

QAuth

Authorizations of Users Responsibility

White Paper

July 2022

ANNOUNCEMENT

Copyright

© Copyright 2022 QSAN Technology, Inc. All rights reserved. No part of this document may be reproduced or transmitted without written permission from QSAN Technology, Inc.

QSAN believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Trademarks

- QSAN, the QSAN logo, QSAN.com, XCubeFAS, XCubeSAN, XCubeNXT, XCubeNAS, XCubeDAS, XEVO, SANOS, and QSM are trademarks or registered trademarks of QSAN Technology, Inc.
- Microsoft, Windows, Windows Server, and Hyper-V are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux is a trademark of Linus Torvalds in the United States and/or other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Mac and OS X are trademarks of Apple Inc., registered in the U.S. and other countries.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
- VMware, ESXi, and vSphere are registered trademarks or trademarks of VMware, Inc. in the United States and/or other countries.
- Citrix and Xen are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries.
- Other trademarks and trade names used in this document to refer to either the entities claiming the marks and names or their products are the property of their respective owners.

TABLE OF CONTENTS

Announcement.....	i
Notices.....	iv
Preface.....	v
Executive Summary	v
Audience	v
Technical Support	v
Information, Tip, and Caution	vi
1. Overview	1
1.1. QAuth Concept	1
2. Configure QAuth.....	3
3. Conclusion	4
4. Appendix.....	5
4.1. Apply To	5
4.2. Reference.....	5

FIGURES

Figure 1-1	Account Permissions for Storage Managers.....	2
------------	---	---

NOTICES

Information contained in this manual has been reviewed for accuracy. But it could include typographical errors or technical inaccuracies. Changes are made to the document periodically. These changes will be incorporated in new editions of the publication. QSAN may make improvements or changes in the products. All features, functionality, and product specifications are subject to change without prior notice or obligation. All statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

PREFACE

Executive Summary

In order to improve management and execution efficiency, enterprises often distinguish several levels of authorization among all employees. XEVO grants appropriate permissions to different users through access control with QAuth functionality.

Audience

This document is applicable for QSAN customers and partners who are interested in learning about QAuth to easily manage accounts. It assumes the reader is familiar with QSAN products and has General IT experience, including knowledge as a system or network administrator. If there is any question, please refer to the user manuals of products, or contact QSAN support for further assistance.

Technical Support

Do you have any questions or need help trouble-shooting a problem? Please contact QSAN Support, we will reply to you as soon as possible.

- Via the Web: https://www.qsan.com/technical_support
- Via Telephone: +886-2-77206355
- (Service hours: 09:30 - 18:00, Monday - Friday, UTC+8)
- Via Skype Chat, Skype ID: qsan.support
- (Service hours: 09:30 - 02:00, Monday - Friday, UTC+8, Summer time: 09:30 - 01:00)
- Via Email: support@qsan.com

Information, Tip, and Caution

This document uses the following symbols to draw attention to important safety and operational information.



INFORMATION

INFORMATION provides useful knowledge, definition, or terminology for reference.



TIP

TIP provides helpful suggestions for performing tasks more effectively.



CAUTION

CAUTION indicates that failure to take a specified action could result in damage to the system.

1. OVERVIEW

In computer systems security, user permission is an approach to restricting system access to authorized users. QAuth is a policy-neutral access-control mechanism defined around users, groups, and their privileges. The components of QAuth, such as user permissions and group permissions, make it simple to perform user assignments.

1.1. QAuth Concept

We predefine four commonly used groups and assign corresponding management storage permissions. Their characteristics are described below.

- **Administrators:** Accounts belonging to Administrators have all read and write permissions on the system. At least one administrator account must be online. The default administrator account name is “admin”. It can be disabled and replaced by another name for security reason.
- **Users:** Accounts belonging to Users have most read-only permissions. It is designed for the observer.
- **System Managers:** Accounts belonging to System Managers have permissions to operate the system, such as system settings, firmware update, system reboot or shutdown ...etc.
- **Storage Managers:** Accounts belonging to Storage Managers have permissions to operate storage configurations, such as creating or deleting pools, taking snapshots ...etc.



TIP

The default administrator account “admin” is easy to guess. It is strongly recommended to create another administrator account instead of the default account.

Account Settings

- Administrators
- Users
- System Managers
- Storage Managers**
- Customize Group1
- Customize Group2

Accounts

Permission

Categories	Hide	Read Only	Read & Write
+ Frame	☐	☐	☒
Dashboard	☐	☐	☒
Storage	☐	☐	☒
Host	☐	☐	☒
Protection	☐	☐	☒
Analysis	☐	☒	☐
+ System	☒	☒	☒
+ Message	☒	☒	☐

Cancel

Apply

Figure 1-1 Account Permissions for Storage Managers

- **Customize Group:** There are also two user-defined custom groups. Administrators can define custom group name and permissions.

2. CONFIGURE QAUTH

The following is a tutorial for configuring QAuth functions. Follow the steps and you can learn them quickly.

For XEVO

- [QAuth Tutorial in XEVO](#)

3. CONCLUSION

QAuth feature combines easy management and information security from unauthorized access. IT managers can grant appropriate permissions to different users through access control with QAuth capabilities.

4. APPENDIX

4.1. Apply To

- XEVO firmware 1.0.1 and later

4.2. Reference

- [XEVO Software Manual](#)