControlTimeOut
- Set SDM Access Control time out time in second (e.g: 60 = 1 min)

API Location:
http://www.yourhost.com/SDM/Modules/AccessControl/api.php

Function (Controller API):

Login Submit Submit the Login action. User need to pass a username, password			
Input	POST	action	"login"
	POST	userid	String (login user username)
	POST	password	String (login user password)
Output	{"response":{ "loginStatus" : "LOGINSUCCESS" , "token" : "202cb962ac59075b964b07152d" }}		Login Success with correct username and password. A login token will reply
	{"response":{"loginStatus":"LOGINFAIL"}}		Login Fail with wrong username or password

Logout Submit Submit the Logout action.			
Input	POST	action	"logout"
	POST	token	String (Login Token)
Output	{"response": {"loginStatus":"LOGOUTSUCCESS"}}		Logout Success. Login session have removed
	{"response":{"loginStatus":"LOGOUTFAIL"}}		Logout fail. Login session still keep

Verify Login Check the user is either in login status or not. If user login session is over time limit. A timeout message will fire and clear all session with user. Login time limit can edit in the config file. Each time call this function. The session time will renew and extend if pass parameter extendSession with "yes".			
Input	POST	action	"verifyLogin"
	POST	token	String (Login Token)
	POST	extendSession (Optional)	"yes" - Extend session time
Output	{"response":{"loginStatus":"NOTLOGIN"}}		User is not in Login status
	{"response":{"loginStatus":"ISLOGIN"}}		User is in Login status
	{"response":{"loginStatus":"TIMEOUT"}}		User Login session is over time limit.

Add User Add a new user to access control system. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["addUser"] = "SYS_SDM_USER_ADD"		
Input	POST	action	"addUser"
	POST	token (Optional)	String (Login Token)
	POST	userid	String (New user username)
	POST	password	String (New user password)
Output	{"response":{ "actionResult" : "SUCCESS"}}		Add new user success
	{ "response" :{ "actionResult" : "FAIL", "reason": "DUPLICATE_USERID" } }		Add new user fail Reason: *DUPLICATE_USERID* The userid have been used by other user *INVALID_USERID* The userid is not valid *INVALID_PASSWORD* The password is empty *ACCESS_DENIED*: User do not have permission to add new user *SESSION_TIMEOUT*: User session timeout *INVALID_SESSION*: The input token is invalid *DB_FAIL*: Connect database fail

Verify Permission
Check user permission by login token. You can input one or more permission key to verify. In case you verify more than one permission. If user don't have any one permission of them. The verifyResult will be NOTPASS. If the login session is timeout. The verifyResult will be NOTPASS

Input	POST	action	"verifyPermission"
	POST	token	String (Login Token)
	POST	permissionKey	String (If input more than one permission, separately by "|") e.g: Key1|Key2|Key3

Output	{
	"response": {
	"actionResult": "SUCCESS",
	"verifyDetail": {
	"permission": [
	{ "permissionKey": "SDM_USER_ADD",
	"verify": "PASS" },
	{ "permissionKey": "SDM_GROUP_ADD",
	"verify": "NOTPASS" }
	]
	}
	}
	}
			actionResult:
			SUCCESS - User have all the input permission
			FAIL - User don't have all the input permission
			
			verifyDetail:
			permissionKey - Specific permission key
			verify - PASS have permission / NOTPASS don't have permission

Change Password
Change the password of user.

Input	POST	action	"changePassword"
	POST	token	String (Login Token)
	POST	oldPassword	String (Old password)
	POST	newPassword	String (New password)
Output	{"response":{ "actionResult" : "SUCCESS"}}		Change password success

	{
	"response" : {
	"actionResult" : "FAIL",
	"reason":"INVALID_OLDPASSWORD"
	}
	}
			Change password fail
			
			reason:
			INVALID_OLDPASSWORD:
			The old password input not correct
			
			INVALID_NEWPASSWORD:
			The new password is empty string
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Enable / Disable User Allow user to enable or disable a user account. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["enabledisableUser"] = "SYS_SDM_USER_ENABLE_DISABLE"		
Input	POST	action	"enableUser" / "disableUser"
	POST	token	String (Login Token)
	POST	userid	String (username of the user to been enable or disable)
Output	{"response":{ "actionResult" : "SUCCESS"}}		Enable user account success
	{ "response" : { "actionResult" : "FAIL", "reason":"INVALID_USERID" } }		Enable user account fail Reason: *INVALID_USERID* No such user account with input username *ACCESS_DENIED*: User do not have permission to do the action *SESSION_TIMEOUT*: User session timeout *INVALID_SESSION*: The input token is invalid *DB_FAIL*: Connect database fail

Add Permission Add a new permission to system. Permission Key is unique. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["addPermission"] = "SYS_SDM_PERMISSION_ADD"		
Input	POST	action	"addPermission"
	POST	token (Optional)	String (Login Token)
	POST	permissionKey	String (Permission Key)
	POST	permissionDesc	String (Permission Description)
Output	{"response":{ "actionResult" : "SUCCESS"}}		Add new user success

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "DUPLICATE_PERMISSIONKEY"
	}
	}
			Add new permission fail
			
			Reason:
			INVALID_PERMISSIONKEY
			Permission key cannot only be in letters or number or _ and not start with "SYS_SDM"
			
			DUPLICATE_PERMISSIONKEY
			The permission key already exists
			
			ACCESS_DENIED:
			User do not have permission to add new permission
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Delete Permission Delete permission from system. User permission will be update. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["deletePermission"] = "SYS_SDM_PERMISSION_DEL"		
Input	POST	action	"deletePermission"
	POST	token (Optional)	String (Login Token)
	POST	permissionKey	String (Permission Key)
Output	{"response":{ "actionResult" : "SUCCESS"}}		Delete permission success
	{ "response" :{ "actionResult" : "FAIL", "reason": "INVALID_PERMISSIONKEY" } }		Delete permission fail Reason: *INVALID_PERMISSIONKEY* No such permission key *ACCESS_DENIED*: User do not have permission to add new permission *SESSION_TIMEOUT*: User session timeout *INVALID_SESSION*: The input token is invalid *DB_FAIL*: Connect database fail

Edit Permission Description Edit permission key description. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["editPermission"] = "SYS_SDM_PERMISSION_EDIT"		
Input	POST	action	"editPermission"
	POST	token (Optional)	String (Login Token)
	POST	permissionKey	String (Permission Key)
	POST	permissionDesc	String (Permission Description)
Output	{"response":{ "actionResult" : "SUCCESS"}}		Edit permission key description success

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "INVALID_PERMISSIONKEY"
	}
	}
			Edit permission key description fail
			
			Reason:
			INVALID_PERMISSIONKEY
			No such permission key
			
			ACCESS_DENIED:
			User do not have permission to add new permission
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Show all permission key Show all permission key in the system			
Input	POST	action	showAllPermission

Output	{
	"response": {
	"actionResult": "SUCCESS",
	"permissionList": {
	"system": {
	"permission": [
	{ "permissionKey": "SDM_USER_ADD",
	"permissionDesc": "System pre-define permission to add use" },
	{ "permissionKey": "SDM_USER_DEL",
	"permissionDesc": "System pre-define permission to delete use" }
	]
	},
	"user": {
	"permission": [
	{ "permissionKey": "PRINT_INVOICE",
	"permissionDesc": "Print invoice" },
	{ "permissionKey": "EDIT_INVOICE",
	"permissionDesc": "Edit invoice"}
	]
	}
	}
	}
	}
			Show all permission success and list all the permission with type
			system - SDMAccessControl system pre-define permission.
			user - User define permission.

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "DB_FAIL"
	}
	}
			Show all permission fail
			
			Reason:
			DB_FAIL:
			Connect database fail

Show all permission key of a user
Show all permission key of a select user. User can config this function protect by permission or not. If protect by permission, need to pass a login token.

Config	$SDMAccessControlAPIRequestPermission["showAllPermissionOfUser"] = "SYS_SDM_PERMISSION_VIEWOTHER"		
Input	POST	action	showAllPermissionOfUser
	POST	token (Optional)	String (Login Token)
	POST	userid	String (username of the user to been view)

Output	{
	"response": {
	"actionResult": "SUCCESS",
	"count" : "4"
	"permissionList": {
	"system": {
	"permission": [
	{ "permissionKey": "SDM_USER_ADD",
	"permissionDesc": "System pre-define permission to add use" },
	{ "permissionKey": "SDM_USER_DEL",
	"permissionDesc": "System pre-define permission to delete use" }
	]
	},
	"user": {
	"permission": [
	{ "permissionKey": "PRINT_INVOICE",
	"permissionDesc": "Print invoice" },
	{ "permissionKey": "EDIT_INVOICE",
	"permissionDesc": "Edit invoice"}
	]
	}
	}
	}
	}
		Show all permission success and list all the permission with type
		system - SDMAccessControl system pre-define permission.
		user - User define permission.
		If user do not have any permission. The count element will return 0. "permissionList" element will not appear.

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "INVALID_USERID"
	}
	}
		Show all permission fail
		
		Reason:
		INVALID_USERID
		No such userid record
		
		ACCESS_DENIED:
		User do not have permission to add view other's permission
		
		SESSION_TIMEOUT:
		User session timeout
		
		INVALID_SESSION:
		The input token is invalid
		
		DB_FAIL:
		Connect database fail

Grant permission to a user grant permission to a user. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["permissionGrantToUser"] = "SYS_SDM_PERMISSION_ASSIGN"		
Input	POST	action	permissionGrantToUser
	POST	token (Optional)	String (Login Token)
	POST	userid	String (userid of the user)
	POST	permissionKey	String (Permission Key)
Output	{ "response" : {"actionResult" : "SUCCESS"}}		Grant permission to user success

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "INVALID_USERID"
	}
	}
			Grant permission to user fail
			
			Reason:
			INVALID_USERID
			No such userid record
			
			INVALID_PERMISSION
			No such permission key
			
			ACCESS_DENIED:
			User do not have permission to add grant permission
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Denied permission to a user Denied permission to a user. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["permissionDeniedToUser"] = "SYS_SDM_PERMISSION_ASSIGN"		
Input	POST	action	permissionDeniedToUser
	POST	token (Optional)	String (Login Token)
	POST	userid	String (userid of the user)
	POST	permissionKey	String (Permission Key)
Output	{ "response" : {"actionResult" : "SUCCESS"}}		Denied permission to user success
	{ "response" :{ "actionResult" : "FAIL", "reason": "INVALID_USERID" } }		Denied permission to user fail Reason: *INVALID_USERID* No such userid record *INVALID_PERMISSION* No such permission key *ACCESS_DENIED*: User do not have permission to add denied permission *SESSION_TIMEOUT*: User session timeout *INVALID_SESSION*: The input token is invalid *DB_FAIL*: Connect database fail

Remove permission from a user Remove permission from a user. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["permissionRemoveFromUser "] = "SYS_SDM_PERMISSION_ASSIGN"		
Input	POST	action	permissionRemoveFromUser
	POST	token (Optional)	String (Login Token)
	POST	userid	String (userid of the user)
	POST	permissionKey	String (Permission Key)
Output	{ "response" : {"actionResult" : "SUCCESS"}}		Remove permission from user success
	{ "response" :{ "actionResult" : "FAIL", "reason": "INVALID_USERID" } }		Remove permission from user fail Reason: *INVALID_USERID* No such userid record *INVALID_PERMISSION* No such permission key *ACCESS_DENIED*: User do not have permission to add remove permission from user *SESSION_TIMEOUT*: User session timeout *INVALID_SESSION*: The input token is invalid *DB_FAIL*: Connect database fail

Add User Group Add a new user group. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["addGroup "] = "SYS_SDM_GROUP_ADD"		
Input	POST	action	addGroup
	POST	token (Optional)	String (Login Token)
	POST	groupName	String (New Group Name)
	POST	groupDesc	String (New Group Description)
Output	{"response": { "actionResult" : "SUCCESS", "groupID" : "1" }}		Add new group success New group ID return with groupID

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "ACCESS_DENIED"
	}
	}
			Add new group fail
			
			Reason:
			DUPLICATE_GROUPNAME
			The group name is duplicate with other exists group
			
			ACCESS_DENIED:
			User do not have permission to add remove permission from user
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Update User Group Information Update user group information. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["editGroup "] = "SYS_SDM_GROUP_EDIT"		
Input	POST	action	editGroup
	POST	token (Optional)	String (Login Token)
	POST	groupID	String (Group ID to update)
	POST	groupName	String (Update Group Name)
	POST	groupDesc	String (Update Group Description)
Output	{ "response" : {"actionResult" : "SUCCESS"}}		Update group information success

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "INVALID_GROUPID"
	}
	}
			Update group information fail
			
			Reason:
			DUPLICATE_GROUPNAME
			The group name is duplicate with other exists group
			
			INVALID_GROUPID
			The input group ID is not exist
			
			ACCESS_DENIED:
			User do not have permission to add remove permission from user
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Delete User Group Delete the user group. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["deleteGroup "] = "SYS_SDM_GROUP_DEL"		
Input	POST	action	deleteGroup
	POST	token (Optional)	String (Login Token)
	POST	groupID	String (Group ID to update)
Output	{ "response" : {"actionResult" : "SUCCESS"}}		Delete user group success

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "INVALID_GROUPID"
	}
	}
			Delete user group fail
			
			Reason:
			INVALID_GROUPID
			The input group ID is not exist
			
			ACCESS_DENIED:
			User do not have permission to add remove permission from user
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Show all User Group in system Show all the user group in system.			
Input	POST	action	showAllGroup

Output	{
	"response" : {
	"actionResult" : "SUCCESS",
	"count" : "2",
	"groupList" : {
	"group": [
	{ "groupID" : "5",
	"groupName" : "ManTeam" ,
	"groupDesc" : "Man Team" },
	{ "groupID" : "7",
	"groupName" : "PatrickTeam",
	"groupDesc" : "Patrick Team" }
	]
	}
	}
	}
			Get the group list success with group list detail. If group count is zero, groupList element will not appear.

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "DB_FAIL"
	}
	}
			Get user group list fail
			
			Reason:
			DB_FAIL:
			Connect database fail

Show all User in the Group Show all user in the group.			
Config	$SDMAccessControlAPIRequestPermission["showAllGroupUser "] = "SYS_SDM_GROUP_SHOWALLUSER"		
Input	POST	action	showAllGroupUser
	POST	token (Optional)	String (Login Token)
	POST	groupID	String (Group ID)
Output	{"response":{ "actionResult":"SUCCESS", "count":"2", "groupInfo": { "groupID" : "9", "groupName" : "Test Group" , "groupDesc" : "GroupDesc"}, "groupUserList" : { "groupUser" : [{"userID" : "kelson","status":"A" }, {"userID":"man","status":"A"}]} }}		Get the user list of group success with group Information and group user list. If group user count is zero, groupUserList element will not appear.

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "DB_FAIL"
	}
	}
			Get user group list fail
			
			Reason:
			DB_FAIL:
			Connect database fail

Add user into the group Add user into the group by userid and groupid.			
Config	$SDMAccessControlAPIRequestPermission["editGroupUser "] = "SYS_SDM_GROUP_EDITUSER"		
Input	POST	action	addGroupUser
	POST	token (Optional)	String (Login Token)
	POST	userid	String (Userid)
	POST	groupID	String (Group ID)
Output	{"response":{"actionResult":"SUCCESS"}}		Add user into group success

	<pre>{
	  "response" :{
	  "actionResult" : "FAIL",
	  "reason": "INVALID_GROUPID"
	  }
	}</pre>
			Get user group list fail
			
			Reason:
			INVALID_GROUPID
			The input group ID is not exist
			
			INVALID_USERID
			The input useid is not exists
			
			EXISTING_GROUP_USER
			The user already exists in the group
			
			ACCESS_DENIED:
			User do not have permission to add remove permission from user
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Remove user from group Remove user from group by userid and groupid.			
Config	$SDMAccessControlAPIRequestPermission["editGroupUser "] = "SYS_SDM_GROUP_EDITUSER"		
Input	POST	action	removeGroupUser
	POST	token (Optional)	String (Login Token)
	POST	userid	String (Userid)
	POST	groupID	String (Group ID)
Output	{"response":{"actionResult":"SUCCESS"}}		Add user into group success
	{ "response" :{ "actionResult" : "FAIL", "reason": "INVALID_GROUPID" } }		Get user group list fail Reason: *INVALID_GROUPID* The input group ID is not exist *INVALID_USERID* The input useid is not exists *NOTEXISTING_GROUP_USER* The user not below to such group *ACCESS_DENIED*: User do not have permission to add remove permission from user *SESSION_TIMEOUT*: User session timeout *INVALID_SESSION*: The input token is invalid *DB_FAIL*: Connect database fail

Grant permission to group Grant permission to group. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["assignPermissionToGroup"] = "SYS_SDM_PERMISSION_ASSIGN"		
Input	POST	action	permissionGrantToGroup
	POST	token (Optional)	String (Login Token)
	POST	groupID	String (group ID)
	POST	$permissionKey_i$	String (Permission Key)
Output	{ "response" : {"actionResult" : "SUCCESS"}}		Grant permission to group success

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "INVALID_USERNAME"
	}
	}
			Grant permission to group fail
			
			Reason:
			INVALID_GROUPID
			No such username record
			
			INVALID_PERMISSION
			No such permission key
			
			ACCESS_DENIED:
			User do not have permission to add grant permission
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Remove permission from group Remove permission from group. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["assignPermissionToGroup "] = "SYS_SDM_PERMISSION_ASSIGN"		
Input	POST	action	permissionRemoveFromGroup
	POST	token (Optional)	String (Login Token)
	POST	groupID	String (Group ID)
	POST	permissionKey	String (Permission Key)
Output	{ "response" : {"actionResult" : "SUCCESS"}}		Remove permission from group success

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "INVALID_USERNAME"
	}
	}
			Remove permission from group fail
			
			Reason:
			INVALID_GROUPID
			No such username record
			
			INVALID_PERMISSION
			No such permission key
			
			ACCESS_DENIED:
			User do not have permission to add remove permission from user
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Show user detail
Show user detail of selection user by userid. Return the user status, last login time, last access time and last update time. Also will display all the group the user below to. User can config this function protect by permission or not. If protect by permission, need to pass a login token.

Config	$SDMAccessControlAPIRequestPermission["showUserDetail "] = "SYS_SDM_USER_SHOWDETAIL"		
Input	POST	action	showUserDetail
	POST	token (Optional)	String (Login Token)
	POST	userid	String (User ID)

Output	{"response":{
	"actionResult" : "SUCCESS",
	"userInfo":{
	"userid" : "user1",
	"userStatus" : "A",
	"lastLoginDateTime" : "2014-03-21 12:40:24",
	"lastAccessDateTime" : "2014-03-21 12:40:24",
	"lastUpateDateTime" : "2014-01-29 10:32:56"
	},
	"groupInfo" : [
	{ "groupID" : "1",
	"groupName" : "Group1" }
	]
	}}
			Get the user detail success with user info. If user is below to group. Group Info will show all the group that user below to. If user do not below to any group, groupInfo element will not appear.

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "DB_FAIL"
	}
	}
			Get user detail fail
			
			Reason:
			INVALID_USERID
			The input useid is not exists
			
			ACCESS_DENIED:
			User do not have permission to add grant permission
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Show all User in the system Get all the userid and user status in system. User can config this function protect by permission or not. If protect by permission, need to pass a login token.			
Config	$SDMAccessControlAPIRequestPermission["showAllUser "] = "SYS_SDM_USER_SHOWALL"		
Input	POST	action	showAllUser
	POST	token (Optional)	String (Login Token)

Output	{ "response" : {
	"actionResult" : "SUCCESS",
	"userList" : {
	"user":[
	{"userID":"user1","UserStatus":"A"},
	{"userID":"user2","UserStatus":"A"},
	{"userID":"user3","UserStatus":"P"},
	{"userID":"SystemAdmin","UserStatus":"A"}
	]
	}
	}}
			Get user list success

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "DB_FAIL"
	}
	}
			Get user group list fail
			
			Reason:
			ACCESS_DENIED:
			User do not have permission to add grant permission
			
			SESSION_TIMEOUT:
			User session timeout
			
			INVALID_SESSION:
			The input token is invalid
			
			DB_FAIL:
			Connect database fail

Show permission of the Group
Show the permission of group. User can config this function protect by permission or not. If protect by permission, need to pass a login token.

Config	$SDMAccessControlAPIRequestPermission["showAllPermisisonOfGroup "] = "SYS_SDM_PERMISSION_VIEWOTHER"		
Input	POST	action	showAllPermissionOfGroup
	POST	token (Optional)	String (Login Token)
	POST	groupID	String (Group ID)

Output	{"response":{
	"actionResult" : "SUCCESS",
	"count" : "3",
	"permissionList" : {
	"system" : {
	"permission":[
	{"permissionKey" : "SYS_SDM_USER_ADD"},
	{"permissionKey" : "SYS_SDM_USER_DEL"}
	]},
	"user": {
	"permission":[
	{"permissionKey":"PRINT_REPORT"}
	]}
	}
	}}
			Get permission of group success.
			
			If the group do not have any permission. The count element will return 0. "permissionList" element will not appear.

	{
	"response" :{
	"actionResult" : "FAIL",
	"reason": "DB_FAIL"
	}
	}
			Get permission of group fail
			
			Reason:
			DB_FAIL:
			Connect database fail

Example:

PHP

```php
<?php
	$protocol = strpos(strtolower($_SERVER['SERVER_PROTOCOL']),'https')  === FALSE ? 'http' : 'https';
	$host     = $_SERVER['HTTP_HOST'];
	$script   = $_SERVER['SCRIPT_NAME'];
	$params   = $_SERVER['QUERY_STRING'];
	$apiURL = $protocol . '://' . $host ."/~manho/SDMProject" . "/SDM/Modules/AccessControl/api.php" ;

	$post = array(
		"action"=>"login",
		"userid"=>"SystemAdmin",
		"password"=>"Admin",
	);

	$ch = curl_init();
	$options = array(
		CURLOPT_URL=>$apiURL,
		CURLOPT_RETURNTRANSFER=>true,
		CURLOPT_POST=>true,
		CURLOPT_POSTFIELDS=>http_build_query($post),
	);
	curl_setopt_array($ch, $options);

	$apiResult = curl_exec($ch);
	curl_close($ch);

	$json = json_decode($apiResult,true);

	if($json["response"]["loginStatus"] == "LOGINSUCEESS"){
		echo "Your Login Token: ". $json["response"]["token"];
	} else {
		echo "Login Fail!";
	}

?>
```