Mastercard Datacash ATS Backups

This guide shows you how to back up and generate the node encryption keys and the transaction log needed to recover the transaction log that stores offline transactions, which are only in the this transaction log until the daily submission.

Node Encryption Keys

Node encryption keys are use solely by Mastercard's datacash ATS solution. It is important to backup and secure this key to be able to recover any transaction log. the Transaction log will store card holder data and store off line transactions which will include anything under the floor limit until it has a chance to upload them.

If the encryption keys are lost, then the card data cannot be accessed and the acquirer will be unable to pay the retailer. MasterCard Payment Gateway Services and Comtrex Systems has no means to access encrypted data without the keys.

If an encryption key backup falls into the wrong hands, it may be possible for the card data to be accessed and compromised.

If the integrity of a key is suspected of having being compromised, the key must be replaced. The key must be deleted with caution. If a live key is deleted, all data dependent on it will no longer be accessible and monies may be lost. If the compromised key was the current key, it must be replaced by generating a new key.

The process to back and generate keys requires administrator privileges to perform these sensitive operations. The key custodians must be therefore be logged on to an account that has administrator or backup operator rights. Access to this account must be protected by a strong password. A strong password here means a password consisting of at least eight characters and comprised of a mixture of uppercase letters, lowercase letters, and digits.

Node Encryption Key Generation

New keys must be generated on a regular basis. By default the lifetime of a key is 365 days. The key lifetime is specified when it is created. Key generation is performed automatically if all keys have expired, but users may wish to manually generate keys in order to have a controlled system where keys are generated and then immediately exported to a key backup file and key backup file moved to a secure location. The following guidelines must be considered:

- Any location (on site or offsite) that backup keys are stored, that location must have adequate physical security measures to ensure that unauthorized entry to the backup keys cannot be gained.
- If a courier is being used to transport backups to another location, a reputable vendor must be used and the security of the backups during the transportation to the offsite location must be adequate to ensure that unauthorized access cannot be gained to the backup.
- Keys are rotated (renewed) based on the date, the default lifetime for a key being 365 days

Node Encryption Key Backup

Keys can be backed up to an external file (named ATSKEYS.XML by default). Backups can only be performed from a Windows account that has the Backup Operator privilege enabled - this account must be restricted to trusted members of staff (those who have key custodian responsibilities). The backup file itself is encrypted by two passwords (which must contain both letters and numbers, and must be at least 8 characters long). These passwords must be supplied by two different key custodians, thus preventing either of them from maliciously restoring the keys alone. Allowing malicious users to perform a backup could result in the card data being

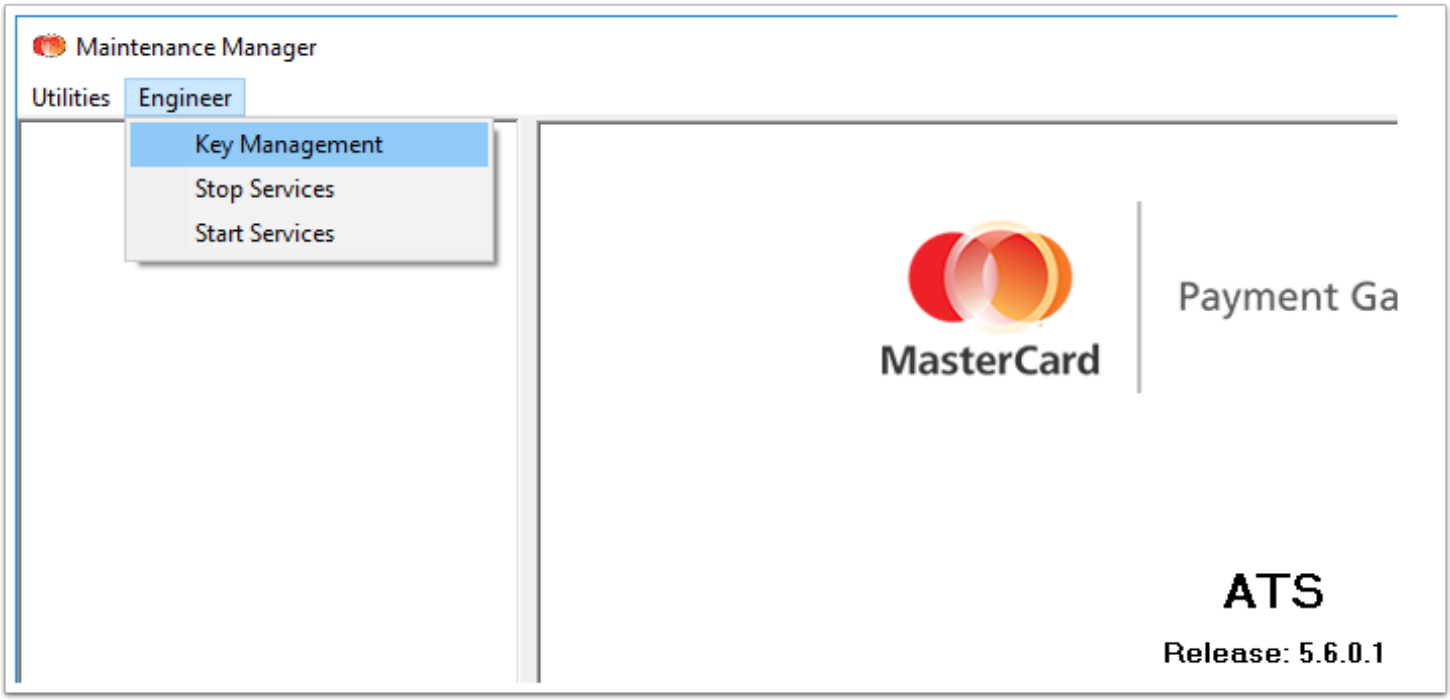
compromised. The backup must be copied elsewhere and the original file securely deleted. See the key backup procedure later in this section.

When keys are backed up two passwords must be entered - one password from each of two key custodians. Each key custodian knows only their own password. Both custodians must therefore be present to backup or restore keys.

It is the responsibility of the Customer to store the key backup files in a secure location. They could for example be copied to a USB thumb drive and the thumb drive stored offsite in a safe. The key backup files should not be stored on a second PC unless that PC is offsite, not connected to any network, and physical access to the PC is controlled.

It is strongly advised to restrict access to keys to the fewest number of custodians necessary. There must not be so many copies of the keys that control is lost as to who has a copy of the keys. Also to store keys securely in the fewest possible locations and formats.

Once the keys have been backed up and transferred to an alternate PC or USB thumb drive, the backup file on the local machine must be securely deleted by using a forensic tool, such as the free utility SDELETE.

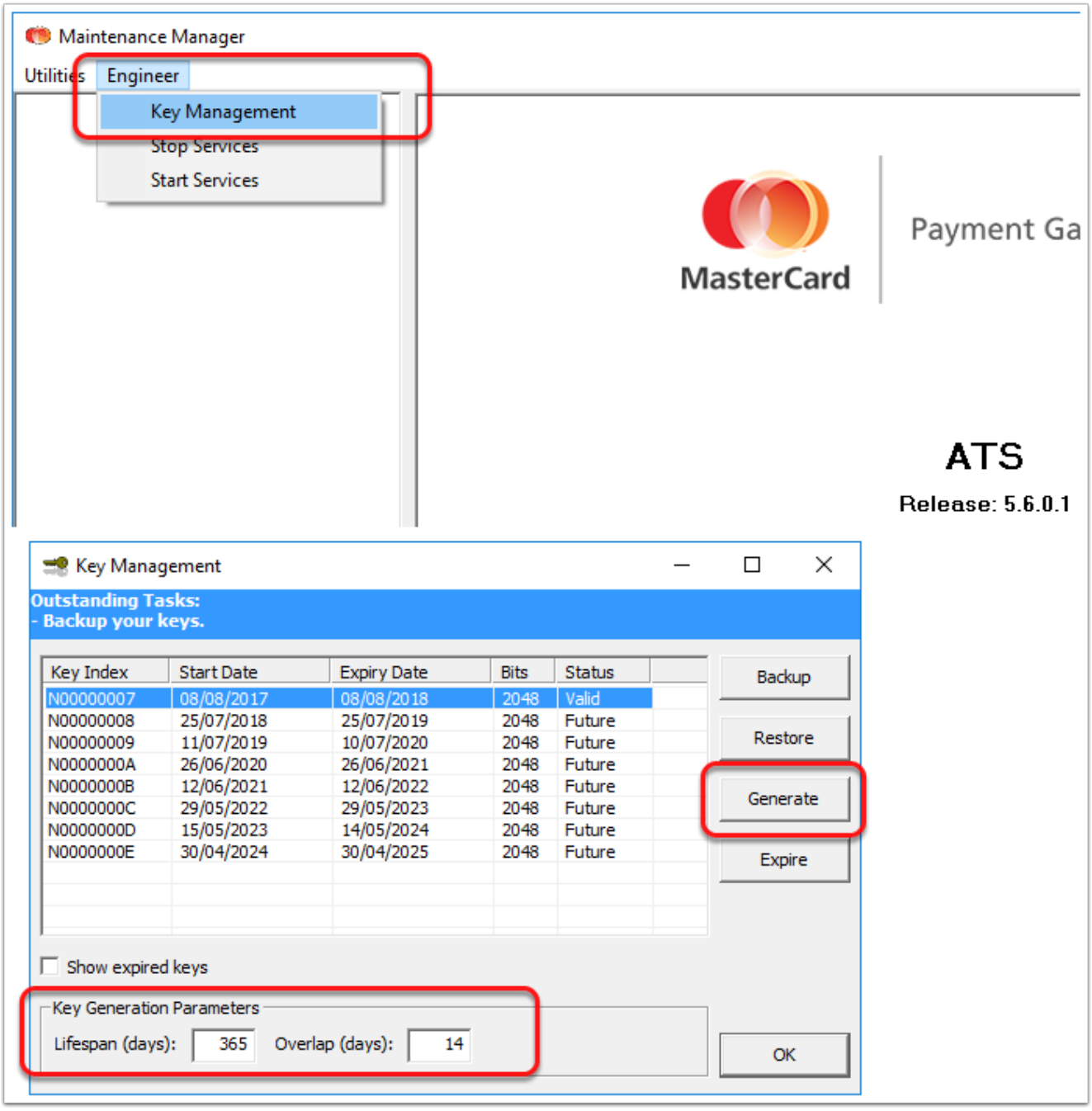


How to Generate New Node Encryption Keys

Open the Maintenance Manager program and go to the [Engineer] menu and select [Key Management].

Simply set the Lifespan (default 365) and Overlap days (default 14) and press [Generate], in the example below you can see that there is a Node Key every year up until 2025. if you do this you'll still need to update each Node Key.

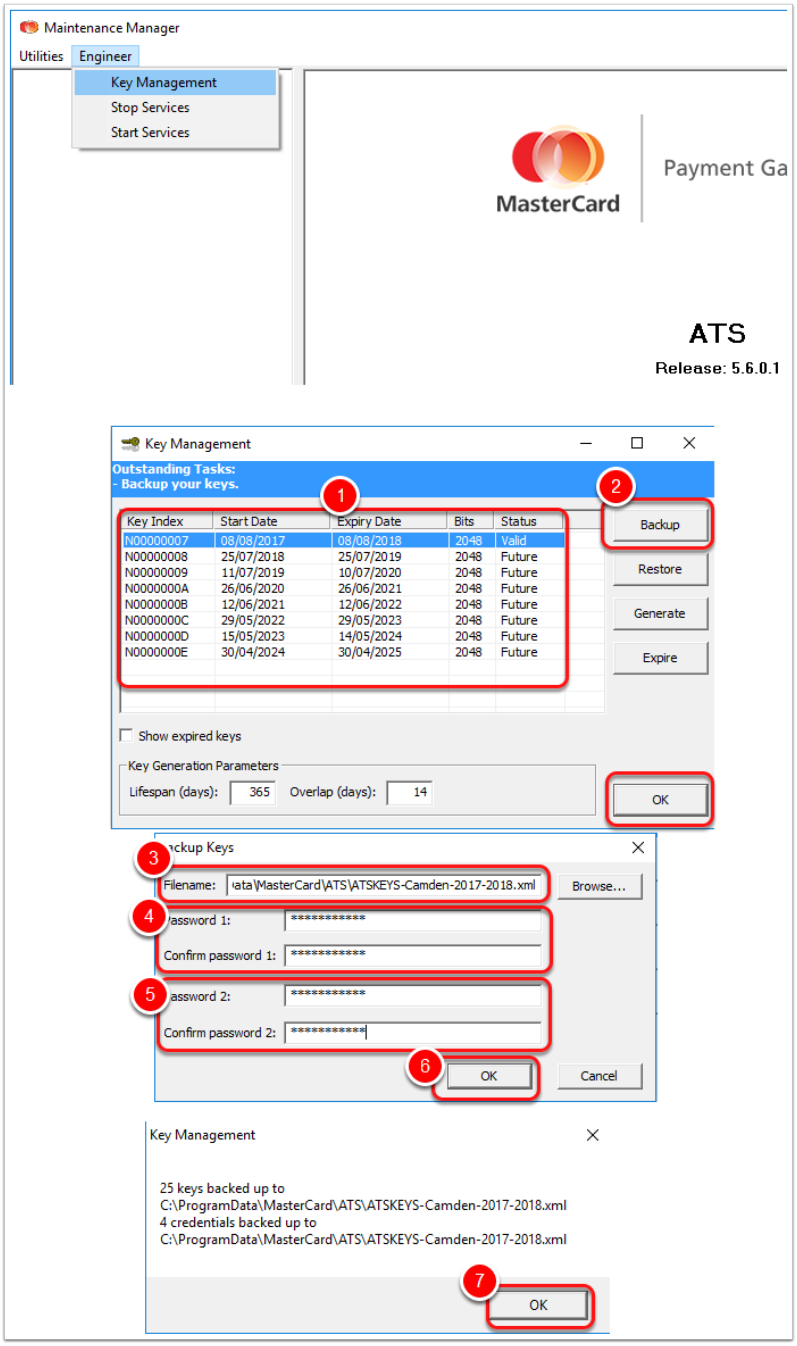
Once finished Press [OK}



How to Back up Node Encryption Keys

Open the Maintenance Manager program and go to the [Engineer] menu and select [Key Management].

1. Select a Key line in the grid you wish to backup
2. press [Backup]
3. Change the name of the file to something that allows you to I dentify it
4. Person 1 enters in Password 1 and confirms
5. Person 2 enters in Password 2 and confirms
6. Press [OK]
7. Press [OK], you'll see multiple keys backed up, but this is not all the key lines
8. Repeat for each Key



How to Restore the Key

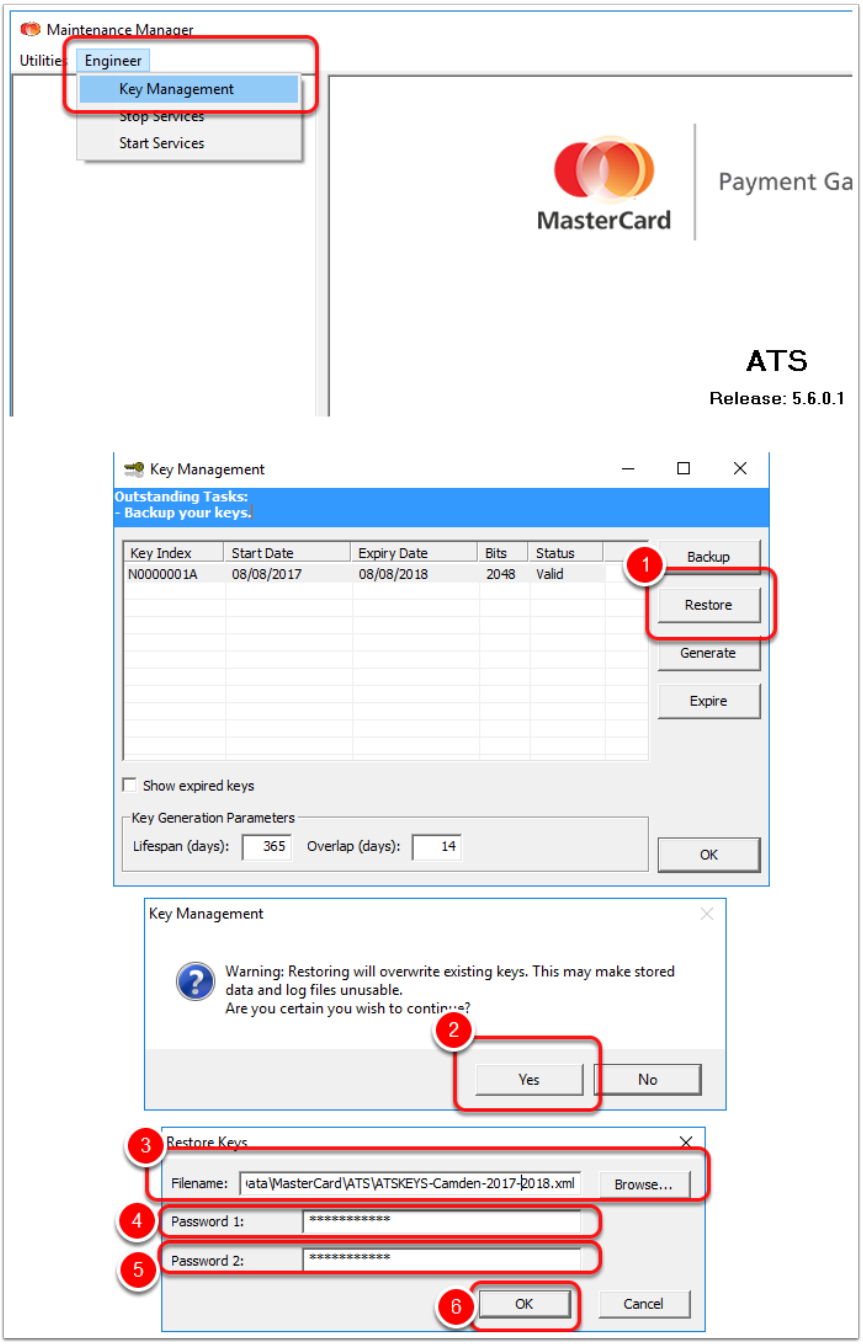
You need to restore the key after the the transaction log file and ASTCFG.XML has been copied to the Mastercard Datacash ATS data directory, the Datacash ATS windows service can not be running when this is replaced but must be running after.

Default ATS data directory is C:\Program Data\Mastercard\ATS

To restore the encrytion key open the Maintenance Manager program and go to the [Engineer] menu and select [Key Management].

1. Press [Restore]
2. Press [Yes] to confirm that the keys will be overridden.
3. Find the Key back up file

4. Person 1 to enter in Password 1
5. Person 2 to enter in Password 2
6. Press [OK]
7. Ensure the Datacash ATS Scheduler Windows Service is running and wait for the overnight submission to submit any transactions.



Transaction Log Back up

There are a few different log files you can backup but the C:\ProgramData\MasterCard\ATS\ECP_TRAN.LOG file is the one with the transaction data that will need recovering.

To back this file up you need to stop the Datacash ATS windows service, copy the file and start the service again.

Note that while the service isn't running no payment can be taken and any payments in waiting will need to be resent from POS to the PEDs again. If a transaction is midway through and the service stop then the transactions will be in a state where we can not tell if it has go through or not.