

Itesso – IDPMS customer release notes IDPMS 3.16.4

Change log

Version	Author	Description	Date
1.0	DVH	Initial version	22-06-2015
1.1	DVH	Adding On Premise Update	15-07-2015
1.2	DVH	Review	15-08-2015

Contents

Overview	3
PCI SSC Data Security Standards	4
Understanding PCI	4
Important note	4
IDPMS settings	5
IDPMS Security Settings	5
Changes for the IDPMS user	7
User right settings.....	7
Changes to the folio screen.....	7
View credit card numbers	7
User account security and password policy	8
Credit Card data	8
Credit card encryption	8
Purge credit card data	8
IDPMS Automatic On Premise Update.....	9
General	9
Update types.....	9
Manual update check	10
Update Notification	10
Update notification IDPMS e-mail.....	10
Update installation	11
Diagnostic data collection	12
Other changes	13

Overview

This document describes the major changes and enhancements in IDPMS version 3.16.4. A detailed document on all (technical) updates can be requested via our support department.

Although IDPMS version 3.16.4 does not seem to have an extended list of new features and fixes, it does contain two new modules that are of major importance for future IDPMS releases.

This document describes the functionality of these two new modules and lists the smaller enhancements in this version.

Our Itesso support department will contact the hotel to schedule the installation of this new IDPMS version or you can contact them directly for quicker scheduling.

PCI SSC Data Security Standards

IDPMS versions previous prior to v3.16 are fully complied with the Payment Application SSC Data Security Standards (PA DSS) 1.0 as an optional module.

As of version 3.16 IDPMS is the certified version following the latest PCI PA-DSS 2.0 guidelines and the security settings are no longer optional.

Understanding PCI

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. Defined by the [Payment Card Industry Security Standards Council](#), the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

For more information about PCI compliancy please visit web page(s): [PCI Security Standards Council page](#) or [Wikipedia PCI](#)

Important note

IDPMS v3.16 ensures that you are PCI Ready but not PCI Compliant. If you want your IDPMS environment to be PCI Compliant then one of our Product Specialists has to come on-site to provide all workstations running IDPMS with new database connectivity software. Also the SQL Server configuration running the IDPMS database has to be modified.

For more information our Itesso Sales team can be contacted.

IDPMS settings

As of IDPMS v3.16 the PA DSS rules for payment applications are enforced as a standard. This means the security options in the IDPMS setting are enabled by default and cannot be switched off.

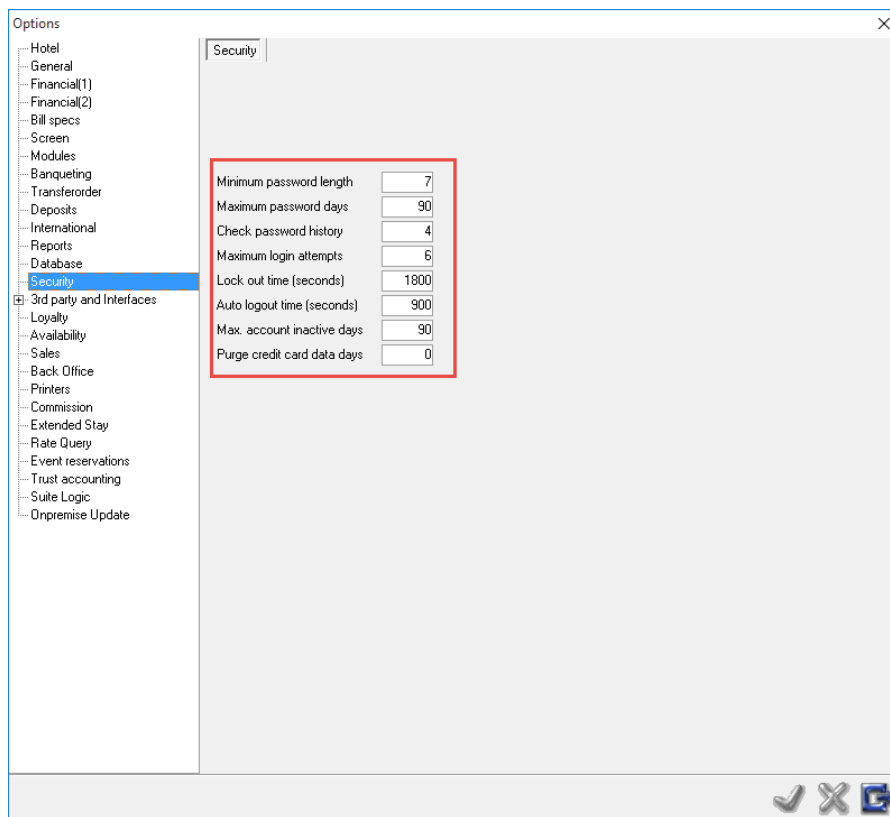
For IDPMS this means:

- Security settings for the IDPMS users related to password policies and user account expiry.
- Auto log out after 15 minutes.
- Encryption of credit card data with a for each hotel unique encryption key.
- Automatic removal of all credit card data after 60 days.

IDPMS Security Settings

The Security setting can be found in the IDPMS settings. The values are populated automatically and set to the PA DSS required values. Although the values can be changed to a higher or lower value, IDPMS will set them back to the default values if they exceed the minimum or maximum value for the specific settings.

For example: Auto logout time can be set to a lower value but not to a higher value as 900 seconds, as this is the maximum idle time allowed by the PA DSS standards. So if a user is not using IDPMS actively for 15 minutes he/she is logged out automatically

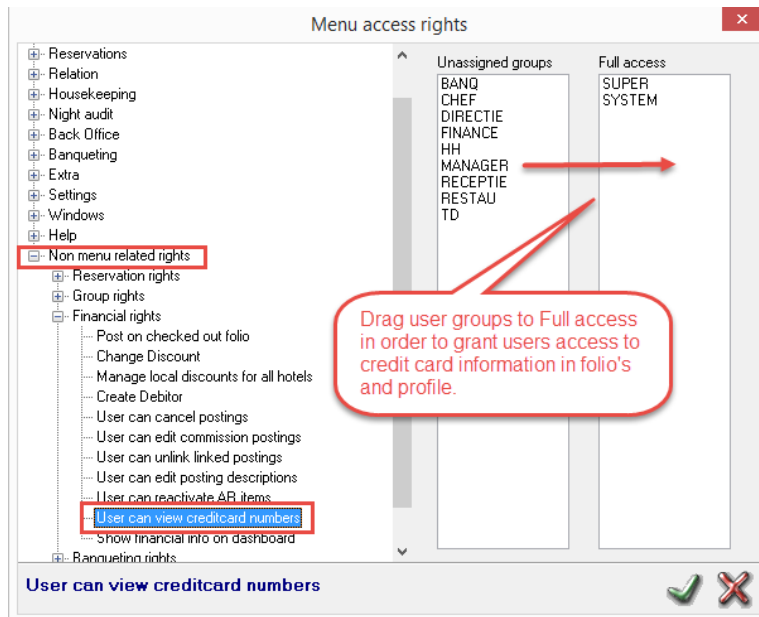


- **Minimum password length:** The minimum password length can be set here. The minimum number of characters is 7.
- **Maximum password days:** Maximum days after the user password expires and must be renewed.
- **Check password history:** Number of password changes before a previous password can be re-used.
- **Maximum login attempts:** Maximum number of login attempts before the user is locked out.
- **Lock out time:** The time between last unsuccessful login and user being locked out and the time the user login/name is activated/available again. For example: User has attempted to login with incorrect password. After x unsuccessful attempts the user account will be disabled for the time defined in this setting.
- **Auto logout time:** IDPMS will automatically logout any user after a period of system inactivity. The maximum time for the system idle is 15 minutes in PCI DSS environments.
- **Max Account Inactive days:** Maximum number of days a user name can remain unused. After this period the user account is automatically deactivated. Deactivated users can only be reactivated by an IDPMS user with sufficient right or by the Itesso support desk.
- **Purge credit card days:** All credit card data in guest profiles, reservations and log files is automatically erased/purged after the number of days configured relative to the last depart date.

Changes for the IDPMS user

User right settings

With the PCI DSS settings enabled new user right settings are required. In order for an IDPMS user to be able to view credit card information the user right indicated below must be set for each IDPMS user group entitled to view credit card information.



Changes to the folio screen

In the (group) reservation screen the credit card number is masked.

Payment	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
Guarantee	<input type="text"/>	Tot. Excl/Incl	100,00	105,00	
	A	B	C	D	
Card #	<input type="text" value="444433XXXXXXXX1111"/>			Expiry date	<input type="text" value="12/15"/>
Card holder	<input type="text"/>			Credit limit	<input type="text" value="0,00"/>

View credit card numbers

In order to view the credit card details the user can double click the credit card number. User is then prompted if the credit card number should be displayed. If user selects “Yes” the credit card number is displayed and this event is logged in the IDPMS database. This screen will stay open till closed by the user.



User account security and password policy

PCI rules also enforce the way user credentials are handled. The following rules are applied to the IDPMS user credentials.

- Strong passwords: This setting enforces strong password policy. (password should at least contain a capital letter, a numeric value and one special character like “!” or “#”
- Minimum password length 7 of characters.
- A limited time after which the user password expires and must be renewed.
- Check on password history. Number of password changes before a previous password can be re-used.
- Maximum number of login attempts before the user is locked out.
- Lock out time: The time between last unsuccessful login and user being locked out and the time the user login/name is activated/available again. For example: User has attempted to login with incorrect password. After x unsuccessful attempts the user account will be disabled for the time defined in this setting.
- Auto logout time. The number of seconds of inactivity / idle time after which IDPMS will automatically log out the logged on user.
- Max Account Inactive days: Maximum number of days a user name can remain unused. After this period the user account is automatically deactivated. Deactivated users can only be reactivated by an IDPMS user with sufficient right or by the Itesso support desk.

Credit Card data

Credit card encryption

IDPMS will generate unique encryption keys for each hotel. These keys are used for the encryption of credit card data. An attempt to read credit card data directly from the database will result in unreadable data.

Purge credit card data

Another important requirement of the PCI DSS requirements is purging of all credit card data 60 days after departure date. This means that during the Night Audit all credit card data stored in credit card fields in (group) reservations, relation profiles and logging is removed automatically.

IDPMS Automatic On Premise Update

General

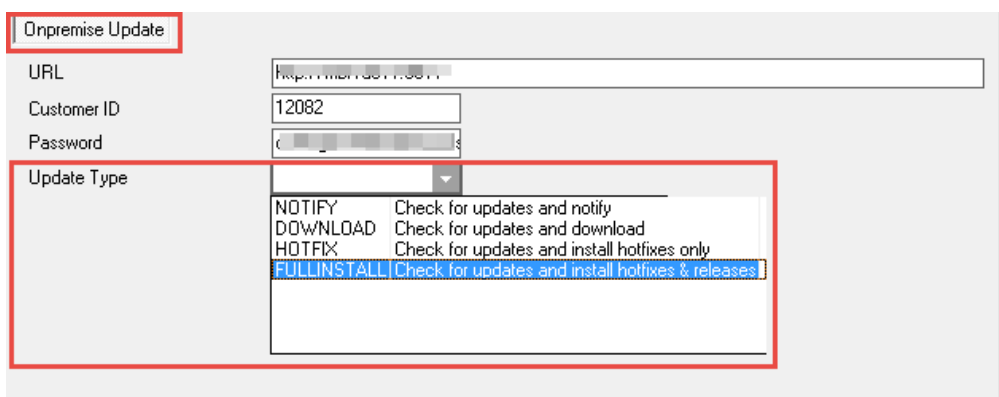
IDPMS release 3.16.4 has another important feature. It enables IDPMS to check for version updates and to apply these updates automatically if desired.

The advantage of this feature is that it allows Itesso to release new IDPMS versions and/or updates at a higher frequency. Updates may contain less new features or fixes per version but the time between versions can be made significantly shorter. With this hotels can benefit from new functionalities and fixes quicker.

Update types

IDPMS has a choice of four Auto update settings. The hotel can choose which type they want to use by selecting their choice in the IDPMS On Premise Update setting from the IDPMS option screen. The default set value is FULLINSTALL suitable for most hotels. For hotel chains and multi property environments the default settings will be set to NOTIFY as other update and acceptance procedures may apply.

- 1) NOTIFY
This setting will check for updates and notify selected IDPMS users that updates are available. The hotel can contact support to schedule a manual update.
- 2) DOWNLOAD
This setting will check for updates, download them and notify selected IDPMS users. This option can be used for hotels that update IDPMS themselves at their own convenience.
- 3) HOTFIX
This setting will check for updates, download updates, notify selected IDPMS users and update the IDPMS version automatically for Hotfix releases only.
- 4) FULLINSTALL
This settings is used to check for updates and install any hotfix or new IDPMS version automatically.



Onpremise Update

URL:

Customer ID:

Password:

Update Type:

NOTIFY	Check for updates and notify
DOWNLOAD	Check for updates and download
HOTFIX	Check for updates and install hotfixes only
FULLINSTALL	Check for updates and install hotfixes & releases

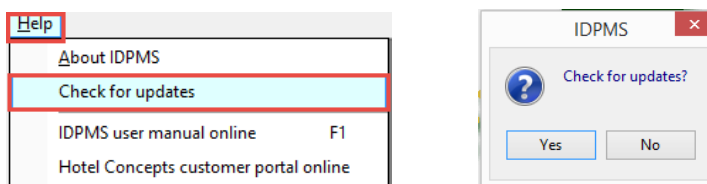
At the end of each night audit process IDPMS will check if there are updates available and, depending on the configured update type setting, apply the updates and/or send out a notification.

Manual update check

Users may also check manually for updates by navigating to the IDPMS help menu and select the option “Check for Updates”. This menu item is only available for user that are member of an IDPMS user group designated as Update Admin.

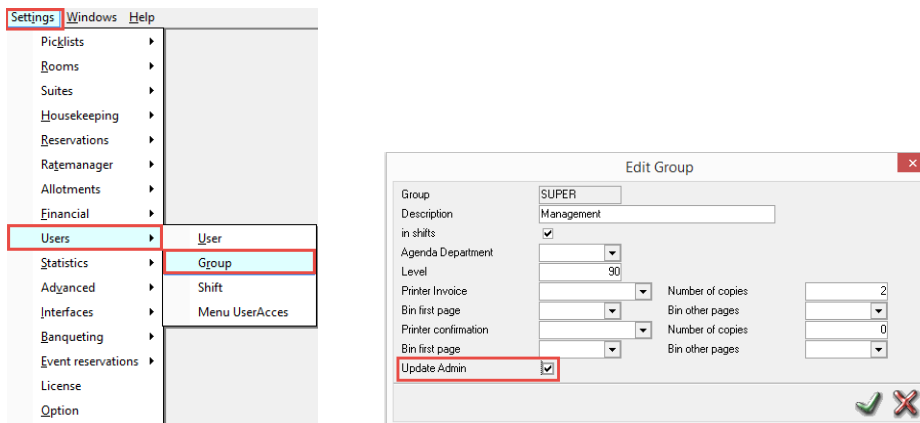
Depending on the On Premise Update settings, IDPMS will process all available updates immediately after the option “Check for update” has been selected.

The manual update check can be found in the help menu and IDPMS prompts if it should check for available updates.



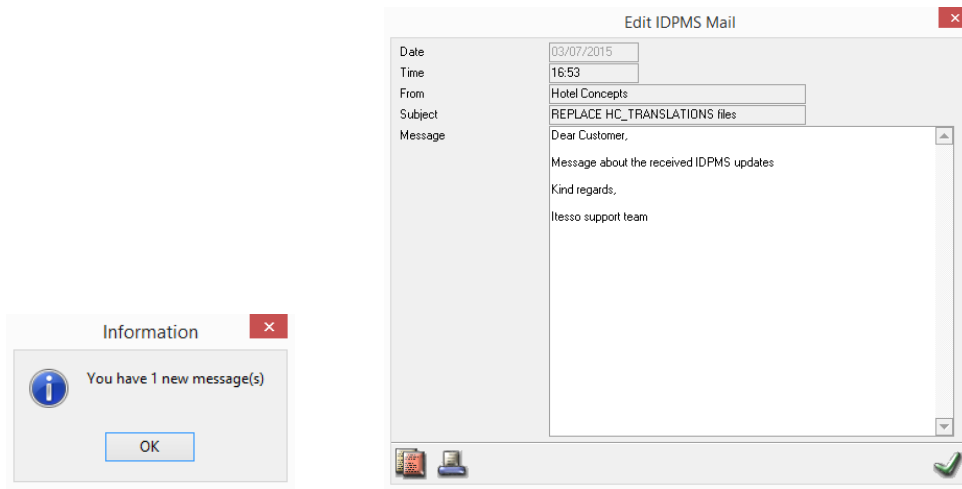
Update Notification

If an update is available a selected group of users will receive a notification through the internal IDPMS e-mail system. All users linked to the assigned user group(s) that is/are marked as “Update Admin” will receive a notification if an update is available.



Update notification IDPMS e-mail

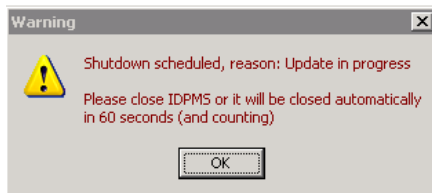
If an update is found an IDPMS e-mail message is created containing information about the update and all users part of the Update Admin member group are informed



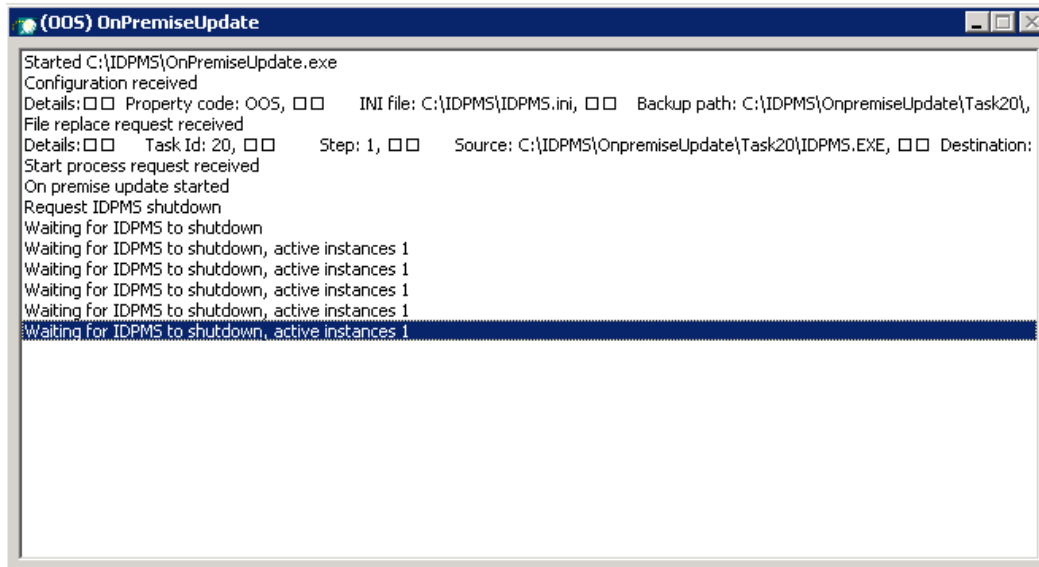
Update installation

If an IDPMS update was found and the update setting is set to FULLINSTALL, IDPMS will immediately download the files and apply the update. Some updates can be done while IDPMS is running, others may require IDPMS to shut down.

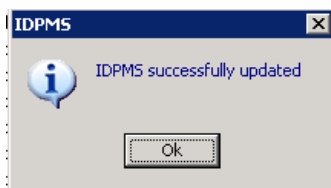
In case an update has to replace files that are in use when IDPMS is still running, IDPMS will be shut down automatically in 60 seconds. This action cannot be cancelled and all open IDPMS instances will be closed automatically



After IDPMS has been closed on all workstations the On Premise Update application executes the update and the progress can be followed on screen.



After the update has been completed IDPMS is automatically started and the result of the update is displayed on screen. This is only displayed on the client/computer that initiated the update. On other clients/pc's IDPMS has to be started by the user.



In case the update did not succeed any changes made during the update procedure are rolled back and the Itesso support desk is notified automatically. The hotel will be contacted to fix the possible cause of the failed update.

Diagnostic data collection

The On Premise Update module will also send diagnostic data related to all Itesso software installed at the hotel to an Itesso server. This data contains information such as IDPMS software version number, running interfaces, database size and any errors that were logged by IDPMS and/or interfaces.

This information not only allows Itesso to schedule important updates or hotfixes for our customers but also enables us to pro-actively support any error or issue before they happen. For example disk space limitation that may prevent the database server to write data to the IDPMS database or monitor the functioning of interfaces.

Other changes

Below a summary of other enhancements and improvements. For a detailed list contact our Itesso support agents.

- Review of credit card encryption logic following latest PCI DSS specifications
- Review of all modules and logic related to PCI DSS.
- Fixed a number of memory leaks which could lead to exhaustion of computer RAM memory especially in terminal server environments where IDPMS can stay active for longer periods at a time.
- When extended rate functionality was switched off the rate grid screen was not correctly displaying all fields. Extended rates allow hotels enter rates up to 6 adult and multiple children in the rate grid screen.
- Fixed misalignment in various screens that allow user to multiple select lines. For example the posting detail screen (F5) and the batch assign room number screen. When selecting multiple lines the selection shifted to different line then the ones that were selected.
- General performance improvements for Azure/Cloud environments.
- A bug in the Rate Query has been fixed that showed the hotel availability and rate in combination with a group block. Now the available rates and rooms from the selected block are displayed again.
- Rate Query performance for fetching and displaying grouped rates has been significantly improved.
- CCV format error that occurred when doing a direct sale has been fixed.
- Fixed a bug that caused reloading of manual rates in reservations linked to a group when viewing daily rates from within the group itself.