Recovery Password, Backup & Restore

Overview

Upon upgrading the Paxton10 software to version 4.7 SR2 or higher, the system will require a Recovery Password to be created. This password applies to the system, and not the user creating it. The password is used to encrypt any backups created and it is then needed to restore from those backups.

It is important to remember and appropriately store the Recovery Password, as without it, you will not be able to restore your system.

The Recovery Password can be changed in the system Options menu, but it will only apply to any subsequent backups that are created.

Create the Recovery Password

Upon upgrading the Paxton10 software to version 4.7 SR2 or higher, when a System Engineer user logs into the system it will require them to create a Recovery Password. The Recovery Password must be created and the message cannot be closed until the password has been set.

A backup USB stick must be plugged into the Paxton10 server in order to proceed.

The requirements for the password (length, special characters etc) are the same as if creating a user for the system. The system will indicate if the password entered is acceptable or not.

Once successfully set, a new backup will be immediately created and it will be encrypted with the new password. The system will automatically delete any unencrypted backups. Any existing encrypted backups on the USB stick will not be deleted, as they may be required if intending to migrate to a new or factory reset server (see below).

Migrating to a new or factory reset server

IMPORTANT:

a) If you intend to restore from a backup that was created on a system without a Recovery Password unencrypted) to a new server that is requesting you to create an initial Recovery Password, do not proceed and instead contact Paxton Support, as the backup data will be automatically deleted from the USB stick.

b) If you intend to restore from a backup that was created on a system with a Recovery Password (encrypted) to a new server, it is essential that the Recovery Password set on the new server matches the old server.

Change the Recovery Password

The Recovery Password can be changed from the system Options menu. A backup USB stick must be plugged into the Paxton10 server in order to proceed. Once successfully set, a new backup will be immediately created and it will be encrypted with the new password. The system will automatically delete any other existing backups as these are deemed redundant as the password is no longer known.

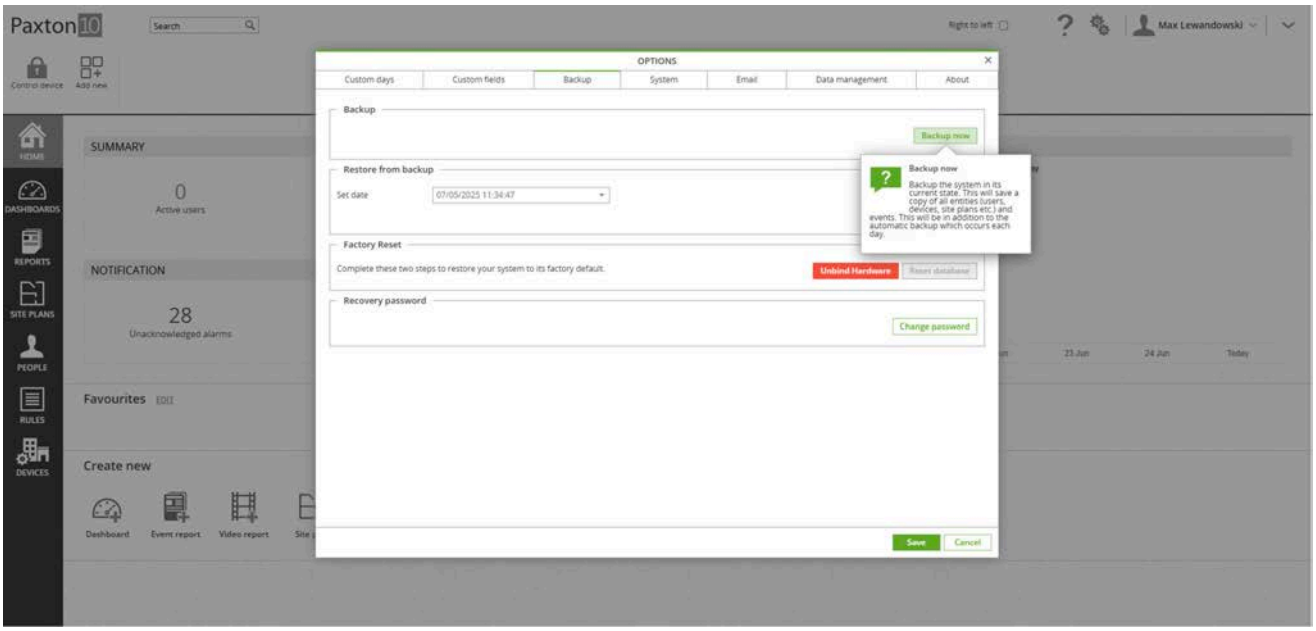
APN-0061-AE

Backup the system

The system is backed up automatically each day, however it can also be backed up manually.

Manual backup

Select the '**System options**' icon from the top right of the screen, select the '**Backup**' tab, then select '**Backup now**'



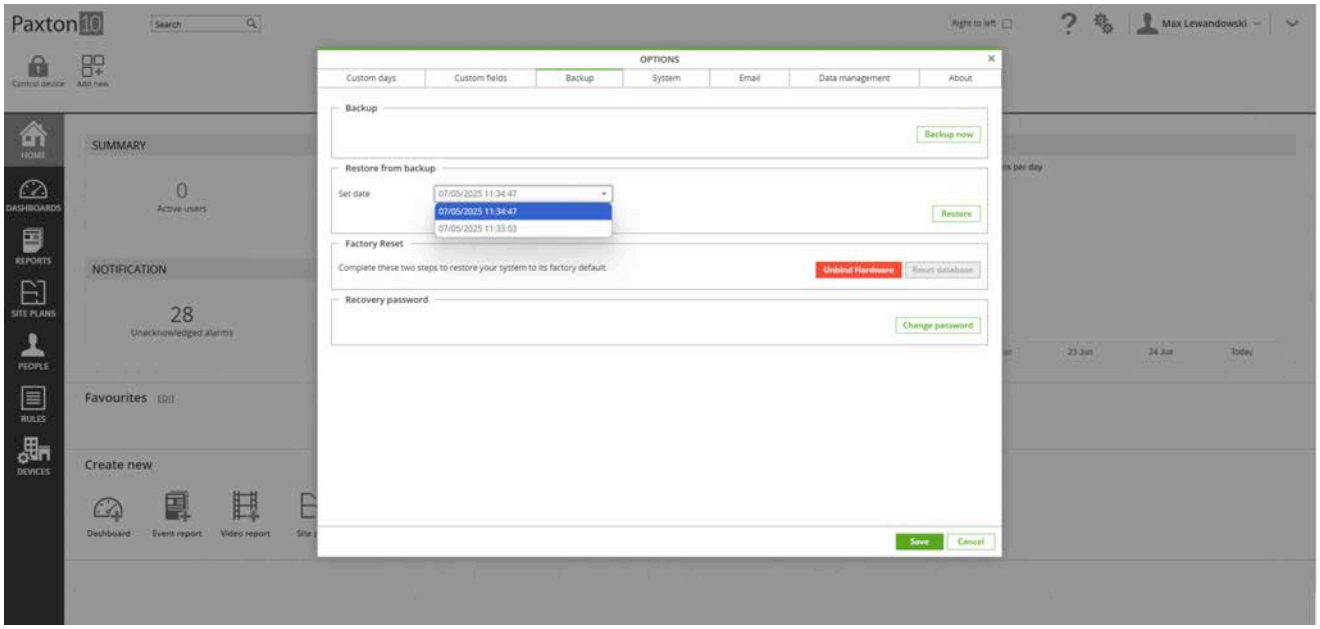
The system can still be used while a backup is in progress. A notification message is displayed when the backup is complete.

Restore from backup

The system can be restored to a previous state. Restoring the system will restore all settings and elements to the state they were in when the system was backed up. All events and changes made since the chosen date will be lost.

1. Select the '**System options**' icon from the top right of the screen, then select the '**Backup**' tab
2. Select the date to restore from the drop down
3. Select '**Restore**'
4. If the backup is encrypted with a Recovery Password, you will be prompted to enter it

Note: If the system has requested the Recovery Password to restore, without it, you will not be able to restore the system. In this situation, it is advised that you change the Recovery Password in the system Options menu. This password will then apply to any subsequent backups created. You should then seek to manually fix the issues that triggered the need to perform a restore, e.g. manually re-create accidently deleted users.



When the restore begins, all users will be logged out of the software. The Paxton10 software will redirect you to the login page when the restore is complete.

Restoring Limitations

Restoring from a backup allows you to revert your system to a known working point in time. However, there are some limitations to what can be restored. The following guide outlines the unsupported scenarios.

Unsupported Scenarios

Restoring Deleted Hardware Devices

If a hardware device has been deleted from hardware management after the relevant backup was captured, restoring will show that hardware device in hardware management, but it will not function as it has reset. You will need to delete the hardware device from hardware management, let it rediscover, and rebind it to the software device.

Restoring Reset Hardware Devices

If a hardware device is reset using the reset button on the physical device after the relevant backup was captured, restoring will show the hardware device in hardware management, but it will not function as it has reset. You will need to delete the hardware device from hardware management, let it rediscover, and rebind it to the software device.

Restoring Reset Master Controllers

If a master controller is reset using the reset button on the physical hardware device after the relevant backup was captured, restoring will show the hardware device in hardware management, but it will not function as it has reset. You will need to delete all hardware devices from that topology from hardware management, add a master controller, rebind it to the software device, and let it rediscover all secondary devices. All secondary devices need to be bound again and remapped to existing software devices.

Restoring After a Failover

If a failover has occurred and a new master controller has been configured after the relevant backup was captured, restoring will show the hardware device in hardware management as the master controller, but it will not function correctly as it is no longer the master controller. You will need to delete all hardware devices from that topology from hardware management, add a master controller, rebind it to the software device, and let it rediscover all secondary devices. All secondary devices need to be bound again and remapped to existing software devices.

Differences in Software Versions

If you are restoring to a backup point that was captured on the latest software version to a new server, please ensure that server is first updated to the latest software version before restoring. If you are restoring a backup where there is a mis- match in versions, then database issues may be experienced due to version changes and triggering a firmware update or downgrade to hardware, which may fail.

Factory Reset and System Restoration

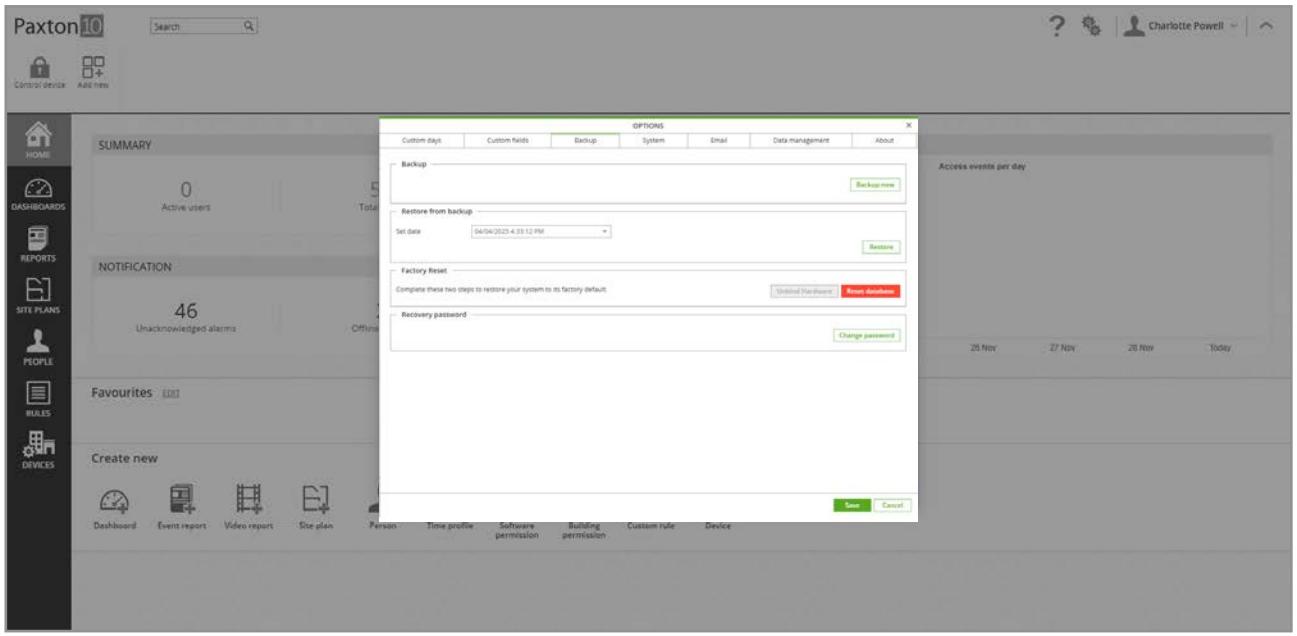
Return to system default

It is possible to factory reset the software to its default settings. Doing so will remove all user data and preferences, including any devices and bound system devices.

1. Select the '**System options**' icon from the top right of the screen, then select the '**Backup'** tab

2. Select '**Unbind Hardware**' - This will unbind any hardware connected to allow it to be connected to a different system

3. Select '**Reset database**' to factory reset the system



All users will be logged out and the system restored with its initial settings. The Paxton10 software will redirect you to the first-time login page when the restore is complete, allowing you to create a new system engineer login.

Paxton10 controllers bound to the system prior to the system restore may need to be reset before they can be redetected by the system. Hold down the reset button located on each controller for 10 seconds.