Quantum

Scaler Key Manager (SKM) Release Notes 2.9.1

Original Product/Software Release Date October 2024

Contents

© 2024 Quantum Corporation. All rights reserved. Your right to copy this manual is limited by copyright law. Making copies or adaptations without prior written authorization of Quantum Corporation is prohibited by law and constitutes a punishable violation of the law. ActiveScale, DXi, DXi Accent, FlexSync, FlexTier, iLayer, Lattus, Myriad, Quantum, the Quantum logo, QXS, Scalar, StorNext, SuperLoader, Unified Surveillance Platform, USP, Vision, and Xcellis are either registered trademarks or trademarks of Quantum Corporation and its affiliates in the United States and/or other countries. All other trademarks are the property of their respective owners. Quantum specifications are subject to change.

Purpose of This Release

SKM 2.9.1 Release

The SKM 2.9.1 (291Q.GC00200) release supports the following:

- VM instances (Hyper-V, VMWare, and KVM).
- Appliance servers (M6, M6 version 2, and SR250). Please note that appliance server upgrades require service support. Contact Quantum for additional information.

This release provides the following enhancements and updates:

- Security updates (Ubuntu 22.04).
- All critical and high Nessus scan issues identified in the previous 290Q release have been corrected.
- Additional fixes and enhacncements (see Fixed Issues on page 5).

Prior SKM Releases

This section provides prior SKM releases:

SKM 2.9 Release

The SKM 2.9 (290Q.GC00600) release provided:

- Security updates (Ubuntu 22.04).
- All critical and high Nessus scan issues identified on or before December 31, 2023 have been corrected.

SKM 2.8.1 Release

The SKM 2.8.1 (281Q.GC00600) release provided:

- Corrected all critical scan issues identified by Nessus for the 280Q release.

SKM 2.8 Release

SKM 2.8 provided:

- Security updates (Ubuntu 18.04).
- Default password updates.
- TraceRoute support added.
- vmWare support added.

SKM 2.7 Release

SKM 2.7 provided:

- Support for the SR250 hardware appliance
- Security updates

SKM 2.6 Release

SKM 2.6 provided:

- Updates the operating system Ubuntu 16.04.
- Provided TLS 1.2 support.
- Upgraded SKM servers (VM and appliance) will default to TLS 1.0.
- New installations of SKM servers (VM or appliance) will default to TLS 1.2.
- Corrects critical and high identified security issues.

SKM 2.5.2 Release

- SKM 2.5.2 provided support for VMWare ESXi 5.x and 6.x only.

SKM 2.5.1 Release

- SKM 2.5.1 continues to support the SKM appliance and VMWare ESXi 4.x.

These notes also provide library, tape drive, and firmware compatibility information. Visit https://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SKM/Index.aspx for additional information about Scalar Key Manager.

Obtaining the Latest Firmware Release

To obtain SKM 2.9.1 firmware, you must contact Quantum Service and Support:

https://www.quantum.com/ServiceandSupport/Index.aspx

Firmware Notes

Note: To upgrade to firmware release 291Q.GC00200, the VM must be at firmware release 260Q.GC00600.

These release notes list information should be aware of as you set up, configure, and use SKM.

- You may upgrade your VM instance for 2.6, 2.7, 2.8, 2.8.1, or 2.9 using the new procedure outlined in the SKM 2.9.1 User's Guide. There is no upgrade script associated with this release.
- Appliance server upgrades (M6, M6 version 2, and SR250) require Quantum service support. Contact Quantum for additional information.
- SKM and Quantum Encryption Key Manager (Q-EKM) are not supported on the same library.
- Password — If you change the password on the SKM server (the default password is "password"), it is extremely important that you remember the new password. The password can be different for each SKM server, so be sure to remember both. If you forget your password, you will lose login access to the SKM server, including backup and restore capability. Quantum will NOT be able to reset or restore the password.
- Date settings on SKM servers and library — The date on the SKM servers and the library must be set to the current date. Incorrect date settings may interfere with the TLS certificates and cause the library to stop communicating with the SKM servers.
- Backing up the keystores — It is extremely important that you back up both SKM servers (best practice) every time you generate new data encryption keys and before you use these new keys to encrypt data. You should also back up the servers when you import keys. You must back up each server separately because the keystores contain different data. The only way to read encrypted tapes is via the data encryption keys in the keystore. If your SKM servers fail without a backup, you will permanently lose access to all your encrypted data. If an SKM server fails and needs to be replaced, the backup is required to restore operation.
- Generating encryption keys — Generating encryption keys on an SKM server from more than five connected libraries at the same time is not recommended.

Library Compatibility

SKM 2.9.1 supports all Scalar libraries. For firmware pre-requisite versions, reference the tape library documentation and/or firmware release notes.

Note: SKM releases earlier than version 2.1 are no longer supported. Contact your Quantum representative to upgrade to a current release.

Fixed Issues

This release of firmware has the following fixed issues.

Change Request Number	Description
SKM-13	Ubuntu updated to 22.04.
SKM-59	Host ID SSH key now regenerates after initial configuration of IP address on VM hosts.
SKM-60	All critical and high Nessus scan issues identified in the previous 290Q release corrected.
SKM-61	Upgrade path for Appliance servers (M6, M6 version 2, and SR250). Please note that appliance server upgrades require service support. Contact Quantum for additional information
SKM-62	Disk monitoring scrip for SR250 appliance servers fixed.
SKM-65	/tmp file fixes.
SKM-68	SHA1 communication certificates removed from the default OpenSSH. **Note:** Update the utility you use for SSH (such as PuTTY) to the latest version.

Known Issues

This release of firmware has no known issues.

Related Documents

The following publications provide information related to SKM. For the latest versions, visit www.quantum.com/documentation

Document Number	Documentation Center
6-68933	Scaler Key Manager Documentation Center
6-68935	Scaler i500 Documentation Center
6-68921	Scaler i6000 Documentation Center

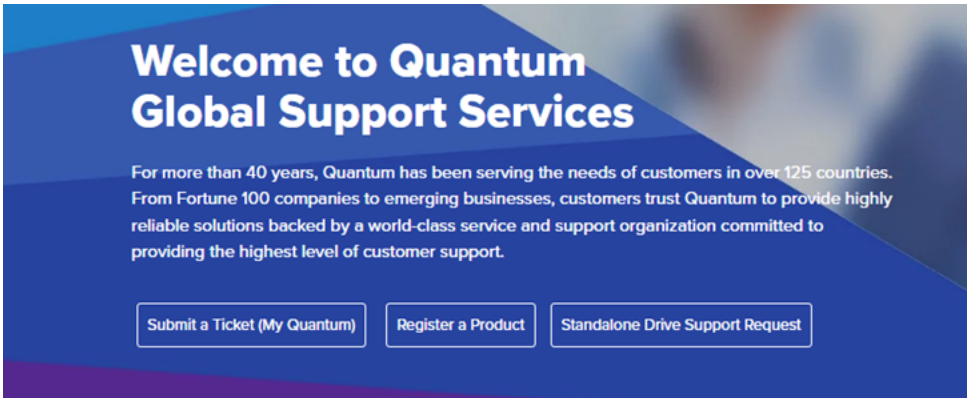
Document Number	Documentation Center
6-68528	Scaler i3 Documentation Center
6-68529	Scalar i6 Documentation Center

Contacting Quantum Support

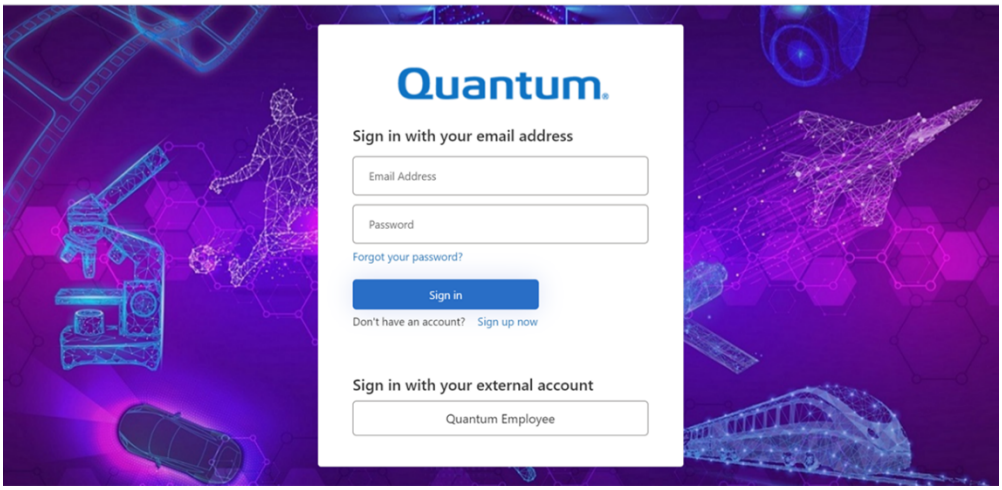
Below is information related to contacting Quantum Support as well as steps to improve your Quantum customer journey.

Submit a Ticket (Service Request)

If you need to submit a ticket or speak to Quantum technical support, go to the Support page at https://www.quantum.com/en/service-support/



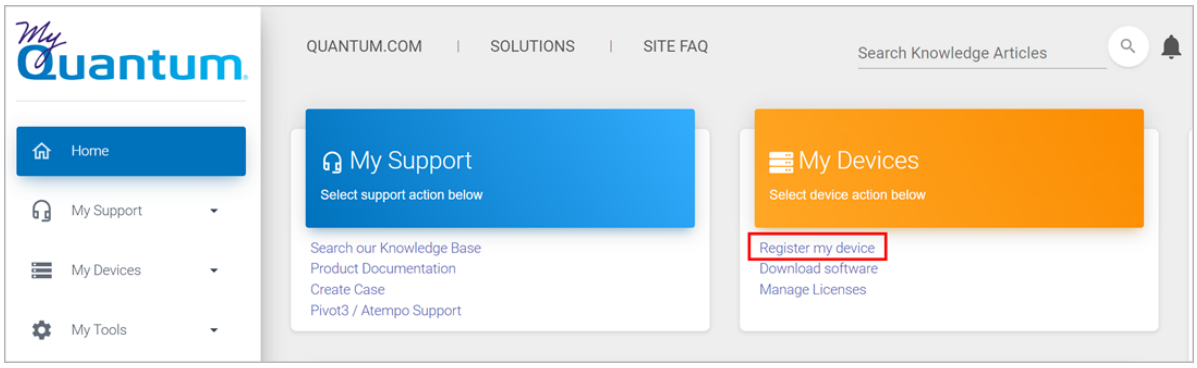
To start the process with Quantum Technical Support, click **Submit a Ticket**. From here, sign in to the MyQuantum Service Delivery Platform or create an account. For more information, refer to the Use MyQuantum Service Delivery Platform on the next page section below.



Use MyQuantum Service Delivery Platform

MyQuantum is a single portal for everything Quantum. You can view assets, open support cases, receive real-time updates, and search the Knowledge Base and documentation, all through a secure, online portal.

1. Create an account and log in to the MyQuantum Service Delivery Platform.
2. Register a product on MyQuantum.



3. Request site access to the Cloud-Based Analytics (CBA) monitoring portal and follow the instructions to set up product(s) to connect to CBA. You can use CBA to monitor Quantum products remotely, from a single dashboard, and Quantum Support can use it to help troubleshoot products more efficiently.

Refer to product documentation for product-specific information related to CBA.

Use Cloud Based Analytics (CBA)

Quantum products are equipped with a Cloud Based Analytics (CBA) agent that can provide log files and snapshots to Quantum CBA servers that are running in the cloud.

CBA enables Quantum systems to collect data regarding system and environment performance. The collected data is bundled and uploaded to the remote CBA server for analysis. You can access Quantum system performance and health results on the CBA dashboard (at https://insight.quantum.com) or through the MyQuantum Service Delivery Platform.

The CBA dashboard displays the analytic results of the uploaded CBA data using flexible charting tools, along with an overall health score of each Quantum system configured for the CBA account.

Escalate a Case

To escalate a case, follow the process documented here: https://www.quantum.com/en/service-support/resources/escalation/

Contact Quantum Sales

https://www.quantum.com/en/company/contact-us/