

Appendix C: LVS[®] 95XX Data Backup

Copyright ©2022
Omron Microscan Systems, Inc.

All rights reserved. The information contained herein is proprietary and is provided solely for the purpose of allowing customers to operate and/or service Omron Microscan-manufactured equipment and is not to be released, reproduced, or used for any other purpose without written permission of Omron Microscan.

Throughout this manual, trademarked names might be used. We state herein that we are using the names to the benefit of the trademark owner, with no intention of infringement.

GS1 Solution Partner



Disclaimer

The information and specifications described in this manual are subject to change without notice.

Latest Manual Version or Technical Support

For the latest version of this manual, or for technical support, see your local Omron website. Your local Omron website can be located by visiting <https://www.ia.omron.com> and selecting your region from the Global Network panel on the right side of the screen.

Security Measures

Anti-Virus Protection

Install the latest commercial-quality antivirus software on the computer connected to the control system and maintain to keep the software up to date.

Security Measures to Prevent Unauthorized Access

Take the following measures to prevent unauthorized access to our products:

- Install physical controls so that only authorized personnel can access control systems and equipment.
- Reduce connections to control systems and equipment via networks to prevent access from untrusted devices.
- Install firewalls to shut down unused communications ports and limit communications hosts and isolate control systems and equipment from the IT network.
- Use a virtual private network (VPN) for remote access to control systems and equipment.
- Adopt multifactor authentication to devices with remote access to control systems and equipment.
- Set strong passwords and change them frequently.
- Scan for viruses to ensure safety of USB drives or other external storage devices before connecting them to control systems and equipment.

Data Input and Output Protection

Validate backups and ranges to cope with unintentional modification of input/output data to control systems and equipment.

- Check the scope of data.
- Check validity of backups and prepare data for restore in case of falsification or abnormalities.
- Safety design, such as emergency shutdown and fail-soft operation in case of data tampering or abnormalities.

Data Recovery

Back up and update data periodically to prepare for data loss.

When using an intranet environment through a global address, connecting to an unauthorized terminal such as a SCADA, HMI or to an unauthorized server may result in network security issues such as spoofing and tampering.

You must take sufficient measures such as restricting access to the terminal, using a terminal equipped with a secure function, and locking the installation area by yourself.

When constructing an intranet, communication failure may occur due to cable disconnection or the influence of unauthorized network equipment. Take adequate measures, such as restricting physical access to network devices, by such means as locking the installation area.

When using a device equipped with the SD Memory Card function, there is a security risk that a third party may acquire, alter, or replace the files and data in the removable media by removing or unmounting the removable media. Please take sufficient measures, such as restricting physical access to the controller or taking appropriate management measures for removable media, by means of locking the installation area, entrance management, etc.

Software

To prevent computer viruses, install antivirus software on the computer where you use this software. Make sure to keep the antivirus software updated.

Keep your computer's OS updated to avoid security risks caused by a vulnerability in the OS.

Always use the latest version of this software to add new features, increase operability, and enhance security. Manage usernames and passwords for this software carefully to protect them from unauthorized uses.

Set up a firewall (e.g., disabling unused communication ports, limiting communication hosts, etc.) on a network for a control system and devices to separate them from other IT networks.

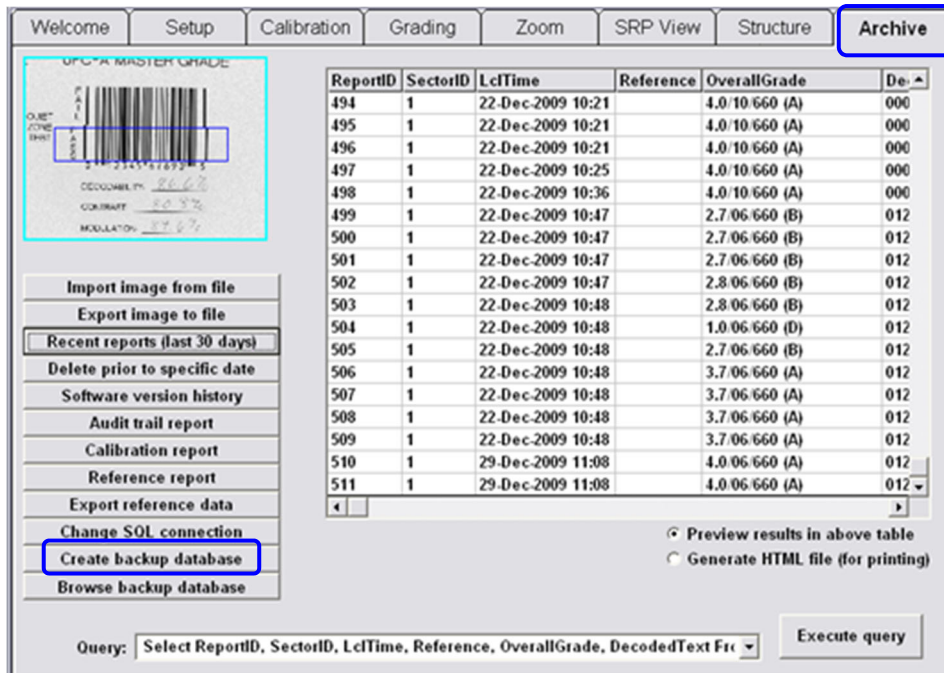
Make sure to connect to the control system inside the firewall.

Use a virtual private network (VPN) for remote access to a control system and devices from this software.

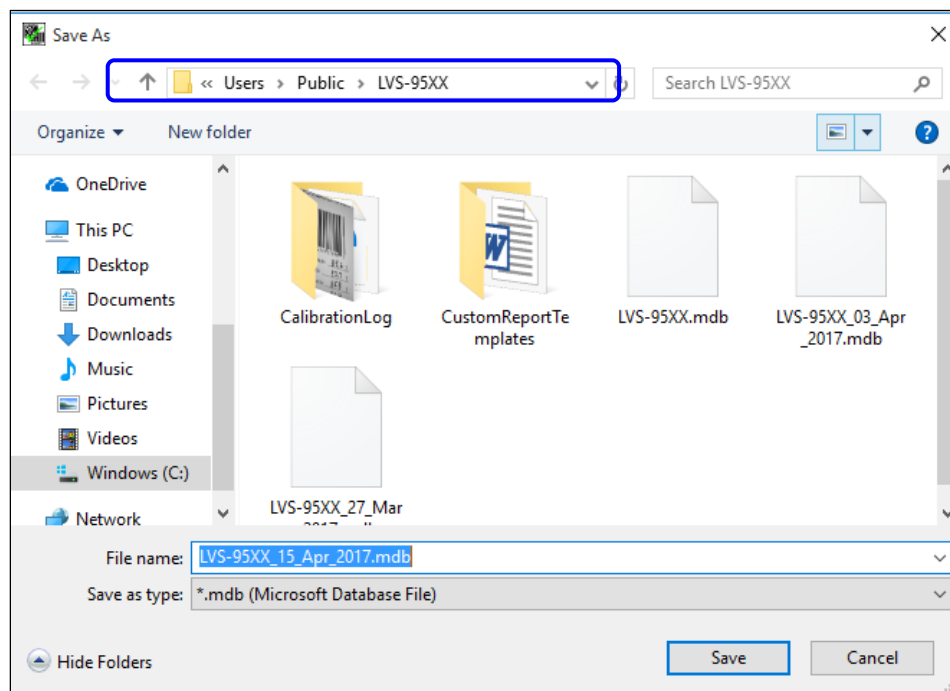
Data Backup

Follow the instructions below to backup data on the LVS-95XX system.

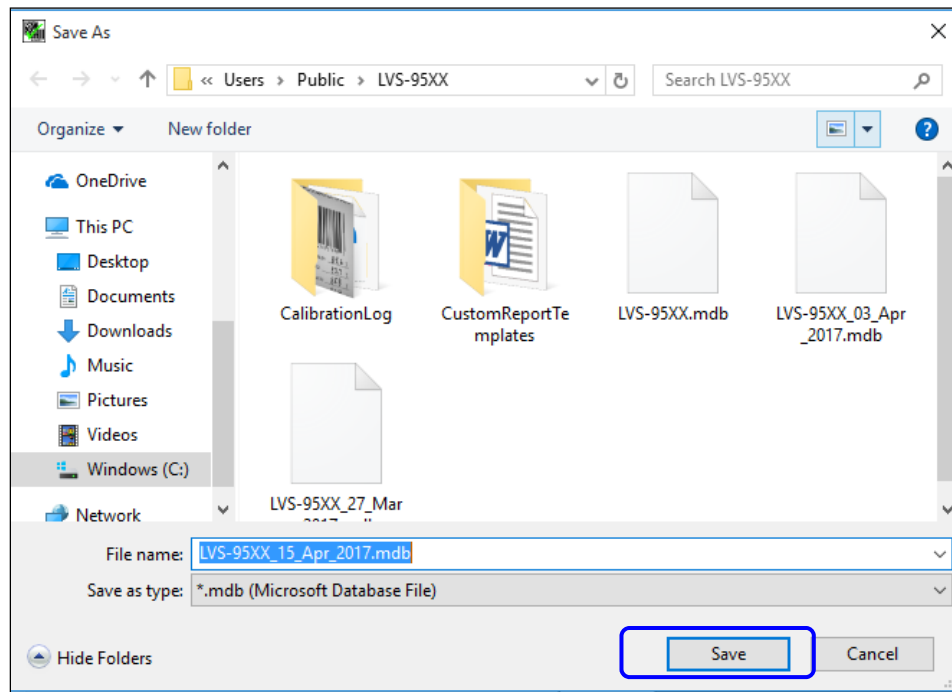
1. Log onto the LVS-95XX system.
2. Click the **Archive** tab, and then click **Create backup database**.



3. Click the **Save in** drop-down list and select the folder or drive to which you want to save.

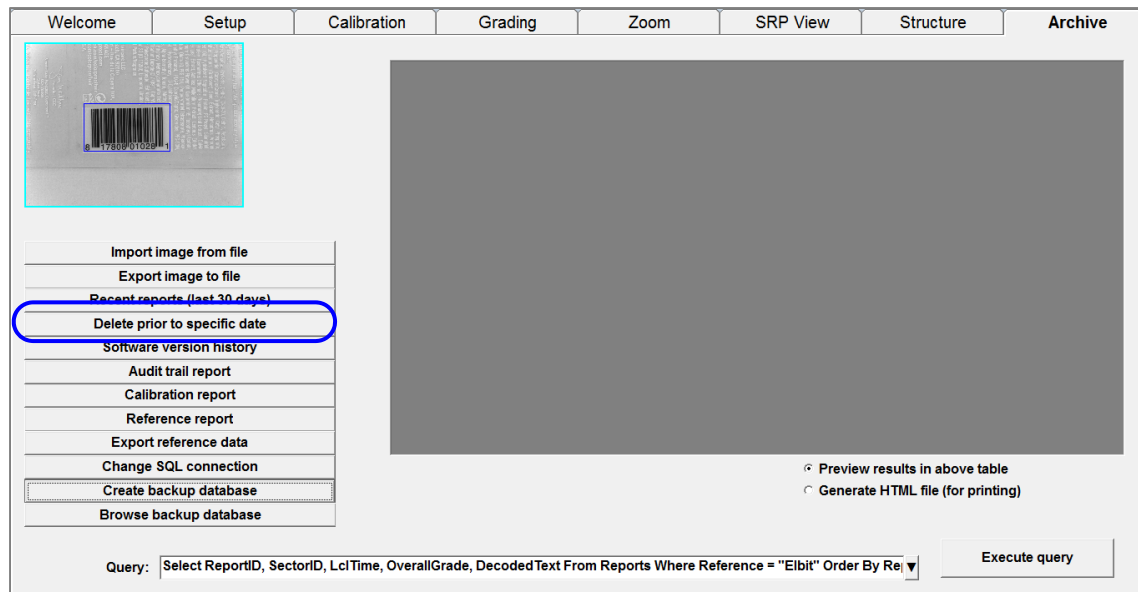


4. In the **File name** box, enter a new name for the file, or keep the default file name which is entered as LVS-95XX_[current date].

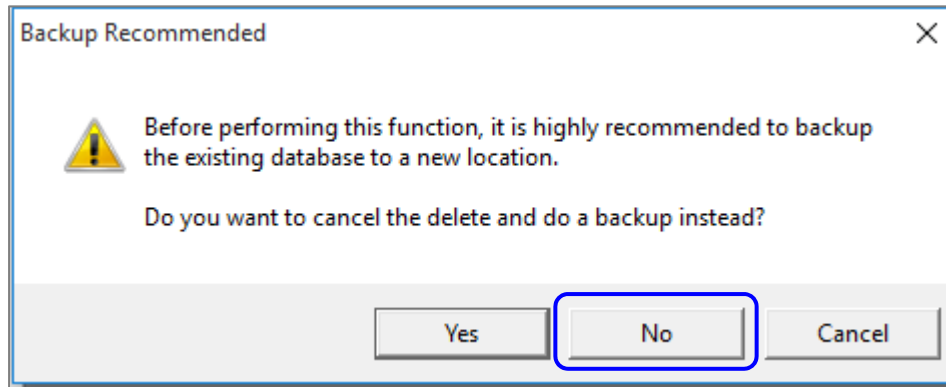


5. Click **Save**.
6. After Backing up the database, select **Delete prior to a specific date**.

NOTE: Only users who are granted the “Allow change archive file” permission are able to delete archive data; this permission can be found by clicking the “Setup Operators” button on the “Setup” tab screen.



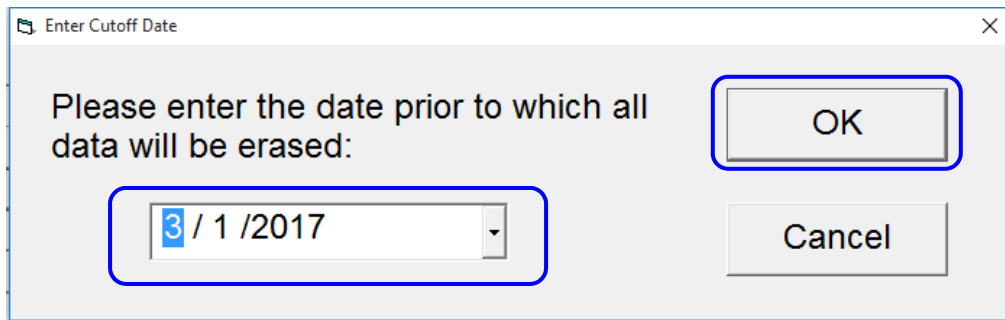
7. If you *did not* create a backup, the below warning will appear prompting to perform the backup first..



If backup has been performed, select **No**.

8. Enter the date prior to which all data will be erased and select **OK**.

The date should be entered as the date the backup was performed (EX.. Current day).



9. The number of deleted records will be displayed on the screen. After deleting the records, close the software and then reopen it. The database will automatically compact and the Archive tab will not contain data prior to today's date.

The Backed up databases can be accessed by selecting Browse backup database.

