RBAC-New Feature Introduction

F300Q Series
P300Q Series
P500Q Series
S300Q Series

Version 1.1
July 2011

Trademarks

All products and trade names used in this manual are trademarks or registered trademarks of their respective companies.

Qsan Technology, Inc.

2F., No.23, Lane 583, Ruiguang Rd.
Neihu Dist., Taipei 114
Taiwan, R.O.C.

Tel: +886-2-7720-2118
Fax: +886-2-7720-0295

Email: sales@Qsan.com.tw
Website: www.QsanTechnology.com

Introduction

RBAC (Role-Based Access Control) is an approach to restricting system access to authorized users. Qsan storage systems add this new feature. The account administrator can create a new account with assigning a role to grant the access right.

This feature is also integrated with Microsoft Active Directory service. It allows users to log on the Qsan storage systems with an account which is created in Microsoft Active Directory. It helps administrators to centralize the access control of the Qsan storage systems without maintaining separate account lists.

Environment

Items	Description
Host OS	Microsoft Windows Server 2003 Enterprise Edition with Active Directory service installed.
AD Domain Name	qsan.com.tw
AD Server IP address	192.168.0.1
Storage System	P300Q-D316
Firmware Version	2.1.0 or later

Role Names and Permissions

There are several roles with different permissions. This table shows the roles, system default users, the roles which are mapped to the AD group name and their permissions.

Role Name	Default User	AD Group Name	Permissions
admin	admin	Administrators	• Full permissions.
user	user	Users	• Browse the configurations only. • No permission to change anything.
net	N/A	Network Configuration Operators	• Have permission to change **Network setting**, **Mail setting**, **Notification setting** in **System configurations**. • Have permission to change **NIC** in **iSCSI configurations**. (only for iSCSI models.) • No permission to change **Volume configurations** settings.
data	N/A	Server Operators	• Have permission to operate in **Volume configurations**. • No permission to change **System configurations** settings.

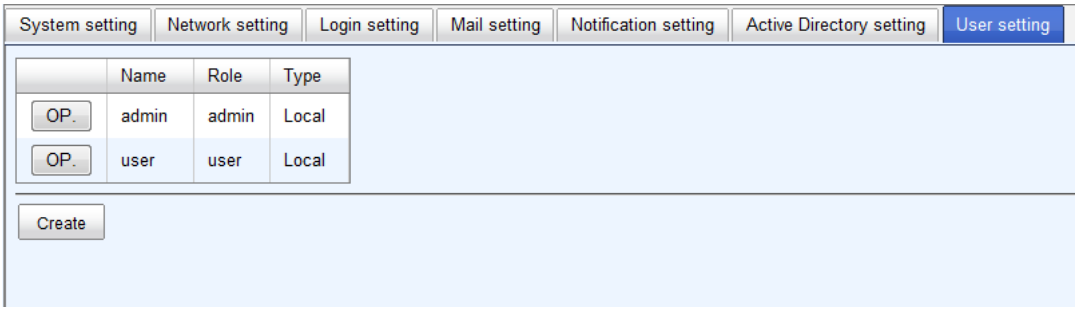
account	N/A	Account Operators	• Have permission to create, modify and delete the accounts, and their permissions. • No permission to change admin group.

Configuration

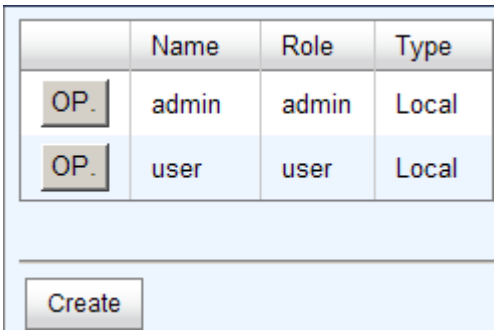
The accounts can be created in local or refer to Microsoft Active Directory service.

Local Account

A new tab of **User setting** is added in the web UI. The username which belongs to the role **admin** or **account** has the permission to create a new account, modify the password or delete the account.



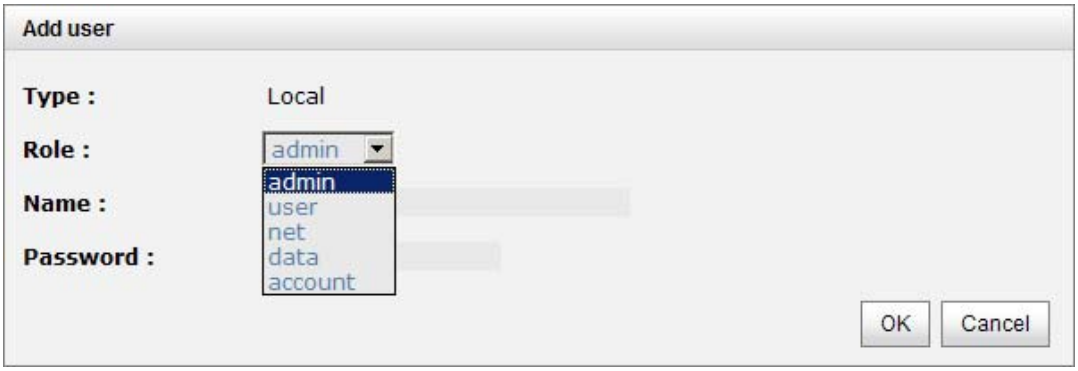
There are two default users in the system: **admin** and **user**. The username **admin** belongs to the role **admin** which has full permissions and cannot be deleted. The other username **user** belongs to the role **user** which has read-only permissions.



TIPS: The username “admin” cannot be changed the role type and it cannot be deleted.

The options are available on this tab:

- **Create:** Add a new account. When clicking **Create** button, it pop-up a dialog as the following. Choose a role, enter a name and password. And then click **OK**.

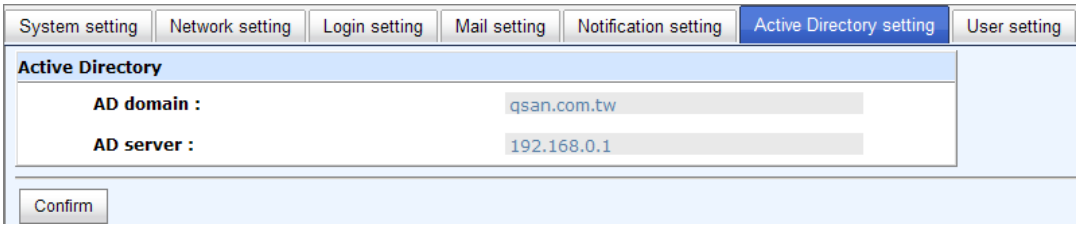


- **OP. -> Change password:** Change the user's password.
- **OP. -> Change user role:** Change the user's role.
- **OP. -> Delete:** Delete the user.

Users can log on the storage system with the new accounts and operate the functions according to the permission of the role.

Refer to Microsoft Active Directory Service

To refer the account created in Microsoft Active Directory service, the AD domain name and IP address of AD server are needed.



The options are available on this tab:

- **AD domain:** Fill in Active Directory domain name.
- **AD server:** Fill in Active Directory server IP address.

When it is done, click **Confirm**.

TIPS: The DNS server with the forward lookup record of the AD server must be configured in the network setting to help the storage communicates with the AD server correctly.

After the above settings are entered, the login authentication supports Windows Active Directory service. First, you should create an account with an AD group in Windows. And then try to use the account to login the storage system. The syntax of the user name in Active Directory is:

- UPN (User Principal Name) (e.g. bob@qsan.com.tw)

The permission of the account depends on what AD group belongs in Windows.

TIPS: When multiple roles are assigned to an account in AD, only one role will take effect. The permission overrides as follows, account operators > users > server operators > network configuration operators > administrators.

TIPS: We recommend not to use the built-in account in AD, such as Administrator, to log on the storage. You should create a new account and assign the role to it properly as instead. As to the policy in the AD, if you log on the storage with “Administrator” account, you may get the privilege of Users.

Applied To

- F300Q / P300Q / P500Q / S300Q Series: FW 2.1.0