



iVitos User Guide

Version 1.0

User Manual

Copyright © 2016 Vitani A/S

Table of Contents

Document information	4
Summary	4
Change History	4
Copyright	4
Introduction	5
Aim	5
Scope	5
Structure of this document	5
Reference	5
Terms, Abbreviations and Definitions	5
GUI	7
Login	7
iVitos GUI	8
Search, Add, Edit, Delete	9
CARDHOLDER	10
Employee	11
Visitor	13
Contractor	14
CARD	16
Issue	16
Remove	17
Block	18
Unblock	19
ACCESS LEVEL	20
Add	20
Remove	21
MANUAL OPERATION	22
Door	22
ACCESS	23
Grant Access	23
Unlock permanent	24
Lock permanent	25
Intrusion	26
INTRUSION	26
Arm	26
Disarm	27
PROFILE	28
User	28
LOG	29
Eventlog	29
FAQ	30

Document information

Summary

Quick Guide for User to daily operation of iVitos.

Version

1.0

Date

5 January 2016

Change History

Version	Date	Author(s)	Nature of Revision
1.0	05-01-2016	CN	First version

Copyright

This manual is proprietary information of Vitani. Unauthorized reproduction of any portion of this manual is prohibited.

No part of this document may be reproduced, in any form or by any means, without permission in writing from the publisher Vitani A/S.

Copyright © 2016 by Vitani A/S, Denmark and its respective companies.

All rights reserved.

Disclaimer

The material in this manual is for information purposes only. Vitani assumes no responsibility for incorrect information this manual may contain.

Vitani reserves the right to vary the specifications, standards and method of operation of any or all of the equipment described herein at any time without notice to any party.

Vitani reserves the right to publicize any such changes by issuing updated versions or new editions. The information contained herein was up to date at the time of publication. We reserve the right to make subsequent changes to technical or organizational details.

Vitani assumes no liability for problems resulting from the use of this manual.

Introduction

Aim

This document describes how the daily user can handle cardholders, cards and intrusion system in iVitos.

Scope

This document focuses on how the daily user can use the iVitos GUI for handling cardholders, cards and intrusion system in iVitos.

This document is intended for the daily users of iVitos and does not require any previous knowledge of the iVitos cloud.

Structure of this document

First part shows how the iVitos GUI is used when logged in as a normal User.

Reference

For further information regarding iVitos please look in:

iVitos Cloud Manager Guide

iVitos Installer Guide

iVitos Controller Installation Guide

iVitos Door Configuration Guide

Terms, Abbreviations and Definitions

iVitos	Cloud based Access Control system used as primary GUI for handling personnel information and access rights for connected door controllers.
Cardholder	Cardholders are persons who can be authorized to enter certain areas in a building by means of an identifier (card).
Schedule	Schedules specifies a period of time during the day.
Holiday	Holidays are specific days defined with a period of time during the day.
Door	A door is defined as any exterior or interior door with an electronic means of entry, such as a keypad or card reader
Access Level	An Access Level is a combination of a door with day/time schedule and eventually intrusion. Access Level is also known as authorization.

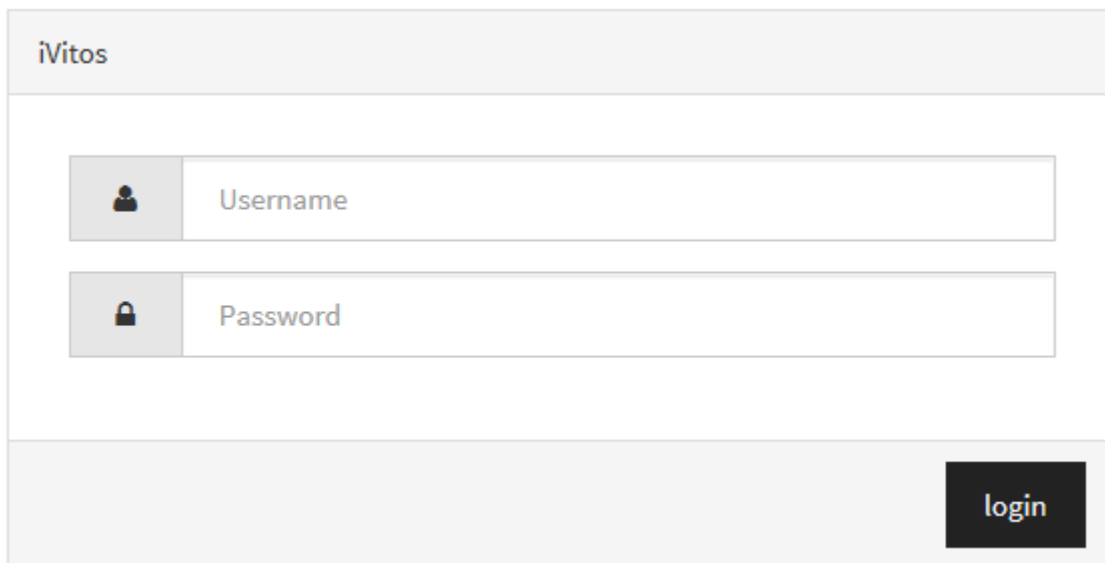
Installer	The company doing the physical installation at the customer/enduser site.
Customer	Customer by Installer
User	Employee by Customer
Technician	Employee by Installer. Person who is doing the physical installation of Door Controller and configuration for the cloud.

GUI

The user interface in iVitos is browser based using HTML5 which makes it possible to manage the daily operation using your preferred device. This could be iPad, Smartphone, PC or which ever device you prefer to use.

Login

The URL for logging in to iVitos is: <https://cloud.ivitos.com>

The image shows a login form for iVitos. At the top, there is a header bar with the text "iVitos". Below this, there are two input fields. The first field is labeled "Username" and has a user icon to its left. The second field is labeled "Password" and has a lock icon to its left. At the bottom right of the form, there is a dark button with the text "login" in white.**Username:**

Enter **Username** with the format portal\username. The portal defines which cloud system you are connected to.

Example: vitani\lk

Password:

Enter **Password**.

iVitos GUI

When logged into iVitos you will see a screen as below.

The iVitos GUI consists of different menu items which are found in the left side of the screen. In the top of the screen you can see PORTAL, INSTALLER, CUSTOMER and you as the user.



Search, Add, Edit, Delete

USER search

				Q	NEW	EDIT	DELETE
	Firstname	Lastname	Email	Mobile			
<input type="checkbox"/>	Elvis	Presley					

1-1 of 1 < >

Most of the screens found in iVitos GUI do have the same setup where you see a **Search** field below the header text and **NEW, EDIT, DELETE** menu in the right side of the screen. In the middle section of the screen you have a list of the items. In this example it is a list of the different Technicians working for a specific Installer.

Search:

The **Search** field is for free text search.

NEW:

The **NEW** menu item will give you a blank screen for entering information to add a new "item".

EDIT:

The **EDIT** menu item will give you a screen with information already entered for the selected "item". Before selecting **EDIT** you need to mark/select the "item" you want to edit. Instead of marking/selecting the "item" you can also just double click on the item line.

DELETE:

The **DELETE** menu item will delete the selected "item". Before selecting **DELETE** you need to mark/select the "item" you want to delete.

CARDHOLDER

Cardholders are persons who can be authorized to enter (certain areas in) your building by means of an identifier (card). iVitos distinguishes between three types of cardholders:

- Employees: people employed directly by your company.
- Visitors: people visiting your company.
- Contractors: people employed either by „vendors“ (i.e. companies/organizations that are hired by your organization to carry out certain tasks) or by „subcontractors“ (companies/organizations hired by the contractor).

All authorizations in iVitos are linked to cardholders rather than identifiers (cards).

Employee

EmployeeID	<input type="text"/>
Firstname	<input type="text"/>
Lastname	<input type="text"/>
Department	<input type="text"/>
Email	<input type="text"/>
Phone	<input type="text"/>
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Valid from	<input type="text"/>
Valid to	<input type="text"/>
Intrusion	<input type="checkbox"/>

EmployeeID:

Enter **EmployeeID** of person. **EmployeeID** is mandatory and shall be unique (you cannot have two cardholders with same **EmployeeID**)

Firstname:

Enter **Firstname** of person.

Lastname:

Enter **Lastname** of person. **Lastname** is mandatory and shall always be filled out.

Department:

Enter **Department** of person.

Email:

Enter **Email** of person.

Phone:

Enter **Phone** of person.

PIN:

Enter **PIN** code for person. **PIN** is mandatory and shall always be filled out.

Confirm PIN:

Enter **PIN** code for person.

Valid from:

Enter **Valid from** date for person. The person will not be granted access until **Valid from** date.

Valid to:

Enter **Valid to** date for person. The person will not be granted access after **Valid to** date.

Intrusion:

The Intrusion column defines if cardholder is allowed to arm/disarm intrusion system in case cardholder gets access granted when reading card.

You enable **Intrusion** for the cardholder by setting a check mark in the field. If the field is blank then a cardholder will NOT be able to arm/disarm the intrusion system when a card is read.

Visitor

VisitorID	<input type="text"/>
Firstname	<input type="text"/>
Lastname	<input type="text"/>
Email	<input type="text"/>
Phone	<input type="text"/>
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Valid from	<input type="text"/>
Valid to	<input type="text"/>

VisitorID:

Enter **VisitorID** of person. **VisitorID** is mandatory and shall be unique (you cannot have two cardholders with same **VisitorID**)

First name:

Enter **Firstname** of person.

Last name:

Enter **Lastname** of person. **Lastname** is mandatory and shall always be filled out.

Email:

Enter **Email** of person.

Phone:

Enter **Phone** of person.

PIN:

Enter **PIN** code for person. **PIN** is mandatory and shall always be filled out.

Confirm PIN:

Enter **PIN** code for person.

Valid from:

Enter **Valid from** date for person. The person will not be granted access until **Valid from** date.

Valid to:

Enter **Valid to** date for person. The person will not be granted access after **Valid to** date.

Contractor

ContractorID	<input type="text"/>
Firstname	<input type="text"/>
Lastname	<input type="text"/>
Department	<input type="text"/>
Email	<input type="text"/>
Phone	<input type="text"/>
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Valid from	<input type="text"/>
Valid to	<input type="text"/>
Intrusion	<input type="checkbox"/>

ContractorID:

Enter **ContractorID** of person. **ContractorID** is mandatory and shall be unique (you cannot have two cardholders with same **ContractorID**)

Firstname:

Enter **Firstname** of person.

Lastname:

Enter **Lastname** of person. **Lastname** is mandatory and shall always be filled out.

Department:

Enter **Department** of person.

Email:

Enter **Email** of person.

Phone:

Enter **Phone** of person.

PIN:

Enter **PIN** code for person. **PIN** is mandatory and shall always be filled out.

Confirm PIN:

Enter **PIN** code for person.

Valid from:

Enter **Valid from** date for person. The person will not be granted access until **Valid from** date.

Valid to:

Enter **Valid to** date for person. The person will not be granted access after **Valid to** date.

Intrusion:

The Intrusion column defines if cardholder is allowed to arm/disarm intrusion system in case cardholder gets access granted when reading card.

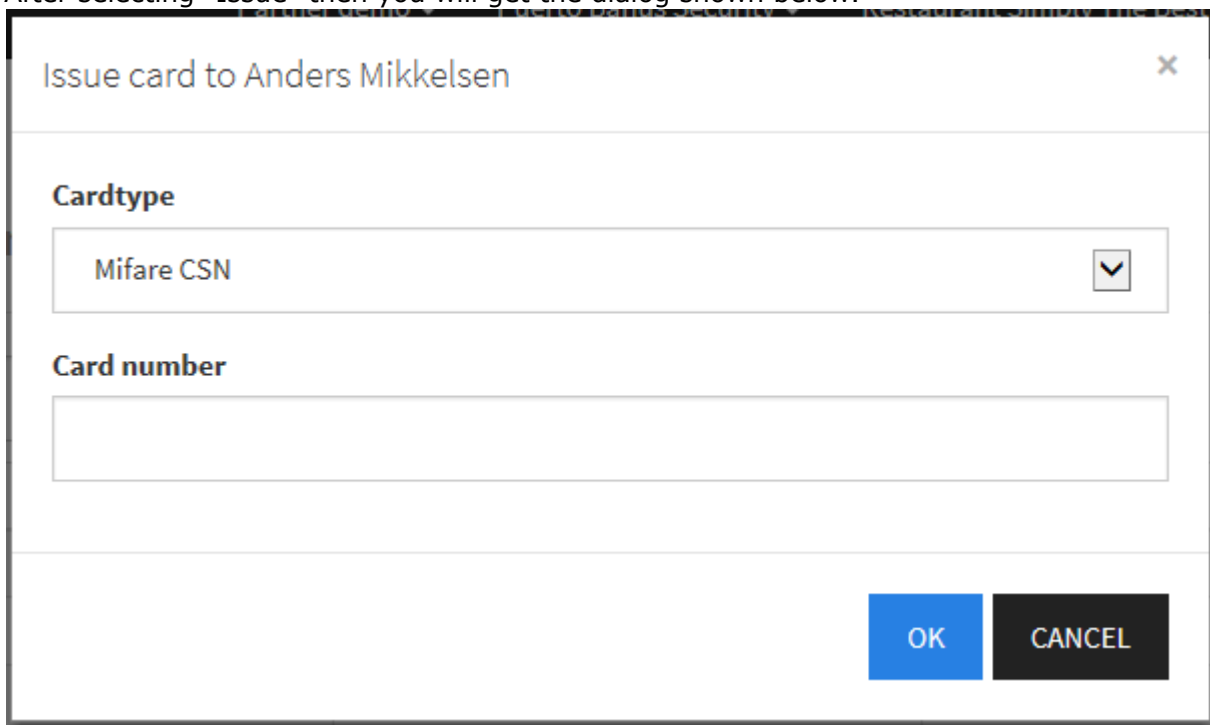
You enable **Intrusion** for the cardholder by setting a check mark in the field. If the field is blank then a cardholder will NOT be able to arm/disarm the intrusion system when a card is read.

CARD

Issue

Select CARD and "Issue" if you want to issue a new card to the selected person. Before issuing a new card you will have to either block or remove existing card because a cardholder can only have one active card.

After selecting "Issue" then you will get the dialog shown below.



Issue card to Anders Mikkelsen

Cardtype

Mifare CSN

Card number

OK CANCEL

Cardtype:

Select **Cardtype** used for cardholder. The **Cardtype** can be one of the following:
Mifare CSN: The Mifare CSN number is used as credential in the system.

Card number:

Enter **Card number** of card. The format of the **Card number** will depend on the Cardtype used.

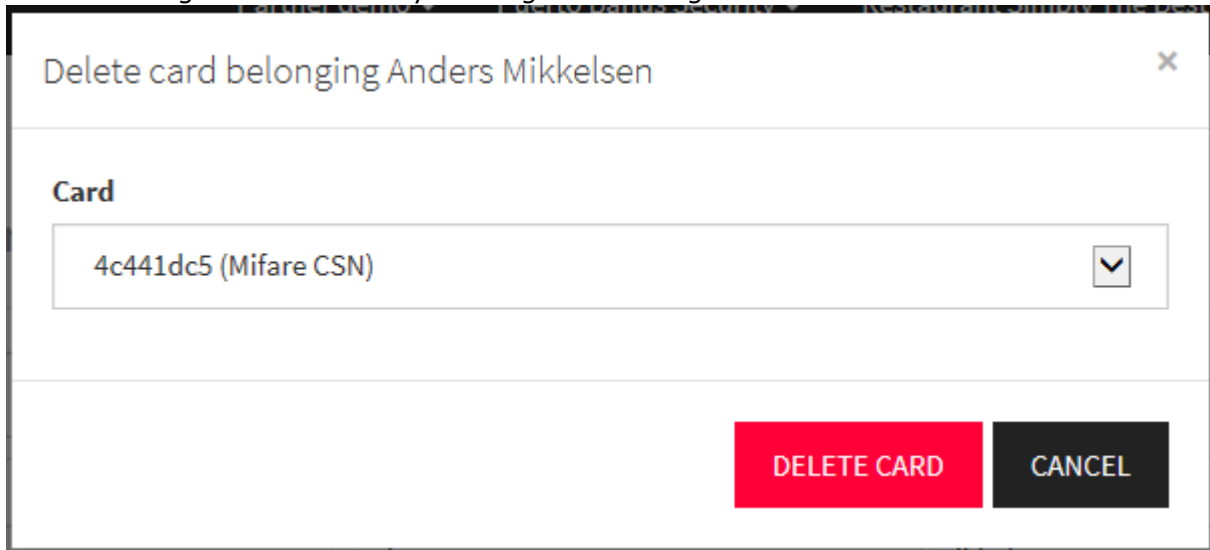
Mifare CSN: The **Card number** shall be specified as an eight digit hexadecimal number.

Normally the easiest way to enter the **Card number** is by using a USB reader which will return the number in correct format.

Remove

Select CARD and "Remove" if you want to delete the card belonging to the selected person. Before issuing a new card you will have to either block or remove existing card because a cardholder can only have one active card.

After selecting "Remove" then you will get the dialog shown below.



The dialog box has a title bar with the text "Delete card belonging Anders Mikkelsen" and a close button (X) in the top right corner. Below the title bar is a section labeled "Card" containing a dropdown menu. The dropdown menu is open, showing the selected card ID "4c441dc5 (Mifare CSN)" and a downward arrow icon. At the bottom right of the dialog box are two buttons: a red button labeled "DELETE CARD" and a dark gray button labeled "CANCEL".

Card:

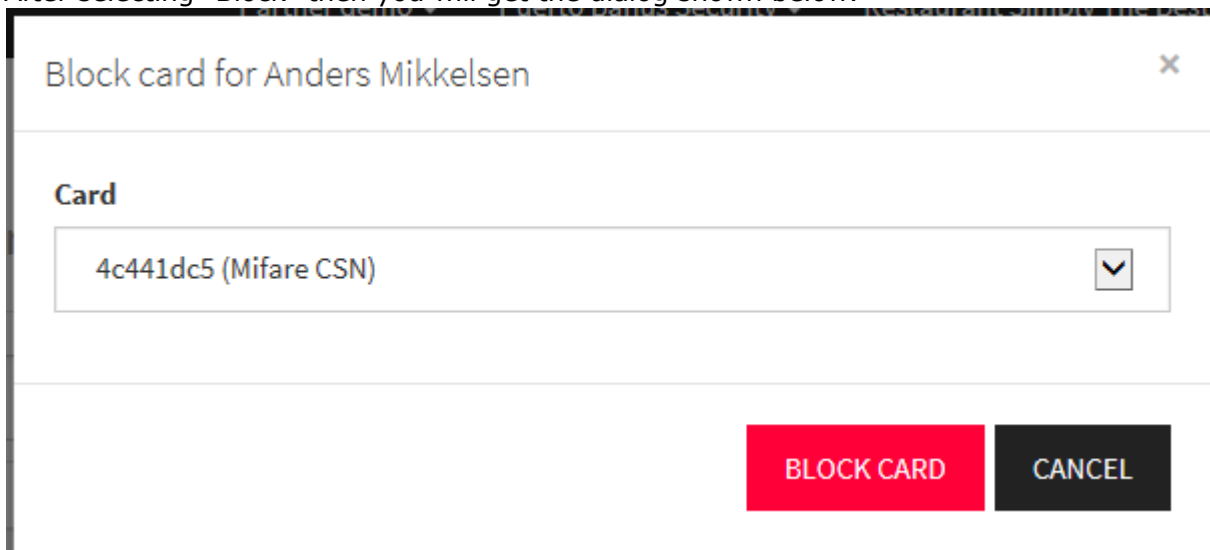
Select **Card** you want to delete.

Block

Select CARD and "Block" if you want to block the card belonging to the selected person. If you block the card then it is no longer valid to use the card and the cardholder cannot be granted access using the card. You normally block a card if the cardholder has lost the card but you still want to keep the card in the system. A blocked card can be unblocked again using CARD and "Unblock"

Before issuing a new card you will have to either block or remove existing card because a cardholder can only have one active card.

After selecting "Block" then you will get the dialog shown below.



Block card for Anders Mikkelsen

Card

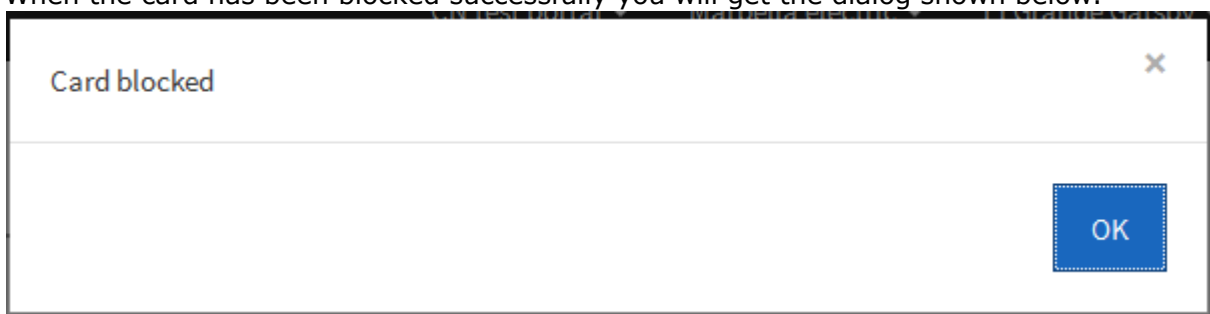
4c441dc5 (Mifare CSN)

BLOCK CARD CANCEL

Card:

Select **Card** you want to block.

When the card has been blocked successfully you will get the dialog shown below.



Card blocked

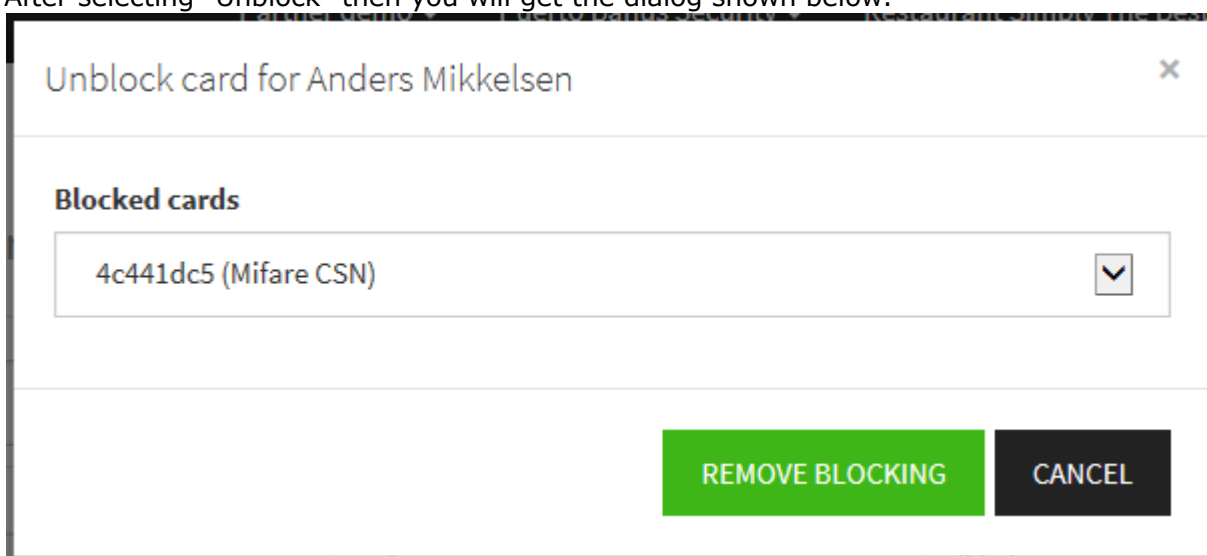
OK

Unblock

Select CARD and "Unblock" if you want to unblock (remove blocking) the card belonging to the selected person. If you unblock the card then it is again possible to use the card and the cardholder can be granted access using the card. You normally unblock a card if the cardholder has lost the card but found it again.

Before issuing a new card you will have to either block or remove existing card because a cardholder can only have one active card. You cannot unblock a card if the cardholder already has an active card.

After selecting "Unblock" then you will get the dialog shown below.



Unblock card for Anders Mikkelsen

Blocked cards

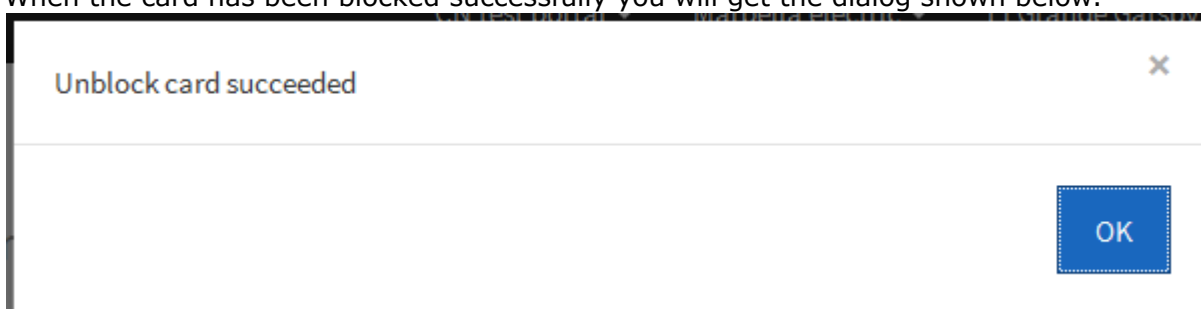
4c441dc5 (Mifare CSN)

REMOVE BLOCKING CANCEL

Blocked cards:

Select **Blocked card** you want to unblock.

When the card has been blocked successfully you will get the dialog shown below.



Unblock card succeeded

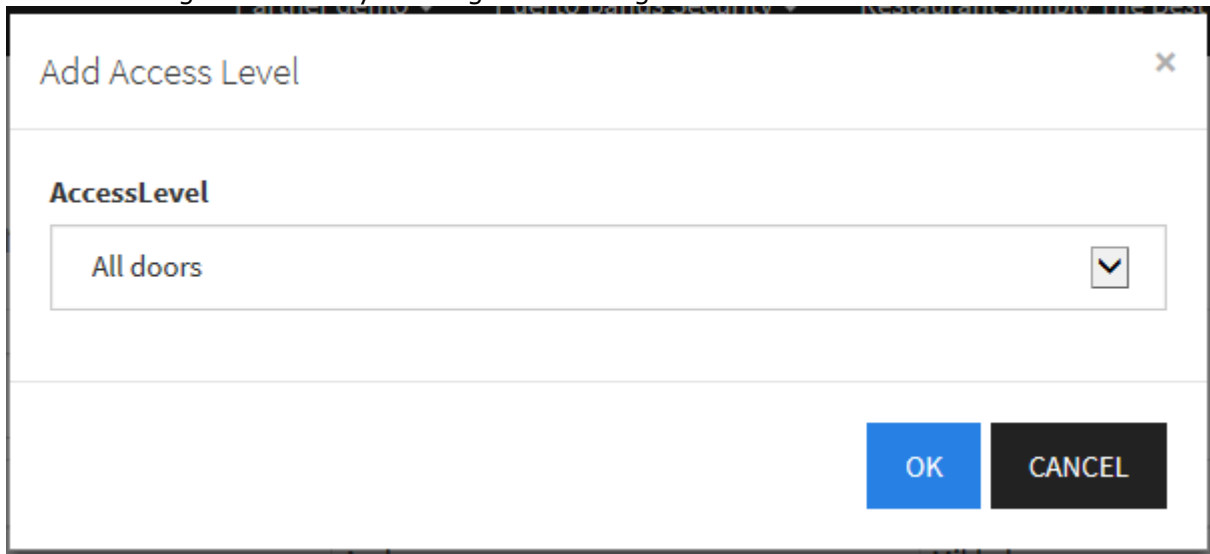
OK

ACCESS LEVEL

Add

Select ACCESS LEVEL and "Add" if you want to add an new access level to the selected person. Each cardholder can have a maximum of 4 Access Levels.

After selecting "Add" then you will get the dialog shown below.

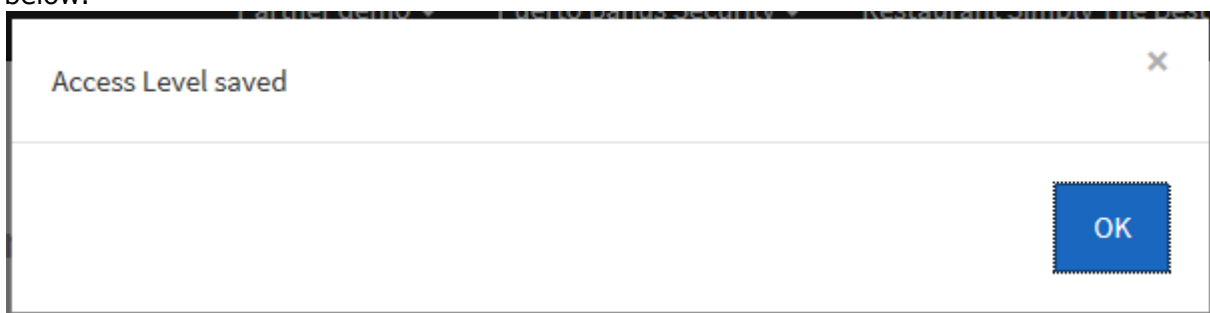


The dialog box is titled "Add Access Level" with a close button (X) in the top right corner. Below the title bar, there is a label "AccessLevel" followed by a dropdown menu. The dropdown menu currently displays "All doors" and has a downward arrow icon on the right. At the bottom right of the dialog, there are two buttons: "OK" (blue) and "CANCEL" (black).

Access Level:

Select **Access Level** used for cardholder. Select the **Access Level** from the different **Access Levels** defined.

When the **Access Level** has been added to the person then you will get the dialog shown below.



The dialog box is titled "Access Level saved" with a close button (X) in the top right corner. At the bottom right of the dialog, there is a single button: "OK" (blue).

Remove

Select ACCESS LEVEL and "Remove" if you want to remove an access level from the selected person. Each cardholder can have a maximum of 4 Access Levels.

After selecting "Remove" then you will get the dialog shown below.

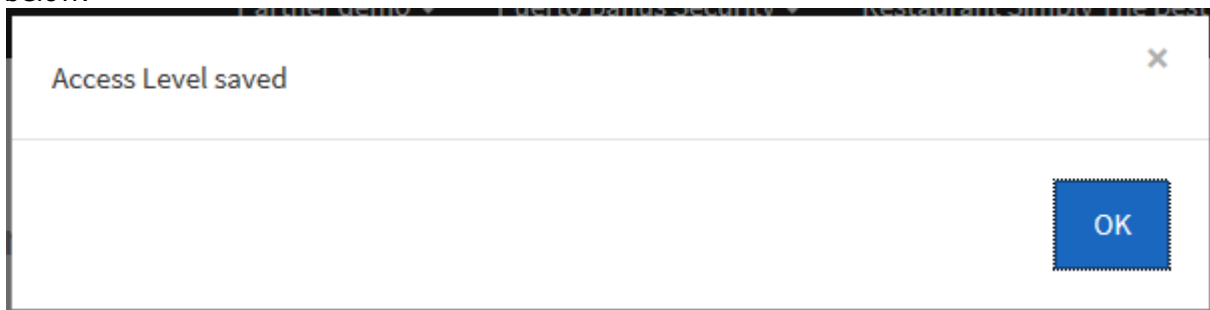


The dialog box is titled "Remove Access Level" and has a close button (X) in the top right corner. Below the title bar, there is a label "AccessLevel" followed by a dropdown menu. The dropdown menu currently displays "All doors" and has a downward arrow icon on the right. At the bottom right of the dialog, there are two buttons: a red "OK" button and a black "CANCEL" button.

Access Level:

Select **Access Level** used for cardholder. Select the **Access Level** from the different **Access Levels** defined.

When the **Access Level** has been removed from the person then you will get the dialog shown below.



The dialog box is titled "Access Level saved" and has a close button (X) in the top right corner. Below the title bar, there is a large empty space. At the bottom right of the dialog, there is a blue "OK" button.

MANUAL OPERATION

Door

DOOR search

				DOOR CONTROLLER ▾		ACCESS ▾	
	Name	IP address	MAC address	Intrusion status	Door status	Door lock	Online
<input type="checkbox"/>	Personnel entrance	10.8.0.50	00:0D:AD:01:CB:E2	Disarmed	Closed	Locked	Yes

The door view shows a list of all doors installed at the customer.

Door name:

Door name.

IP address:

Internal IP address of door controller.

MAC address:

MAC address of door controller.

Intrusion status:

Armed: Intrusion system is armed

Disarmed: Intrusion system is disarmed

Door status:

Open: Door is currently open

Closed: Door is currently closed

Door lock:

Locked: Door is locked

Unlocked: Door is unlocked

Online:

Yes: Door controller is connected to the cloud and operating without errors

No: Door controller is currently not operating in the cloud. Check if Door controller is powered off or there are network problems.

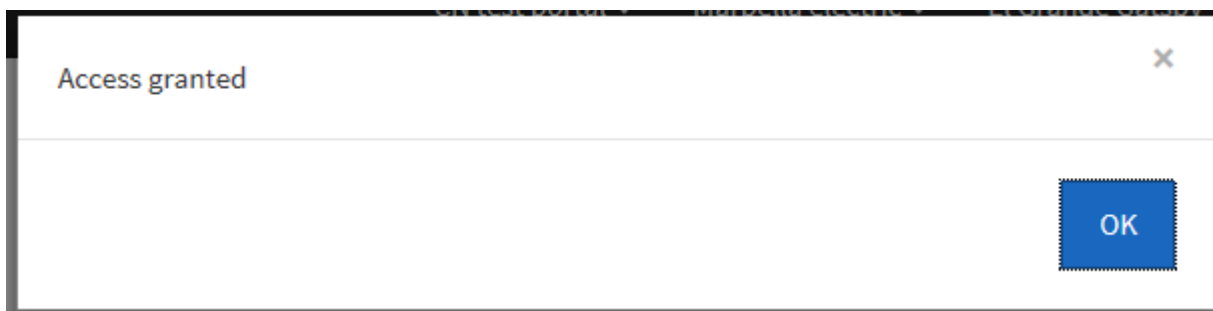
ACCESS

First select the door you want to operate on by setting a check mark in front of the door line,

Grant Access

Select ACCESS and "Grant access" if you want to grant access to a person standing outside the door without any card. The door is then unlocked for 5, 10 or 15 seconds depending on the Unlock time specified in the Door configuration so that the person is able to enter into the building.

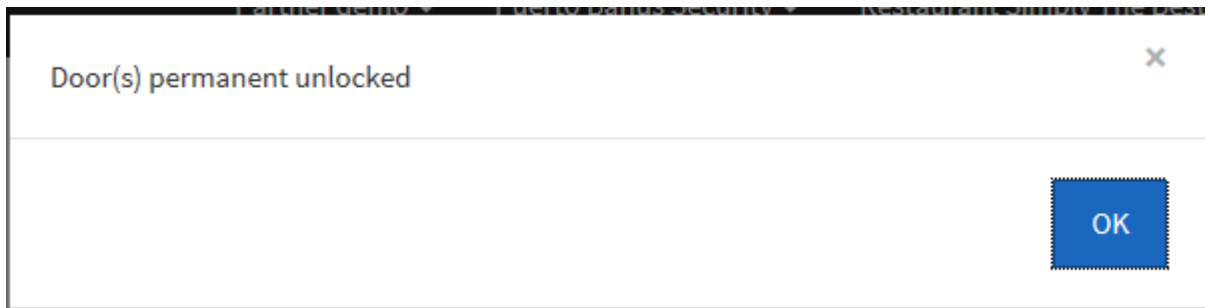
When access is granted successfully you will get the dialog shown below.



Unlock permanent

Select ACCESS and "Unlock permanent" if you want to have access without using a card. The door will then be unlocked and all people can afterwards access the building through the door without using a card. The door will remain unlocked until a "Lock permanent" command is performed by an user in the GUI or a Door "Unlock Schedule" reaches End Time.

When door is permanent unlocked you will get the dialog shown below.

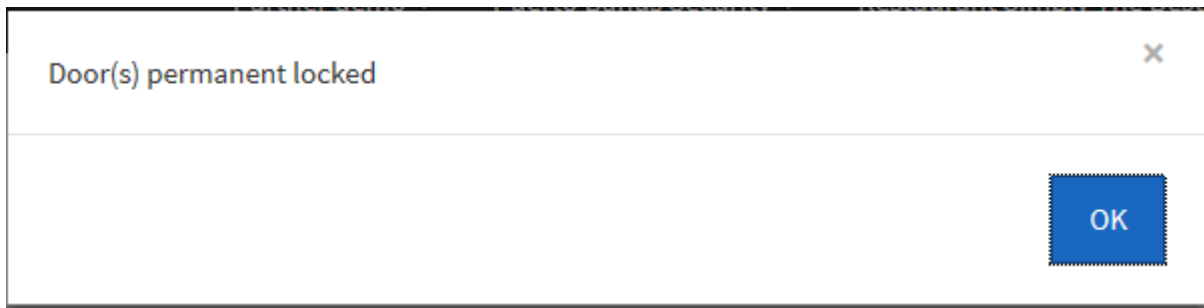


Lock permanent

Select ACCESS and "Lock permanent" if you don't want to have access without using a card. The door will then be locked and all people can afterwards only access the building through the door using a card.

The door will remain locked until a "Unlock permanent" command is performed by an user in the GUI or a Door "Unlock Schedule" begins Start Time.

When door is permanent locked you will get the dialog shown below.



Intrusion

INTRUSION search

		Q	INTRUSION ▾
	Name		Alarm
<input type="checkbox"/>	Personnel entrance		Off

The door view shows a list of all doors installed at the customer which has intrusion enabled.

Door name:

Door name.

Intrusion status:

Armed: Intrusion system is armed

Disarmed: Intrusion system is disarmed

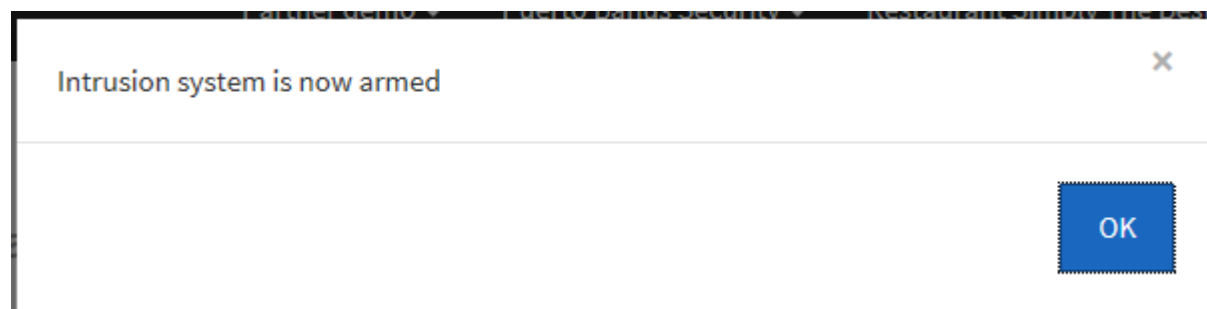
INTRUSION

First select the door you want to operate on by setting a check mark in front of the door line,

Arm

Select INTRUSION and "Arm" if you want to arm the intrusion system.

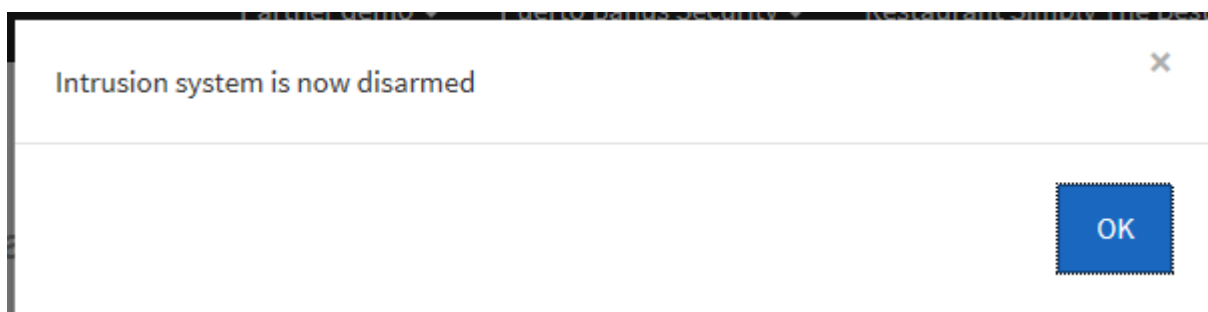
When the intrusion system is armed successfully you will get the dialog shown below.



Disarm

Select INTRUSION and "Disarm" if you want to disarm the intrusion system.

When the intrusion system is disarmed successfully you will get the dialog shown below.



PROFILE

User

An User is the person who does the daily operation of the iVitos solution (add/edit/delete cardholder, add/delete card etc) at the customer site. The User is an employee by the Customer.

USER edit

Firstname	<input type="text"/>
Lastname	<input type="text"/>
Email	<input type="text"/>
Mobile	<input type="text"/>
Superuser	<input type="checkbox"/>
Username	<input type="text"/>
Password	<input type="text"/>
Repeat password	<input type="text"/>

CANCEL
SAVE

First name:

Enter **First name** of person.

Last name:

Enter **Last name** of person.

Email:

Enter **Email** of person.

Phone:

Enter **Phone** of person.

Superuser:

Select if this person is able to add other Users to the Customer.
If marked then person can add other Users.

Username:

Enter **Username** for User. Please notice that the **Username** shall be unique within the portal. You can therefore not input an **Username** already used by another person. When logging into the cloud afterwards you use the format "portal\username".

Password:

Enter **Password** for User.

Repeat password:

Repeat **Password** entered.

LOG

Eventlog

The Eventlog shows all events in realtime which has occurred at the door controller.

EVENTLOG search

<input type="text"/>							
	Timestamp	Server time	Event type	Door name	Firstname	Lastname	Door controller name
<input type="checkbox"/>	25/01-2016 16:54	25/01-2016 16:54	Provide access	Personnel entrance			ivitos000da001cbe2
<input type="checkbox"/>	25/01-2016 16:48	25/01-2016 16:48	AccessPointStateNormalEvent	Personnel entrance			ivitos000da001cbe2
<input type="checkbox"/>	25/01-2016 16:47	25/01-2016 16:47	AccessPointStateNormalUnlockedEvent	Personnel entrance			ivitos000da001cbe2

1-3 of 3

Timestamp:

The **Timestamp** field is the date/time when the event occurred in the physical door controller.

Server time:

The **Server time** field is the date/time when the event was logged in the cloud server. Normally **Timestamp** and **Server time** shall be the same time unless there are network communication problems.

Event type:

The **Event type** field is a textual description of the event occurred.

Door name:

The **Door name** field is the name of the door.

Firstname:

The **Firstname** field is the first name of the cardholder - if event is a card read event.

Lastname:

The **Lastname** field is the last name of the cardholder - if event is a card read event.

Door controller name:

The **Door controller name** field is normally the name/hostname of the door controller.

FAQ