

V364 System Administrator Manual

F9000 System

Version 010

November 11 2016

ISEO[®]

Notice

This documentation contained in this manual is subject to change without notice and does not represent any commitment on the part of ISEO Serrature SpA. ISEO Serrature SpA assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

This document refers to the V364 software version 1.0.x.x

Note

The Software version is defined as follows:

Major. Minor. Maintenance. Build

(example version: 1.0.x.x)

where:

Major : used for major changes in the software and mainly impacting the Graphical User Interface

Minor: used for feature enhancements

Maintenance: only for bug fix

Build: during development it increases until all the test are OK then the current build is released

Index

Index	3
What is V364?	6
Web based Access Control System in a Box	6
Managed with mobile V364 App and Browsers	6
Securing perimetrical and internal doors of your facility	6
Supporting Contactless RFID credentials and F9000 Mechatronic keys	6
Featuring Traditional and Role-Based Access Control	6
Expandable and easy to integrate into a Building Management System	7
Introduction	8
Browser Requirements	8
V364 System Overview	9
The Iseo Data On Credential	9
The System in a Box	10
V364 Features	11
V364 F9000 System Architecture	12
Atlas Controller Lifecycle	14
Login to V364	17
V364 Main Page	18
V364 System Date Time	19
Log out	19
Automatic Web Session Log out	19
V364 Functions summary	20
Quick Start	21
Introduction	21
Create your first Access User and assign a Credential	21
Credentials	26
The F9000 Mechatronic key	26
The User Key	26
The Programming Key	27
F9000 Key Light Signals	27
Replacing Batteries in Key	28
Cylinder lubrication	28
Product compliance	29
USE INSTRUCTIONS	29
Managing key Assignments	29

Reading and writing a credential	30
Roles	32
Traditional and Role-Based Access Control	32
Access Users and Roles	32
Administrators vs. Users and related roles	32
Browsing the Roles List	32
Creating a New Role	34
Editing an existing Role	36
Duplicating a Role	37
Searching for a Role	39
Deleting a Role	39
Time Schedules	40
Time Schedules	40
Browsing the Time Schedules List	40
Creating a New Time schedule	41
Editing an existing Time Schedule	42
Duplicating an existing Time Schedule	42
Deleting a Time Schedule	43
Door Zones	44
Browsing the Door Zones List	45
Creating a Door Zone	46
Editing an existing Door Zone	46
Deleting a Door Zone	47
Creating a Role using Door Zones	47
Access Users	49
Browsing the Access User List	49
Create a new Access User and assign a Credential	50
Credential Assignment Process summary	55
View Access User Details	56
Managing Access Users and the Credential Lifecycle	59
The Credential Lifecycle	62
Read a Credential	77
Searching for an Access User	78
Export User List in .CSV file	79
Import Access User data	81
Credential Receipt	83
Print a Credential Receipt	85
System Administrators	87
System Administrator Roles	87

System Administrators vs. Access Users	88
Browsing the System Administrators List	88
Creating a new Administrator	89
Managing Administrators	90
Deleting Administrators	90
Searching for an Administrator	90
Events	92
Door Events	92
System Administrators Transactions	95
Utilities	96
Download Backup	96
System Preferences	96
System Information	97
V364 Smartphone App	98
Using the V364 App	98

What is V364?

V364 from Iseo is an easy-to-use web-based access control system. Its plug and play design means it does not require software installation or a dedicated PC. Any computer running a WebKit enabled browser (Apple Safari , Google Chrome , Microsoft Edge) can be used to manage the system.

Web based Access Control System in a Box

The core of the system V364 is the Atlas (Master) controller embedding a web server. There is no need to install any software or to buy a dedicated server computer: it's all in the Atlas Box which comes as solid state pre-configured appliance allowing the system up and running in minutes.

V364 is secure due to Linux operating system assuring stability and greater security from external threats or virus attacks. V364 provides system administrator login access levels allowing control of what each person is authorized to manage or view.

Managed with mobile V364 App and Browsers

The V364 web server gives you the freedom to manage and control your facility's points of entry from anywhere and anytime without being tied to a dedicated client workstation. V364 features a user friendly interface to manage your electronic access control system: configuration and changes such as assign or modify access rights, add users, door groups or retrieve reports can be made from any mobile device or desktop computer with browser.

Securing perimetrical and internal doors of your facility

V364 secures perimetrical online readers and internal doors equipped with offline, easy to install, battery-powered devices. Access rights are updated with the online validators or with the mobile validators for the mobile workforce. The online validators, while opening the main facility door, automatically alter the user access rights data on the electronic key. Audit trails will be downloaded from the offline locks while opening the internal doors and then uploaded into the Atlas at validation.

The Atlas web server controller combined with the offline electronic locks Aries, the electronic cylinder Libra and the mechatronic cylinder F9000 delivers a cost-effective access control solution ideal for small to medium sized facilities.

Supporting Contactless RFID credentials and F9000 Mechatronic keys

V364 supports secure Mifare DesFire and Mifare Classic RFID technology with a customizable credential layout to easily accommodate into legacy credentials.

The F9000 mechatronic key are suitable for explosion danger environments as they comply with the ATEX directive and can be mixed with the F9 mechanical Master Key System providing the highest level of security only on selected doors. The F9000 key powers directly the F9000 cylinder allowing installation in whatever your environment is.

Featuring Traditional and Role-Based Access Control

In traditional access control, the access authorizations are directly assigned to the access user. With Role-Based Access Control, permissions are based on the roles that individual

users have as a part of an organization. Roles are closely related to the concept of user groups, simplifying complex access control policies and converging physical access control with logical IT security.

Expandable and easy to integrate into a Building Management System

V364 is designed to easily scale with your need and your budget. As your business grows, V364 will grow with you. You can add doors, Atlas (Slave) controllers for multi-site applications and users to the system at any time.

V364 Connects multiple facilities that reside on the same existing networking infrastructure and will be the core of the your next level of facility integration accordingly to the ISEO Technology Partner program VAR (Value Adder Reseller).

Introduction

This document is designed as a user manual for the V364 system working in combination with the F9000 mechatronic keys and cylinders.

It provides a step-by-step instructions for:

- Setting up Access Users, Roles (doors and Access Users groups) , Time Schedules
- Assigning and revoking access permissions to Access Users
- Setting up login permissions
- Reading events from doors

Browser Requirements

The Atlas controller uses network port 80 to communicate to the user's computer.

In order for the system to work properly, port 80 cannot be blocked by any firewall software.

V364 is currently supported on the web kit enabled browsers and the most common are the following browsers: Microsoft Edge, Safari, Google Chrome.

Javascript must be enabled in the browser. If your browser has scripting disabled, the V364 interface will not function.

V364 uses cookies to preserve session information. If your browser disallows cookies, the V364 interface will not function.

Browse in private with incognito mode is not supported.

Minimum screen resolution is 1024 x 768.

Maximum screen resolution is 1600 x 1200.

Recommended screen aspect ratio 4:3.

V364 System Overview

The vast majority of the available commercial physical access control systems, are connected to a central computer system by wires. The system is normally managed by a Server Computer to which several clients connects and from where all the administration can be done.

This online client server architecture poses two main challenges:

1. Installation cost of wiring all the doors
2. Installation and maintenance cost of the client server computerized system based on Personal Computers

V364 brings an innovative solution to this two challenges:

The Iseo Data On Credential

Due to the installation cost, online or hardwired systems are significantly more expensive per door and most organizations can only afford to manage a small subset of their doors electronically, relying on door locks utilizing common mechanical keys entry for the rest.

The Iseo Data On Credential technology allows for the integration of offline electronic locks into the online access control system allowing more doors to be controlled for the available budget.

Data On Credential enabled mechatronic F9000 cylinders are battery operated and no electrical knowledge is required for installation.

System installation is much simpler than fully 'wired' alternatives, reducing installation costs and time.

The user access rights are held securely on the F9000 mechatronic key credential, and the F9000 cylinder verifies the access credential against its current status.

The access rights are updated and reloaded on the user's credential every time he or she accesses an online reader, such as a main facility door.

The online readers are used to automatically alter the user access rights data on the credential allowing cards to be deleted, re-programmed and/or "validated" for a limited time.

Audit trails can also be downloaded from the locks and credentials to provide information on who was where and when.

As the system is essentially stand alone, security is still maintained and locks can still operate even in the event of a network failure.

The Iseo Data On credential brings together the offline world of electronic locking with the traditional hard-wired online world

Data On Credential Technology

The technological driver of the Data On Credential solution are the F9000 mechatronic keys, smart credentials with read write capabilities whereby the F9000 key become the link back to the online environment through the strategically placed on line devices "Validators". The F9000 mechatronic keys:

- transport access rights from online to offline devices
- transport transactions from offline to online devices
- are refreshed at online devices to maintain higher security

Therefore:

- Access Rights are stored on the F9000 mechatronic key
- Audit Trails are stored on the F9000 mechatronic key

Advantages

The Data On Credential system:

- Reduces installation times and costs
- Collects audit trails from credentials at on-line readers automatically
- The ability to make changes to a user's access profile "on the fly" without having to individually update the standalone locks
- Key Revalidation times limit the amount of risk of exposure with lost user credentials on offline locks and blacklisting further compliments this
- Avoids the need to visit the lock to delete lost cards by forcing smart card validation
- Battery information being brought back to the system
- Replaces the need for mechanical keys systems: A lost key never becomes a financial burden/major financial cost again....
- Equip areas that were never possible before or deemed too expensive to consider (gates, staff lockers, server racks etc.)

The System in a Box

V364 is a web-based access control system that gives you the freedom to access, manage and control your facility's points of entry from anywhere with a Browser and in mobility.

The core of V364 is the Atlas controller embedding a web server.

The Atlas Master is a "system in a box" controller with embedded web server (pre-configured appliance) which provides a fully functional access control server solution in a fraction of the time of conventional software. With no software to install setup is quick and simple. Just connect the Atlas controllers and the system components then open a web browser to launch the intuitive interface which guides you through the process of configuring and managing your system.

V364 combines robustness with simplicity.

The web-based access controller V364 combined with the offline electronic cylinder F9000 delivers a cost-effective solution ideal for small to medium sized facilities.

V364 features a user friendly interface to manage your electronic access control system: changes such as assign or modify access rights, add users, door groups or retrieve reports can be made from any mobile device or desktop computer without the need to install any software or to buy a dedicated computer: it's all in the V364 Box.

V364 therefore is a cost competitive solution for your electronic Access Control and is by design easy to use and easy to install and set up.

V364 is secure due to Linux operating system assuring stability and greater security from external threats. V364 provides Administrator log-on access levels allowing control of what each person is authorized to manage or view.

As your business grows, V364 will grow with you. You can add doors, controllers and users to the system at any time.

V364 Connects multiple facilities that reside on the same LAN and will be the core of your next level of facility integration accordingly to the ISEO Value Adder Reseller program (VAR program).

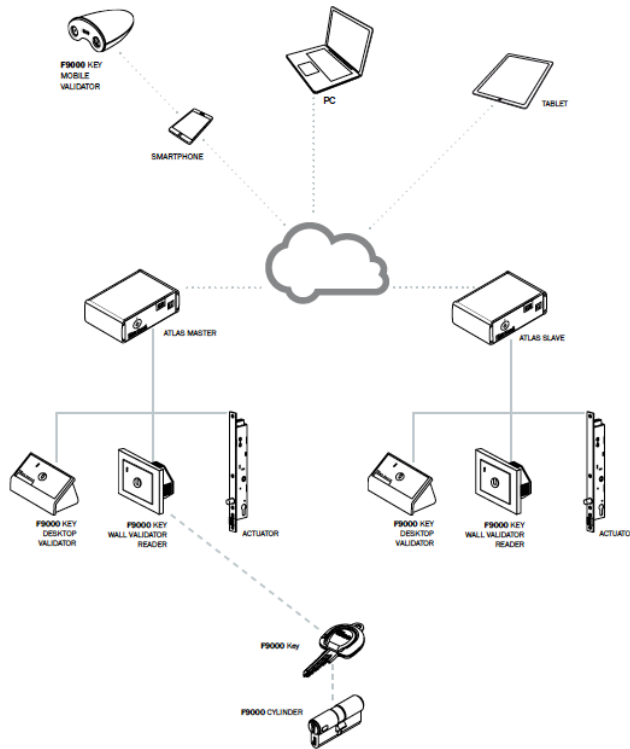
V364 Features

- Built-in web server platform into solid state Atlas master controller
- Managed with V364 mobile application (FOR iOS and Android) and across multiple operating systems supporting “WebKit” powered browsers (GOOGLE Chrome, Safari, MICROSOFT Edge)
- USER-FRIENDLY interface:
 - Modern look and feel
 - Minimal training required to operate the system (highly USER-FRIENDLY)
 - System configuration easy for installers as the Atlas is preconfigured and IP network ready
 - VERY Simple functions TO SET access RIGHTS
- Multiple configurations supporting several memories partition
- Highly scalable architecture supporting Single or Multi-site installations
- Multiple administrators concurrent login sessions
- Multi-language support by individual system administrator login
- System administrators segmentation allowing specific permissions based on the operator role
- Role-Based Access Control
- RFID Mifare Desfire and Mifare Classic credential support with configurable data layouts
- F9000 Mechatronic keys ATEX directive compliant
- Online and offline lock support allowing:
 - Remote disabling of credentials (with validation or void list)
 - Remote collection of audit trails and battery status
- Devices software upgrade ON the field
- Integration into Building Management Systems via web services with SOAP (Simple Object Access Protocol) over HTTP technology.

V364 F9000 System Architecture

The V364 Architecture is based on an IP Network of Atlas Controllers with:

- One Atlas Master Controller
- Several Atlas Slave Controllers



Master/Slave is a model of communication where one device has unidirectional control over one or more other devices. The Master database is regarded as the authoritative source, and the Slave databases are synchronized to it.

In case of IP network failure the slave can continue to work with the last information received from the master.

Each Atlas controller has an IP network address and therefore there is no limit on the number of Slave controllers.

The Atlas becomes Master as a license file configuration file is loaded on it.

Each Atlas controller might have connected devices such as readers and actuators connected to the Atlas I/O channels.

In this way the Atlas controller can and deliver online doors.

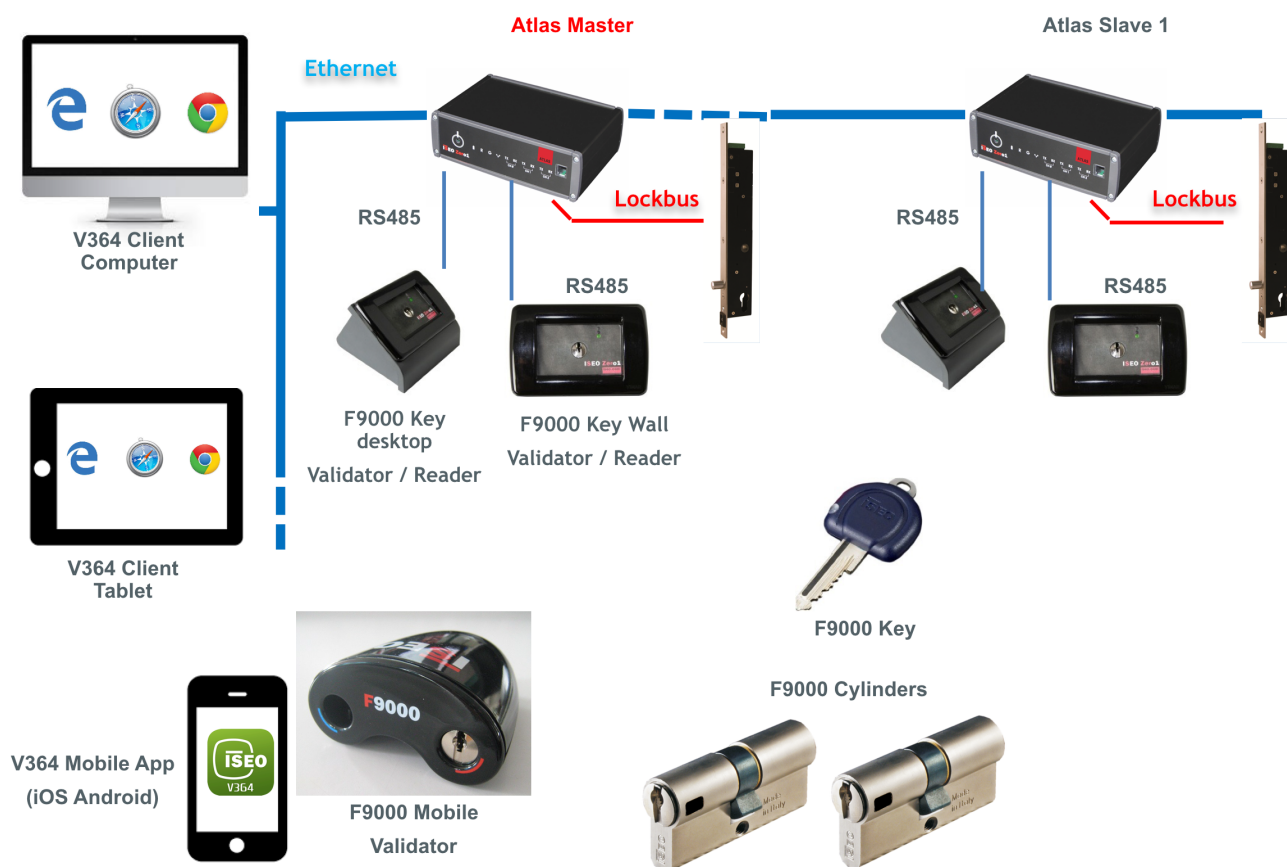
The Atlas controller will have the option to configure the I/O channels for 2 type of field bus:

- LockBus (3 wire bus: Power GND and Data)
- RS485

The standard Atlas has 3 I/O channels configured by default as:

- Channel 0: LockBus
- Channel 1: 485
- Channel 2: 485

The Atlas controllers are “Black Boxes” and do not have Graphic User Interface (GUI) built in devices options, however they provide an embedded Web Server therefore Clients can log to the system with Browsers.



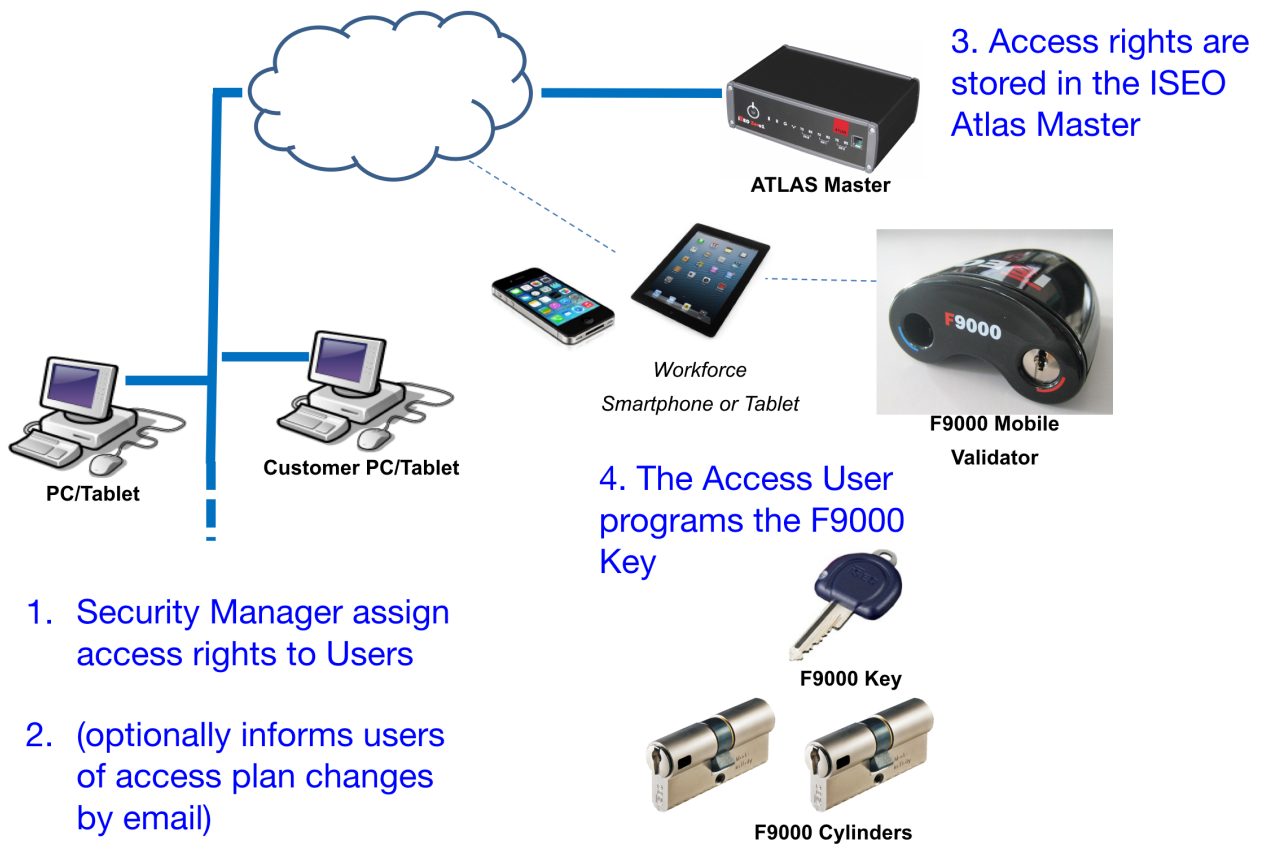
V364 Clients

Clients provide the GUI to the Iseo Access Control Platform.

In every client (either computer either tablet) there must be installed a webkit enabled browser that will connect the V364 Master Atlas controller to manage the access control system.

V364 Smartphone App

A V364 App for smartphone is available for Android and iOS. The V364 app is able to manage the F9000 mobile validator in order to validate the F9000 key typically for a mobile work force. This operation allows to provide access authorization to remote unmanned sites to a Mobile Workforce of technicians always on the move connected to the office with smartphones



Atlas Controller Lifecycle

The Atlas Controller reaches its operational status managing the access control system in a real installation through a set of configuration steps.

Warehouse

The Atlas is mechanically assembled and tested and is stored in the factory warehouse identified by its Serial Number, with the V364 software loaded.

License File Production

A production order is entered for a specific customer, which includes a license file item defining the number of Active Users allowed in the system.

The license is associated to the Atlas Master MAC Address (serial number) and therefore is unique for each Atlas for security purposes and can be loaded only to the selected Atlas.

The license defines the capabilities of the Atlas Master, (in other words of the system) and it also contain the Plant code and the Type of credentials supported (RFID or F9000)

License File Load

The Atlas Master requires the license. The slave will get the License from the Master during the configuration Phase.

Configuration

After loading the license the Atlas Master enters in configuration mode for door and network configuration which will be performed by Iseo Technical Manager (ISEO Zero1 approved installer).

System Configuration steps

Iseo Technical Manager

- Iseo Technical Manager is created and logged into the system.
- Iseo Technical Manager is entitled to setup the system configuration.

System Configuration

- System date and Time (and Time Zone)
- Credentials supported and credential data layout
- Atlas Master and Slaves network configuration
- Readers and Actuators connected to each ATLAS
- Doors setup
 - Define doors
 - Define schedules for doors
 - Door initialization
- Configure User defined fields for Access Users
- Create System Administrator account

In operation

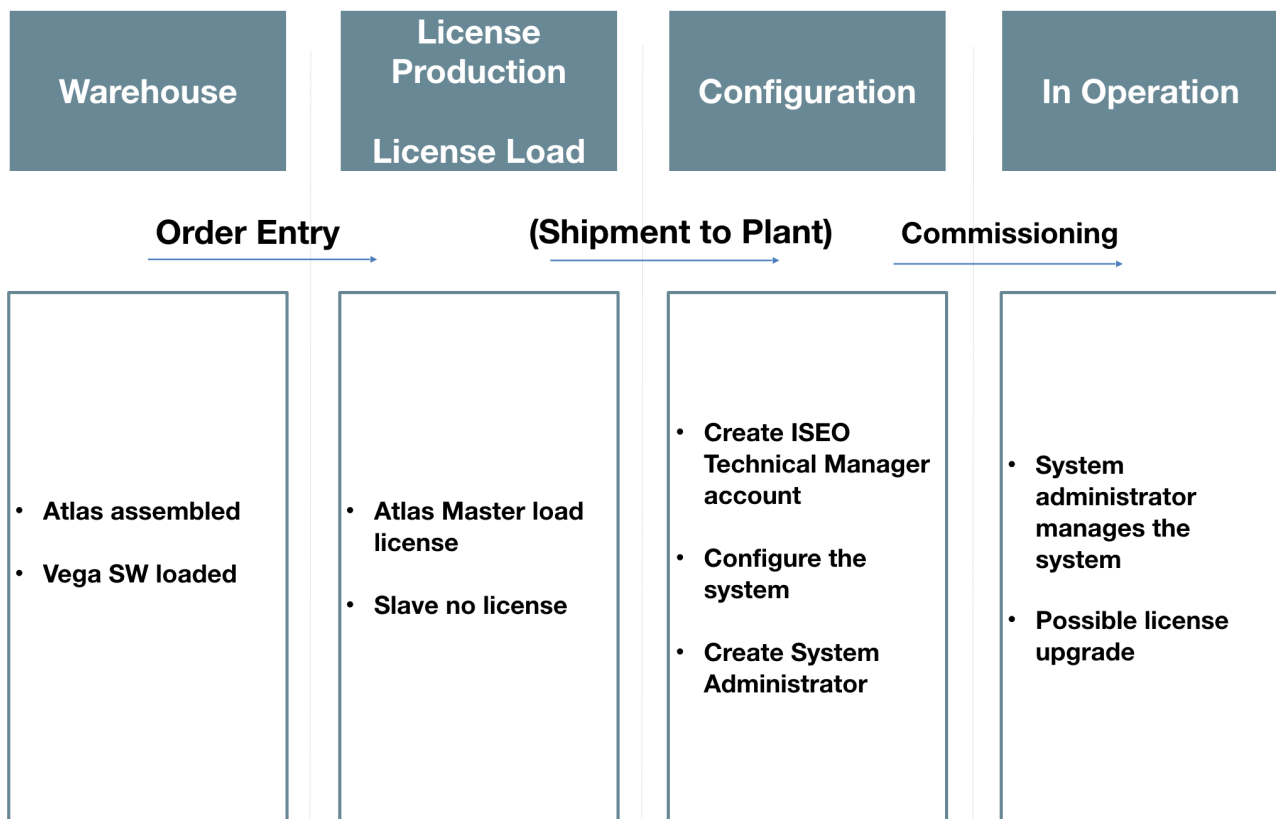
The system is commissioned and put in operation and a Facility System Manager is created (System Administrator).

The System Administrator will create other Administrators which might have different permission on the system based on their roles.

UPGRADE License

It is possible to increase the number of users allowed in the system performing a licence upgrade.

A new license file (License #2) will be generated for the current Atlas Master and loaded performing the license upgrade.



Login to V364

Open the browser and enter the IP address of the V364 controller in the address field. Next, the login will appear. Type in the appropriate System Administrator **login ID** and associated **password** to log into the system.

Note: The Password field is case sensitive.



The login screen for the V364 controller. It features the ISEO logo at the top, followed by the text "V364". Below this are two input fields: "login id" and "password". At the bottom is a "Login" button. The entire login form is centered on a light blue background.

SS CONTROL SYSTEM 0.9.8.9.01 SDK: 2.06.04.02344 Plant Name: GREENAPPLE F8000 V2

If an invalid System Administrator Login ID or Password is entered, the following message will occur:



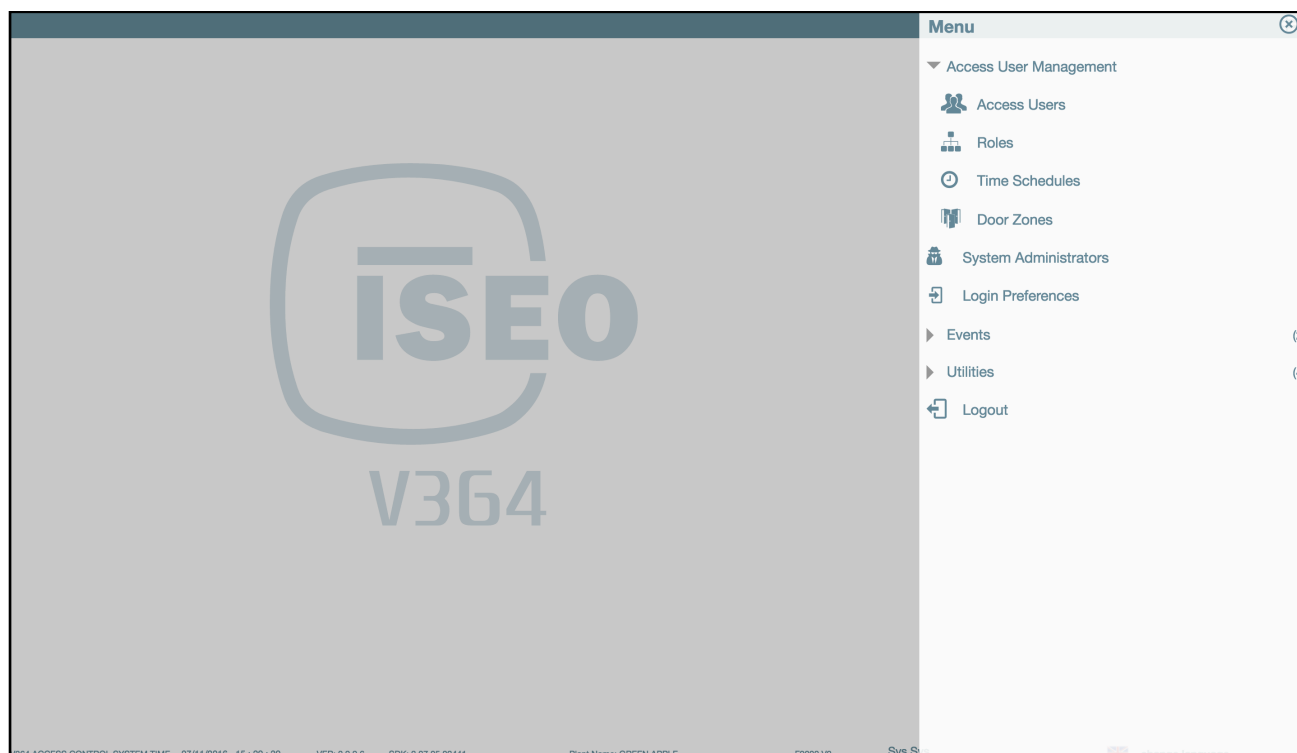
The login screen with an "Authentication Failed" message overlay. The message box says "Authentication Failed" and "Invalid Login ID or password". There is an "OK" button to dismiss the message. The "password" and "Login" fields remain visible below the message box. The background is a solid light gray.

SS CONTROL SYSTEM 0.9.8.9.01 SDK: 2.06.04.02344 Plant Name: GREENAPPLE F8000 V2

Multiple System administrators can login to the V364 system at the same time.
The number of maximum concurrent login sessions is 64 system administrators at same time.

V364 Main Page

Upon login the system administrator will be brought to the V364 Menu options already open:

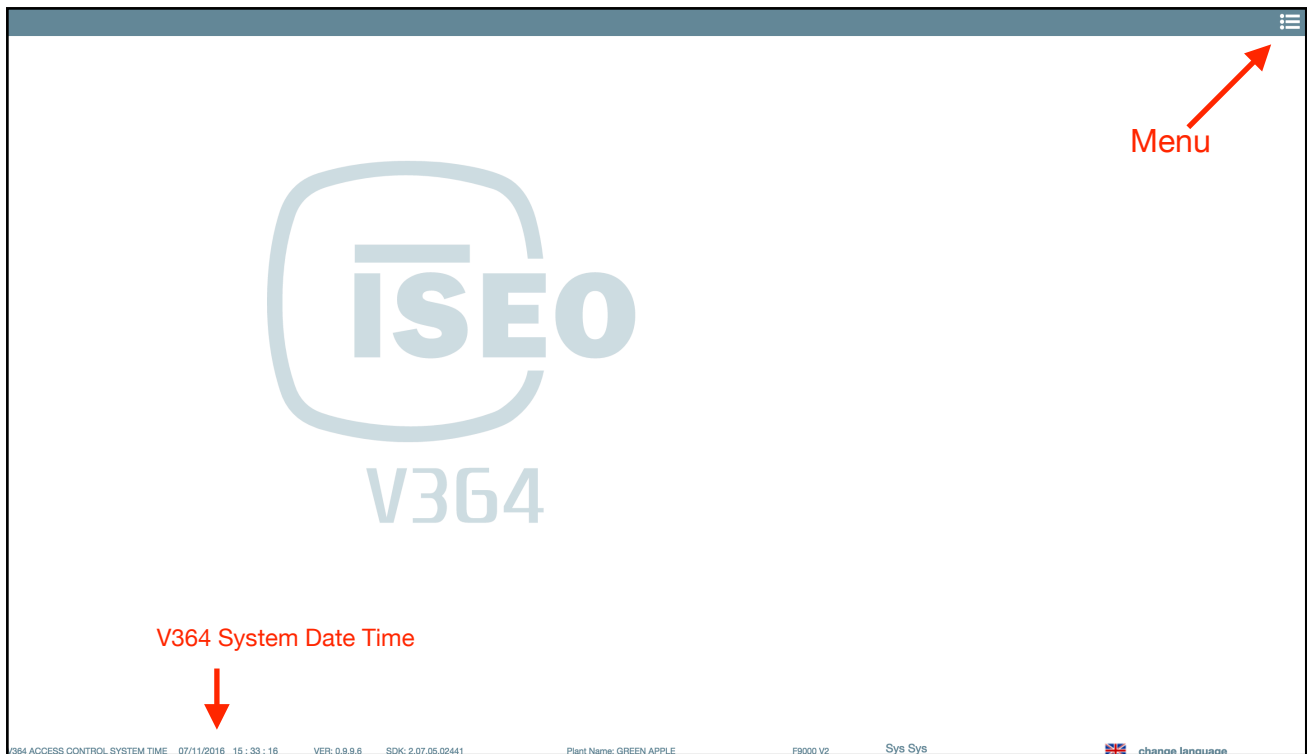


These options are displayed according to the administrator authorizations (the administrator role) in the V364 System.

Each of these tabs is explained at length in its own chapter later in the manual.

V364 provides system administrator login access levels accordingly to the administrator role, allowing control of what each person is authorized to manage or view therefore the tabs showed in the menu button will correspond with the role of the system administrator.

It is always possible to open the option menu by selecting the icon on the top right:



V364 System Date Time

On bottom left it is always shown the V364 system date and time by directly visualizing the Atlas Master clock.

Log out

Log out at anytime by clicking on the Log Out button located in the bottom of the menu screen.

Automatic Web Session Log out

For security purposes, the V364 system will log out the administrator during the web session after a configurable amount of minutes of inactivity (see System Preferences)
After the Log out the administrator needs to login again into the V364 system.

V364 Functions summary

Access User Management • Access Users • Roles • Time Schedules • Door Zones	Add Access Users and assign credentials defining Roles and Time Schedules and Door Zones
System Administrators	Set up system administrators
Login Preferences	Change administrator own password and language
Events • Door Events • System Administrators Transactions	Door Events: view latest events in the doors showing when individual doors were accessed and by whom. System Administrators Transactions: shows all the operation made by the system administrators
Utilities	Backup database, System Information with set Date/Time and time zone, System preferences, Erase Credential
Log Out	Log out from the system.

Quick Start

Introduction

The Quick Start chapter is here to get you up and running with V364. You'll find details on how to quickly create Access Users providing access assignments that will allow you a quick start. Once you've followed the steps in this chapter you'll have an overview of how to provide access to users. After that you'll find more information in the later chapters which describe what V364 can do more in detail.

Create your first Access User and assign a Credential

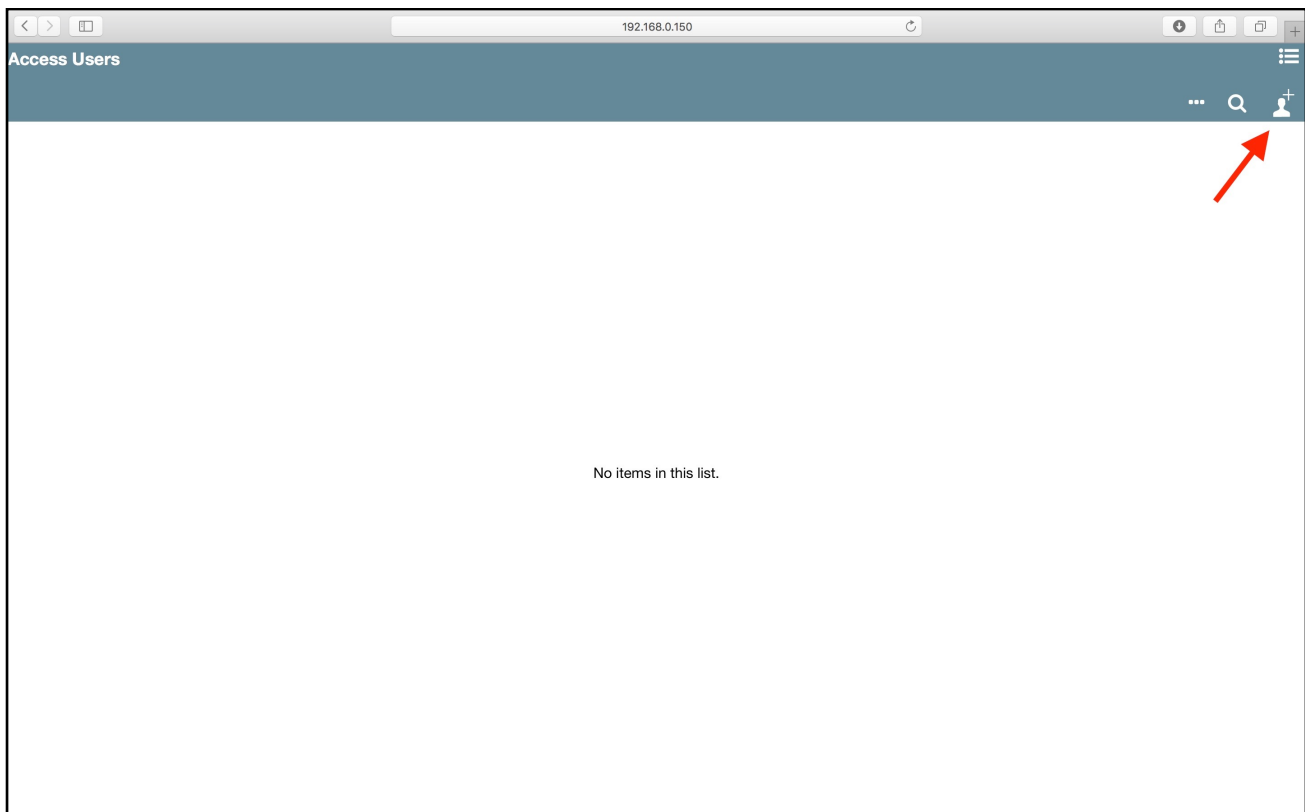
An Access User (or simply a User) is any person who requires access to one or more doors at the facility. An Access User has a unique credential, the F9000 key, that enable entry at the specified doors through the F9000 mechatronic cylinder.

Normally a User has a Role in an organization and also the physical access permissions are associated with the Role the User has in the organization. In other words the User function in the Organization Chart defines also his/her access privileges to the doors he/she is allowed to open.

Assigning to a User a role means assign to the User a group of doors that the user can open. Since several users can have the same Role in the organization, the Role defines a group of people (a set of Access Users) with the same access privileges to a facility. Any modification to the doors associated to a Role will automatically access permission

To create a new user

1. Select the dropdown menu and select Access User Management and then Access Users. The Access Users list displays.



2. Select Add User and the Edit Access User form displays

Access Users

<Back

Last Name

First Name

Role

Select an item from the list

Credential

UID

Personal Information

Access Permissions

Credential Status

Access History

Validity

Activation

08/04/2016

Expiration

08/04/2017

Validation period:

minutes

value

1

Days

366

Assigned Doors

Insert:

User Picture: a .png image file (optional)

Last Name : Access User last Name

First Name: Access User first Name

Role: the Access User role in the organization (the user group to which the Access user is affiliated). Selecting the role from the list you will see the list of the Assigned doors with the role.

Credential UID : the Unique IDentifier of the credential that will be assigned to the Access User which in the F9000 key is marked in this position ("PS1582"):



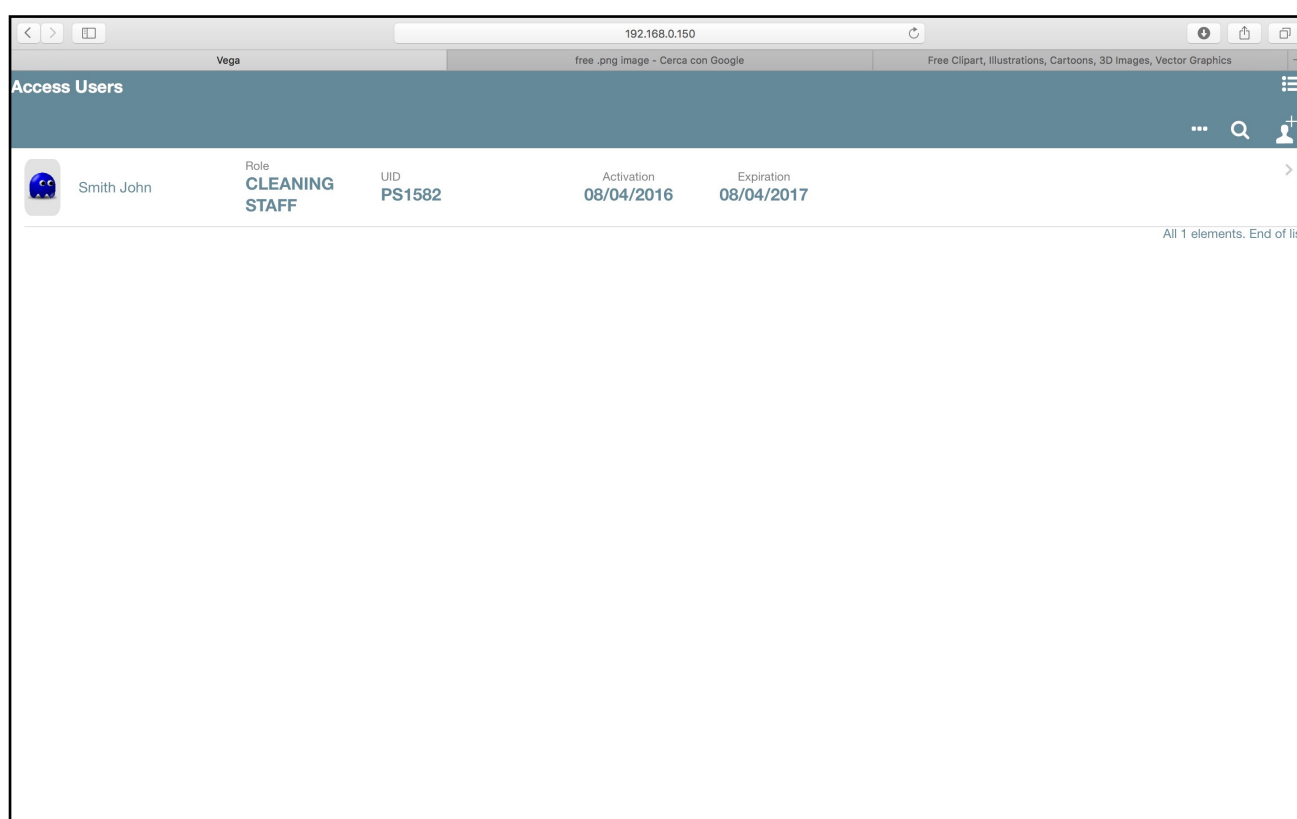
Validity:

Activation Date: set the date that an Access User becomes active. Prior to the activation date, the credential associated to the User will not work. The default is set to the date that the person is added to the system.

Expiration Date: set the date that a Access User will expire. After this date, the associated credential will not work. The default duration is set in the System Preference. By system default is 365 days but it can be modified accordingly the plant requirements.

Validation Period: in minutes, hours or Days (multiple of 24H) the period of time after which the credential validation expires and must be validated again at the online validators.

3. Select Save. The access user List will be displayed with the enrolled Access User.



Now you just have entered the first Access User selecting a Role and enrolling the User with the credential UID (Credential UID enroll process). This is the most efficient way to enroll Access Users into the System and does not require to have a credential reader/writer close to your browser.

After this operation, you can give the F9000 key to the User and ask him/her to insert the F9000 key into any credential Validator. When the Access User will insert the F9000 key into a validator the F9000 key will be written with all the access permission.

Credential immediate write on a credential reader/writer

In addition to the Credential UID enroll process (typing the credential UID), it is possible to write immediately the F9000 key in a credential reader/writer located nearby your browser:

1. Insert the Access User with out typing the Credential UID and select Save.

Access Users

<Back



Anderson
Jerry

✕

✕

Personal Information

Access Permissions

Credential Status

Access History

Role

GM

✕

Credential

 UID

Validity

Activation

06/10/2016

✕

📅

Validation period:

hours

value

10

✕

Expiration

31/12/2016

✕

📅

Days

87

Assigned Doors

Type and Enter

 Gas Refinery Plant
Remote Site Area

🕒

24H
ALWAYS

 General Manager
General Manager

🕒

24H
ALWAYS

 Main Door

🕒

24H
ALWAYS

 Meeting Room
Meeting Room

🕒

24H
ALWAYS

 Operation
Operation

🕒

24H
ALWAYS

 Research & Development
Research and Development

🕒

24H
ALWAYS

6/6 Elements

You will see the Credential Status page:

Access Users

<Back



Anderson
Jerry

✕

✕

Personal Information

Access Permissions

Credential Status

Access History

PENDING



Activation
06/10/2016

Expiration
31/12/2016

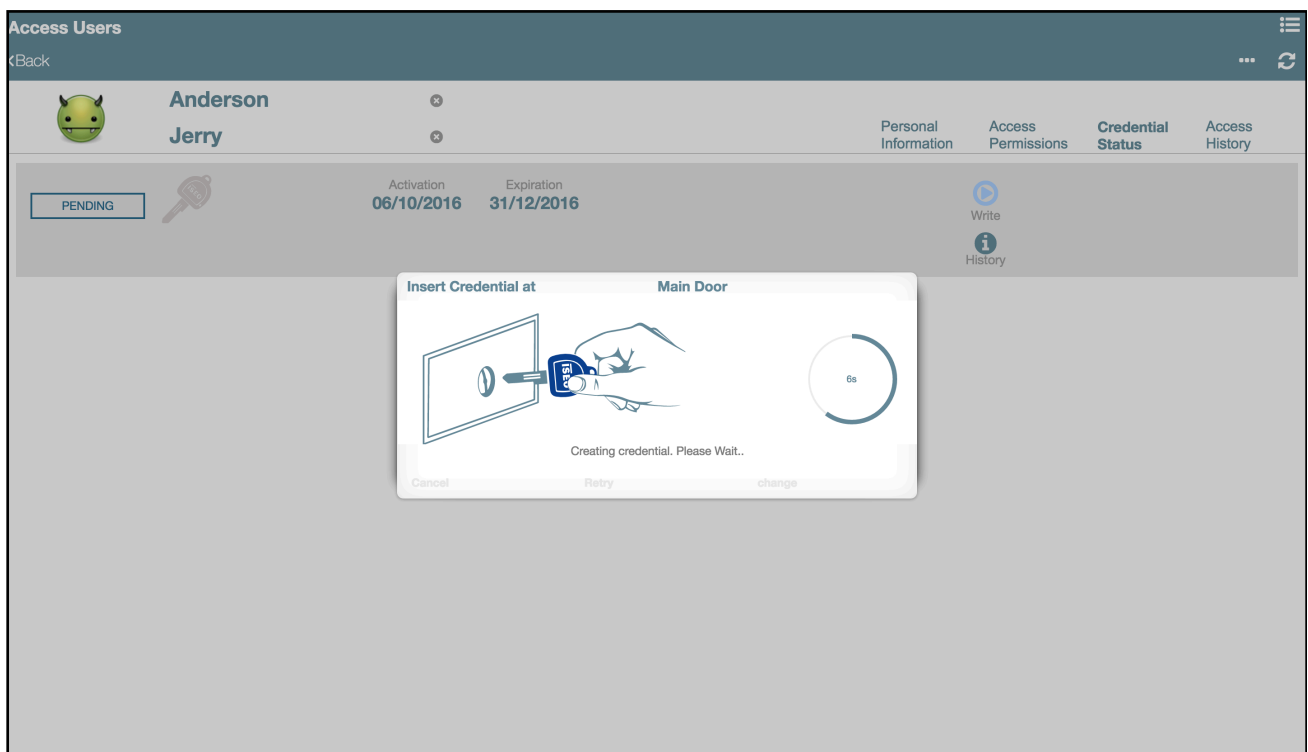
▶

Write

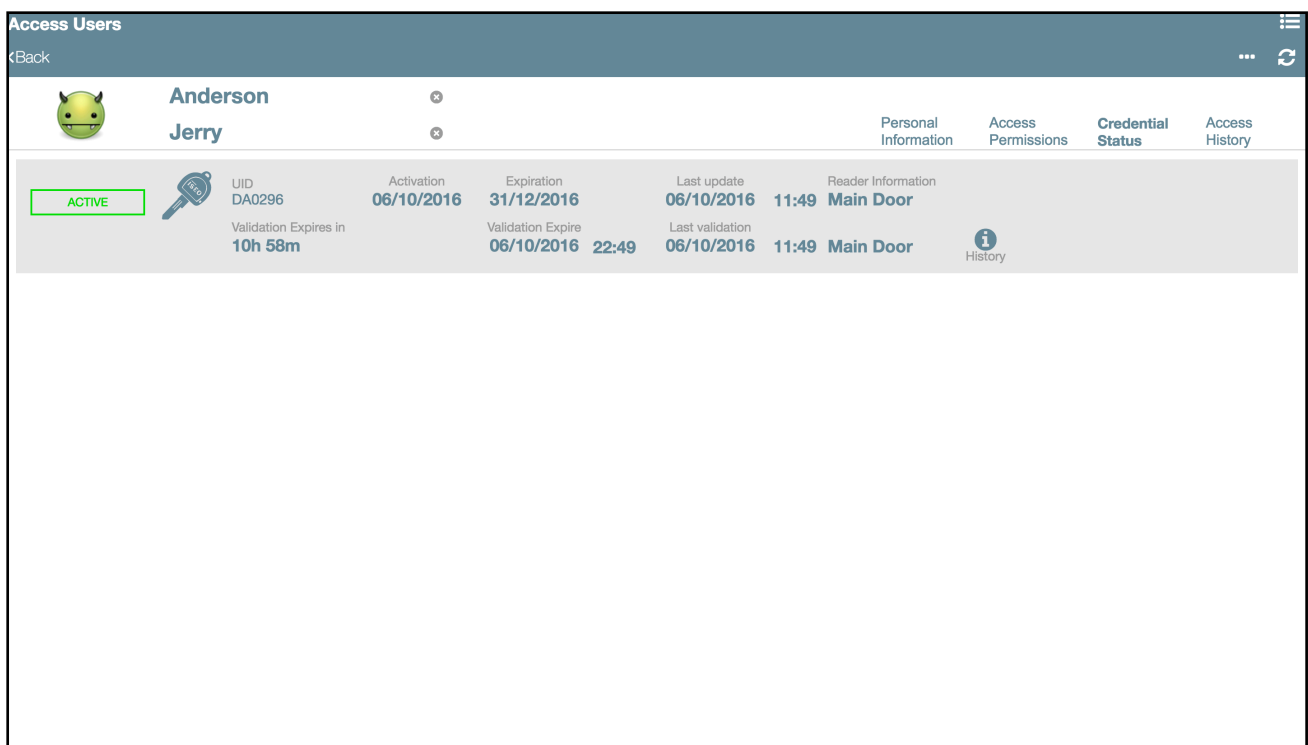
i

History

2. Select the **Write Credential** button a reader dialog box will appear



3. insert the F9000 key inside the reader/writer: the F9000 key will be written and you will see the credential status:



In the next chapters you will learn how to Assign individual doors to the Access Users, create a Role and define Time Schedules.

Credentials

A credential is a physical or logical object used at a reader to prove one's identity. The V364 F9000 system manages F9000 Mechatronic key credentials. Each person in the system can only be assigned one credential at a time. It is not necessary to assign a credential to an access user, but if no credential is assigned to the Access User then the person will not have access to any doors in the system and will be considered an active user if the user list counting as user for the V364 license limit.

A credential can be added to the system by either editing an existing Access User or creating a new Access User record. The credential status information for a person can be displayed by clicking on the Credentials Status tab.

The F9000 Mechatronic key

The F9000 mechatronic key is a physical credential with a form factor of a mechanical key carried by a user to open a F9000 electronic cylinder.

The F9000 cylinder is completely passive; it does not contain any batteries and does not need to be connected to a power supply. Therefore the F9000 cylinder is totally compatible with any mechanical cylinder and can easily upgrade a pure mechanical key system.

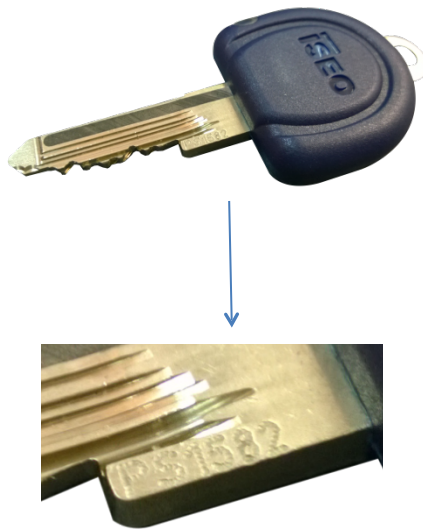


The operating energy is supplied by the key when it is introduced in the cylinder. The electronic cylinder opens when the mechanical code (represented by the pins) and electronic code correspond to the inserted key. Every time the F9000 key (electronic) is inserted, both ENABLED and DISABLED for opening, the cylinder records the date, the time and the key name.

The User Key

The **BLUE** key (user's key) opens the **F9000** electronic cylinder as well any F9 pure mechanical cylinders of the system. It is provided with a mechanical coding but it can also be programmed with an electronic code to ENABLE the openings. Every time a user's key is inserted in an electronic cylinder the key records the date, the time and the cylinder in which it has been inserted. The key hosts the batteries which provide the power supply both to the key itself and to the cylinder. The User key has a built-in clock. The key clock is adjusted at the issuing time and refreshed at any validation.

The User key has a number printed on its surface called the F9000 key UID (Unique Identifier) such as "PS1582".



The Programming Key

The **RED** key (programming key) CANNOT OPEN the cylinder. In fact, it does not have a mechanical coding and it is used to transfer the data to the cylinders. The key hosts the batteries which provide the power supply both to the key itself and to the cylinder. The User key has a built-in clock. The key clock is adjusted at the issuing time.



F9000 Key Light Signals

F9000 keys and cylinders are designed to be installed and used as standard locks, but with the addition of electronic functions. When the keys are inserted in the cylinders a series of light signals indicate the key operating status:

User's key signals when inserted in the cylinder

- **1 green flash:** the key is enabled for opening the cylinder and the battery is charged.
- **1 yellow flash :** the key is enabled for opening the cylinder and the battery is almost flat.
- **1 red flash:** the key is enabled for opening the cylinder and the battery is flat.
- **red for 3 sec :** battery is empty
- **3 red flashes:** the key is not enabled for opening the cylinder (= Logical error like wrong plant, key expired, out of time schedule,...)
- **7 red flash :** key reading error (= physical error due to the fact the data from key have not read completely)

Programming key signals when inserted in the cylinder

- blinking read and green alternatively: communication in progress between the key and the cylinder (uploading history,
- 2 green flash : operation completed
- 7 red flash : key reading error (= physical error **due** to the fact the data from key have not read completely)

Battery status signals when the key is not inserted in the cylinder

To check the battery status press the key-head centre for at least 3 seconds:

1 green flash: battery is charged

1 yellow flash : battery is almost flat

1 red flash: battery is flat

Replacing Batteries in Key

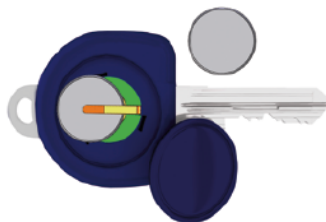
Batteries must not be replaced in potentially explosive atmosphere environment.

Batteries must be reintroduced into the F9000 key within 3 minutes otherwise the internal clock setting will be lost. in the latter case, restore clock setting by synchronising with V364 system at the validator or key programmer (credential reader/writer).

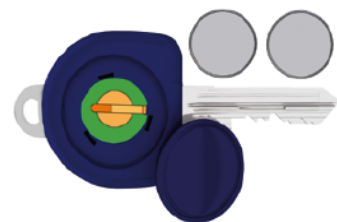
Use only LITHIUM SONY CR1620 3 Volt (70mAh) batteries.



Open cap turning in anti-clockwise direction

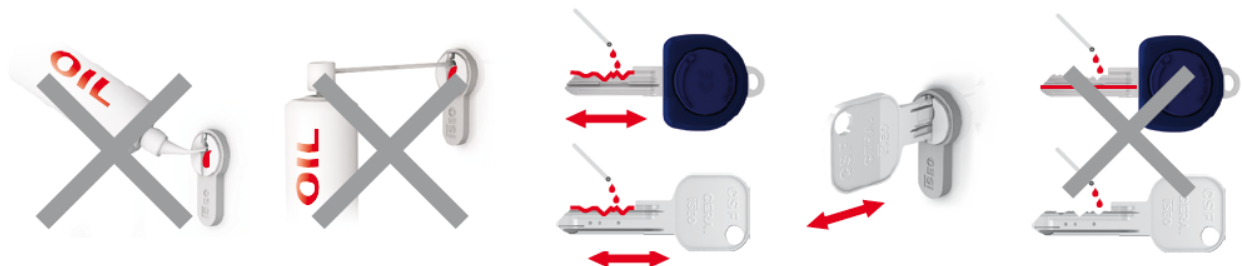


Remove cap and lift gold tab slightly. Turn key to let batteries out



Insert new batteries, positioning them one at a time under the gold tab. Close cap turning in a clockwise

Cylinder lubrication



Iseo recommends cylinders are lubricated at least once a year using “RIVOLTA T.R.S. plus” lubricant.

Lubrication should only be carried out as shown above:

- 1 clean teeth of key carefully
- 2 place a drop of lubricant on teeth
- 3 insert key into cylinder a few times

Product compliance

The product is in compliance with EMC directives (Electromagnetic compatibility).



The products marked with EX Logo are certified By ICIM notified institute nr.0425 in accordance with ATEX directives with following classification: Ex II 2 G EEx ib IIB T4

II = Group II. Comprises equipment intended for use in other places likely to become endangered by explosive atmospheres.

2 = Level of protection: comprises products designed to be capable of remaining within their operational parameters, stated by the manufacturer, and based on a high level of protection for their intended use, in areas in which explosive atmospheres caused by mixtures of air and gases, vapors, mists or air/dust mixtures are likely to occur.

G = Type of explosive atmosphere: Gas vapors

EEx = explosion protections

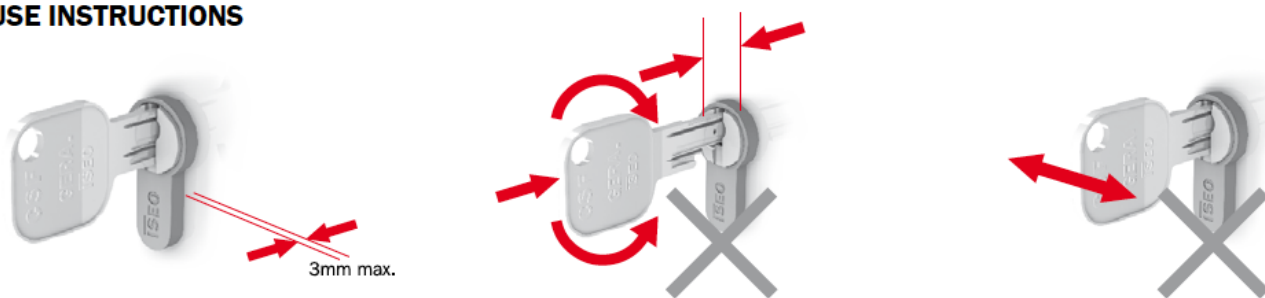
ib = intrinsically safety of the product (EN 60079-11)

IIB = Group of gas (Ethylene)

T4 = Temperature class 135°C (not to be confused with the temperature declared to operate the key max. 60°C)

USE INSTRUCTIONS

USE INSTRUCTIONS



Managing key Assignments

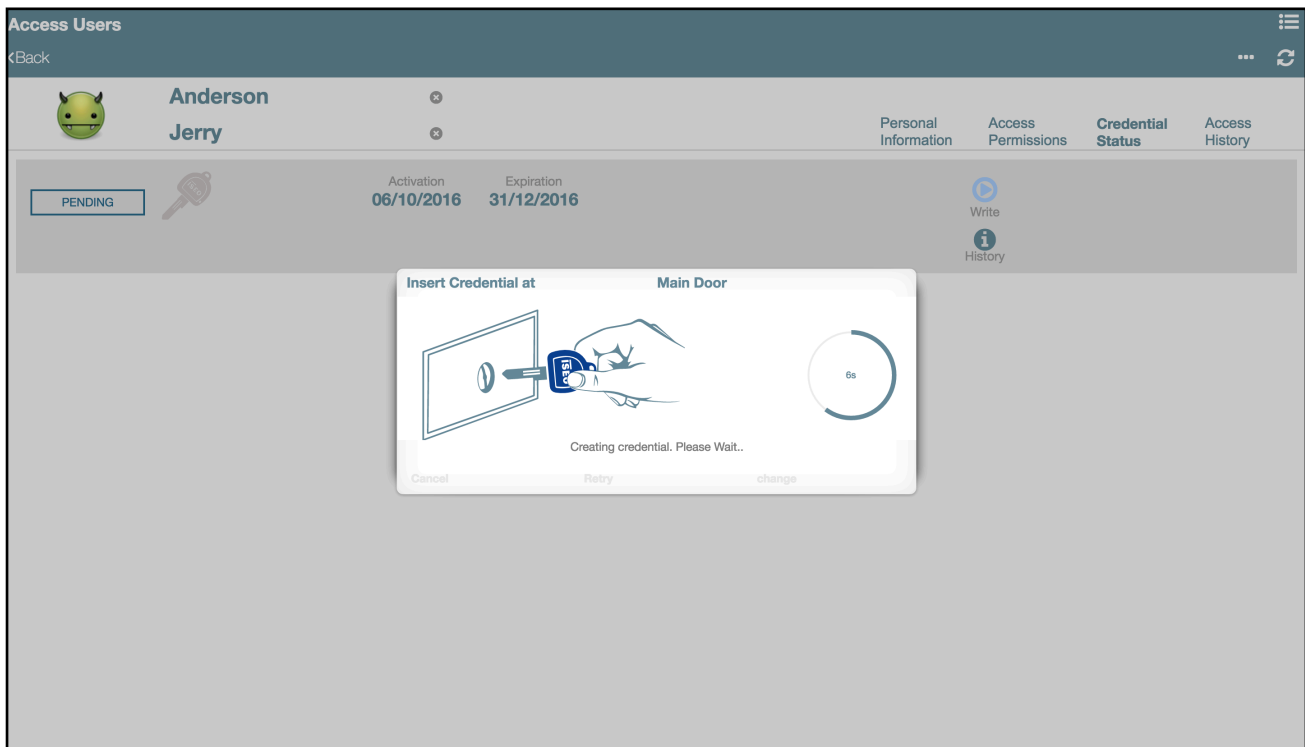
The User F9000 keys are assigned to Access users in order to provide them access to a facility. A User Key can be assigned when the user is first created, or it can be assigned at a later time. Likewise, it is possible to change a user's key assignment or revoke it. Please consult the Access User chapter and the credential lifecycle paragraph.

Reading and writing a credential

The system administrator triggers the operation of writing or reading a credential. The interaction with the reader is the same either reading or writing.

Triggering the Reader / Writer Operation

After triggering a reader / writer operation you will get immediately the following pop up message:



Immediately the reader/writer starts the operation and a timeout icon (10 seconds) shows the remaining time. It requires to insert the credential into the reader indicating whether to insert the programming key (red) or the User key.

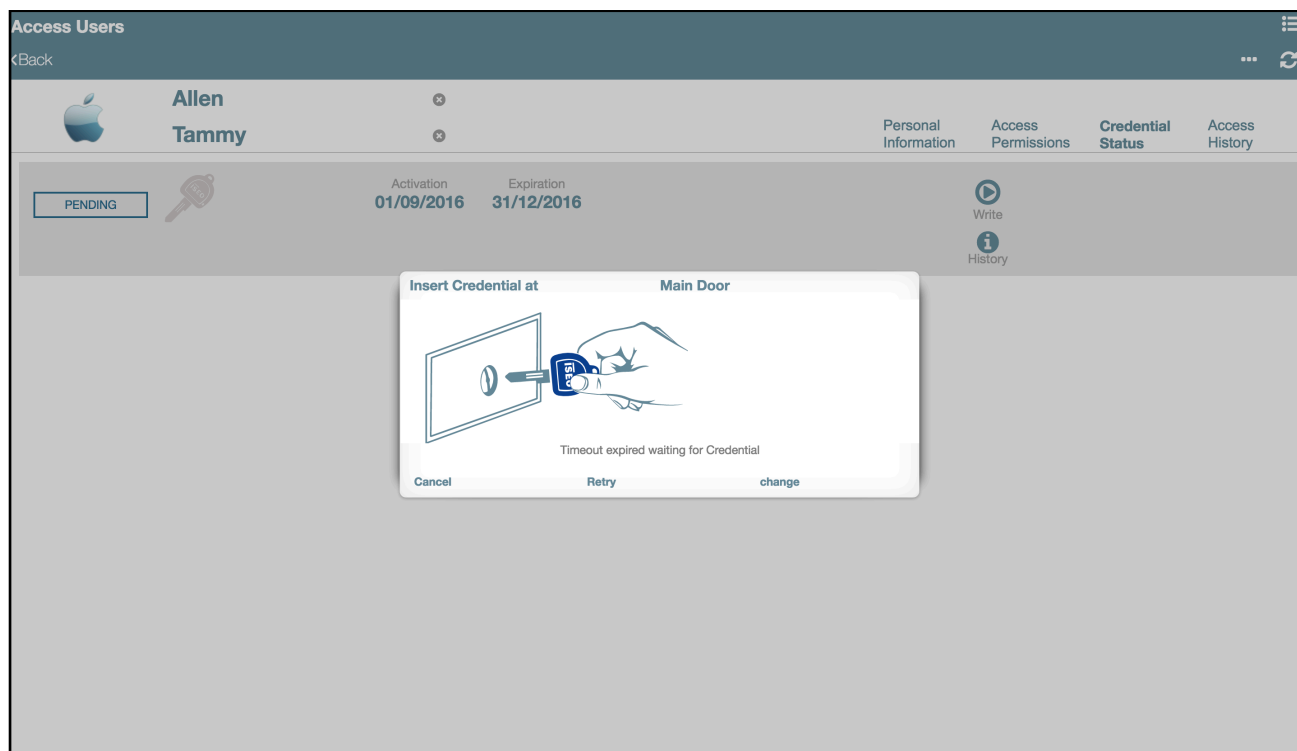
Insert credential at "Reader Name" : is the selected reader and writer for the administrator. After login, the administrator will use the default reader assigned to him. The administrator can select a different one for the session only with **Change Reader** when timeout expires or assign as new default operator reader with the Login Preference menu option.

Timeout Icon : informs about the remaining time to insert the credential at the reader starting from 10 sec. If timeout expires there will be shown the exception "timeout expired". While if the credential is inserted during the 10 seconds we should see "operation in progress" message.

Image with credential and reader: the image will be different depending on the operation type:

1. F9000 Blue key interacting with F9000 reader writer
2. F9000 Red key interacting with F9000 reader writer

If the time out expires then you will see the following :



it is possible to

Retry: will allow to retry the operation on the same reader

Change Reader: will allow to change the reader selecting from a list. It will be possible after the reader selection to use it only during this session or set as default. Selecting The change reader option the timeout bar will stop (cancel operation) and will restart after confirming the new reader.

Cancel : will cancel the operation

Roles

Traditional and Role-Based Access Control

In traditional access control, the access authorizations are directly assigned to the access user. With Role-Based Access Control, permissions are based on the roles that individual users have as a part of an organization. Roles are closely related to the concept of user groups, simplifying complex access control policies.

Access Users and Roles

An Access user (or simply a user) is any person who requires access to one or more doors at the facility. A user has unique credentials, (the F9000 key), that enable entry at the specified doors.

Normally a user has a role in an organization and also the physical access permissions are associated with the role (or function) the User has in the organization.

A user can have only one role which defines his door access privileges.

Several users can have the same role in the organization determining a group of people (a set of users) with the same access privileges to a facility.

A Role (or group of people) has a descriptive name, such as “Marketing Staff.” Access privileges are defined at the Role level. A user inherits access privileges from the role assigned to him or her.

However, an individual user’s privileges can be set to start and/or expire on specified dates and validation period.

In addition to a role the Access Privileges can be assigned simply selecting individual doors for the User.

Therefore Access privileges for an Access User can be:

- defined while setting up a specific role for a group of users (Role Based Access Control) or
- assigned directly to a user assigning doors while creating/modifying the User (Traditional access control)

Administrators vs. Users and related roles

The term Access User (or simply user) refers to an individual who has access privileges to some part of a building. User does not refer to system administrators of the V364; users do not have direct access to the V364 system administration interface. Instead, System Administrators (administrators) add and manage user-related information.

The term Administrator, on the other hand, refers to an individual who has access permissions to login to V364 interface.

An Administrator has also different login access levels allowing control and restriction of what each person is authorized to manage or view. The login access authorization is also defined “administrator Role”.

The system administrators access to the V364 system by a **Login ID** and **Password**.

Browsing the Roles List

To view the list of Roles:

Click the Menu dropdown and select Access User Management then click on the Roles tab. The Roles list displays. The Roles list displays a list of all Roles currently defined in the system.

The list displays the Roles listed alphabetically.

The Role ALL DOORS 24H (“All the doors always”) is a Role defined automatically when the System is first created and cannot be removed.

Roles					
		Users	Doors	Time Schedules	
GM	General Manager	1	7	1	>
M1	M1 Role	199	451	1	>
M2	M2 Role	316	424	1	>
M3	M3 Role	424	106	1	>
M4	M4 Role	600	364	1	>
M5	M5 Role	583	249	1	>
M6	M6 Role	335	239	1	>
M7	M7 Role	167	821	1	>
M8	M8 Role	116	234	1	>
MT	MT Role	182	404	1	>
OPS Team	Operations Team	10	5	3	>
R&D Team	Research & Development Team	6	4	2	>
W1	W1 Role	64	35	1	>
W2	W2 Role	159	28	1	>
W3	W3 Role	31	301	1	>

19/19 Elements

Details displayed include:

- Role Name: the name given to the Role (group of people) , such as “Managers”, “Cleaning Staff”
- Access Users: the number of users currently associated with this role. In other words the number of users which are members of the group (affiliated to the group)
- The number of doors in total associated with the role
- The number of Time Schedules used in the role. The maximum number o Time Schedules is 6 fo reach role. Each Time schedule can have up to 6 time intervals which can be selected individually by weekday.
- The number of Door Zones associated with the role

System Administrators with appropriate login permission can:

- Create a New Role
- Edit an existing Role
- Duplicate and existing Role (in order to create a similar one)
- Searching for an existing role
- Delete a not used Role

Creating a New Role

A Role defines access privileges that can then be assigned to several access users creating a set of users with the same access privileges (a user group) .

For example:

a) The company “Green Apple” might have two doors.

If all employees require the same level of access to both doors, then a single Role, “Green Apple Staff,” would be sufficient.

b) The company “Green Apple” might have three doors. If we say that the staff requires access to “Front Door” only while managers require access to all three doors, then it would make sense to create two Roles (or Access User groups), one called “Green Apple Staff” and one called “Green Apple Managers.”

To create a Role:

1. Click the Menu dropdown and select Access User Management then click on the Roles tab. The roles list displays.
2. Click Add New Role. The Edit Role page displays with blank fields.
3. Insert a Role Name and a description for it.
4. Define Access Permissions assigning individual doors to the role:

On the right side you see the available doors of the system that you can add to the Role
You can change the view and select a Door Zones view (see creating a role with door zones)

If you keep the single door view (available doors) you can:

The screenshot displays the 'Roles' management interface. At the top, there's a header bar with 'Roles' and a back arrow. Below the header, there's a form for creating a new role with fields for 'Role Name' and 'Role Description'. To the right of the form, there's a list of 'Available Doors'. The list includes 11 items, each with a radio button for selection and a door icon. The items are: EEM Office (Electronic Engineering manager Office), GM Office (General Manager Office), Gas Refinery (Gas Refinery Plant), Gym (Gym facility), Lab 01 (Laboratory 1), Lab 02 (Laboratory 2), Lab 03 (Laboratory 3), Lab 04 (Laboratory 4), Lab 05 (Laboratory 5), Lab 06 (Laboratory 6), Lab 07 (Laboratory 7), Lab 08 (Laboratory 8), Lab 09 (Laboratory 9), Lab 10 (Laboratory 10), and Lab 11 (Laboratory 11). The bottom of the interface shows '0/0 Elements' for the 'Assigned Doors' section and '21/21 Elements' for the 'Available Doors' section.

- a. select individually some doors
- b. search for a door (example all doors which contains “Lab”) and select ALL door that have been filtered out with the search

As soon as you select a door the “view zones” button disappears and you see the button ADD.

Pressing ADD the selected doors will be assigned to the Role moving the doors from the right side (available doors) to the left side (assigned doors).

At this point you can still add more doors with a new search or edit the time schedules of the assigned doors.

If you select doors from the assigned doors (on the left side) you can also REMOVE them

5. Edit Time Selecting Edit Time you will have on the right side the available time schedule defined in the system. Selecting one of the Time Schedules you can assign it to the selected doors and Define for each door a Time schedule associated up to a maximum of 6 Time schedules for Role. This Time Schedule determines the weekdays and time intervals in which the users with this role will have access to the doors. To specify when the Role will have access to each door:

The screenshot shows the 'Roles' configuration page for the 'Visitor' role, titled 'visitors using the Gym facility'. The interface is divided into two main sections: 'Assigned Doors' on the left and 'Time Schedules' on the right. The 'Assigned Doors' section has a search bar with 'Type and Enter' and a 'Select all' button. It lists two doors: 'Gym' (Gym facility) and 'Main Door', both with a blue star icon indicating they are modified. Each door has a radio button and a 'Working Hours' label with 'Week Working Hours' below it. The 'Time Schedules' section on the right has a plus icon and a 'Time Schedules' header. It lists two schedules: '24H ALWAYS' and 'Working Hours' (with 'Week Working Hours' below it), both with radio buttons. At the bottom of the 'Assigned Doors' section, it says '2/2 Elements'.

6. Save will save the role and show it in the Role list

Note:

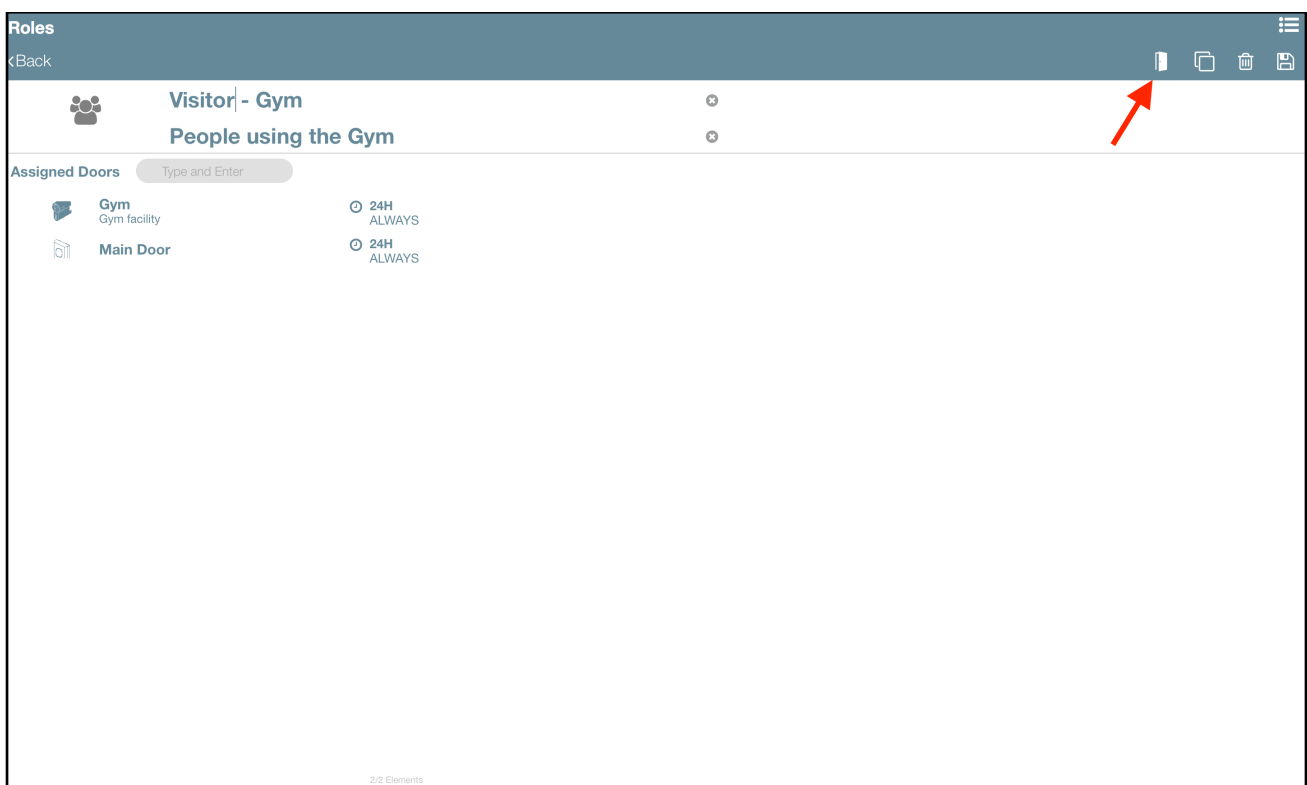
The items with the * are the modified ones based on the previous value of the role

Editing an existing Role

Once a Role is created, its name or access permissions can be edited at any time. Editing a Role changes the access permissions, the days and times during which the users with the same role (the users members in that group) can enter in the plant.

To edit a Role

1. Click the Menu dropdown and select Access User Management then click on the Roles tab. The roles list displays.
2. Click the Role whose permissions you want to change. The corresponding Role details page displays. The Role details page displays the name and access information for a specific Role.
3. To Modify the access permission and the Time Schedules select the Door button:



To add more doors select/search more doors

- Save will add the new selected doors to the existing ones
- Save will save the modified role

To remove some doors select remove and select the doors to remove from the role

- Save will save the modified role

To modify Time Schedules, select edit Time

- Select the doors to associate with a specific time schedule
- Save will save the role

Note:

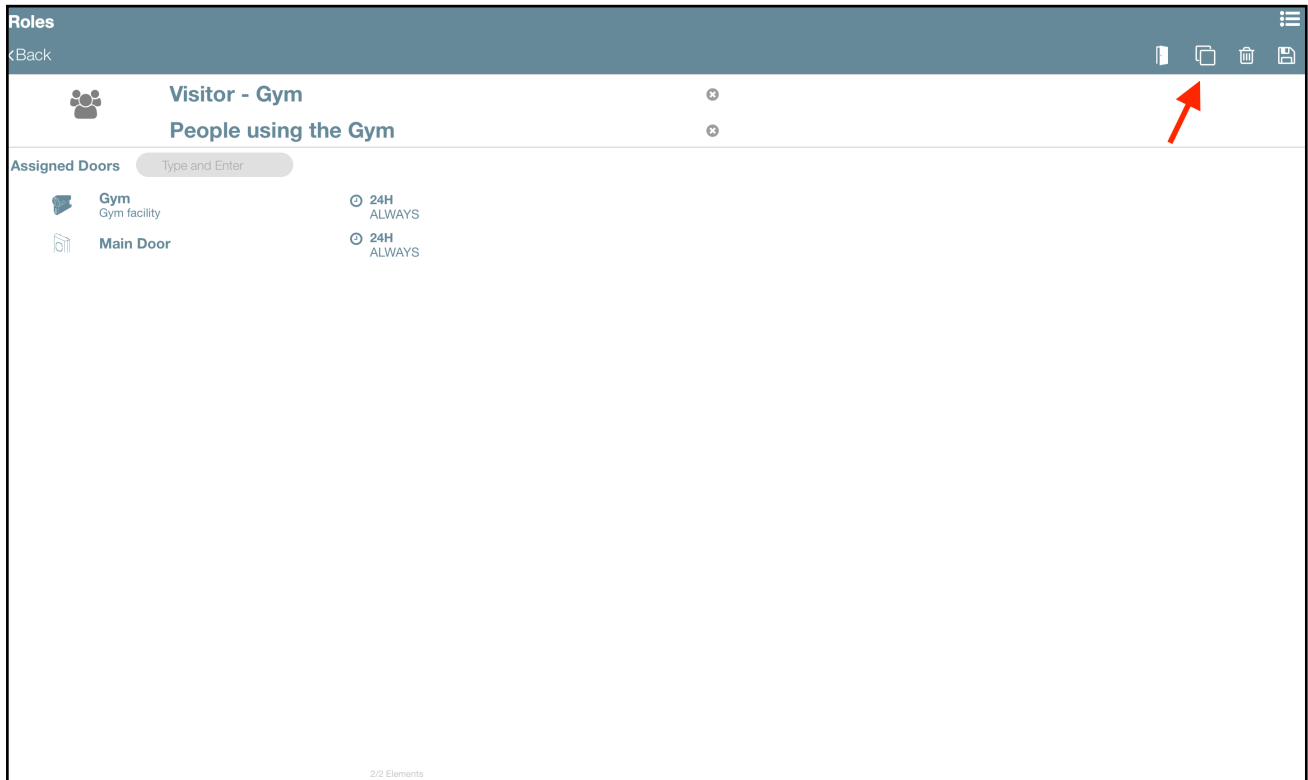
The items with the * are the modified ones based on the previous value of the role

Duplicating a Role

This feature is useful if you want to create a new role just starting modifying an existing one as the new one has little modifications from the original.

Duplication allow a creation of a Role which has the same door assignments and an initial default name of RoleName_Copy.

1. Select the Role to duplicate
2. Press Duplicate button



3. Confirm the duplicate operation
4. You will get a new role with the same access right of the originale ready to allow modifications

Roles

Back

Visitor - Gym_copy

People using the Gym

Assigned Doors

Type and Enter

Select all

Gym

Gym facility

24H

ALWAYS

Main Door

24H

ALWAYS

Available Doors

Type and Enter

Select all

EEM Office

Electronic Engineering manager Office

GM Office

General Manager Office

Gas Refinery

Gas Refinery Plant

Lab 01

Laboratory 1

Lab 02

Laboratory 2

Lab 03

Laboratory 3

Lab 04

Laboratory 4

Lab 05

Laboratory 5

Lab 06

Laboratory 6

Lab 07

Laboratory 7

Lab 08

Laboratory 8

Lab 09

Laboratory 9

Lab 10

Laboratory 10

Lab 11

Laboratory 11

MEM Office

Mechanical Engineering Manager Office

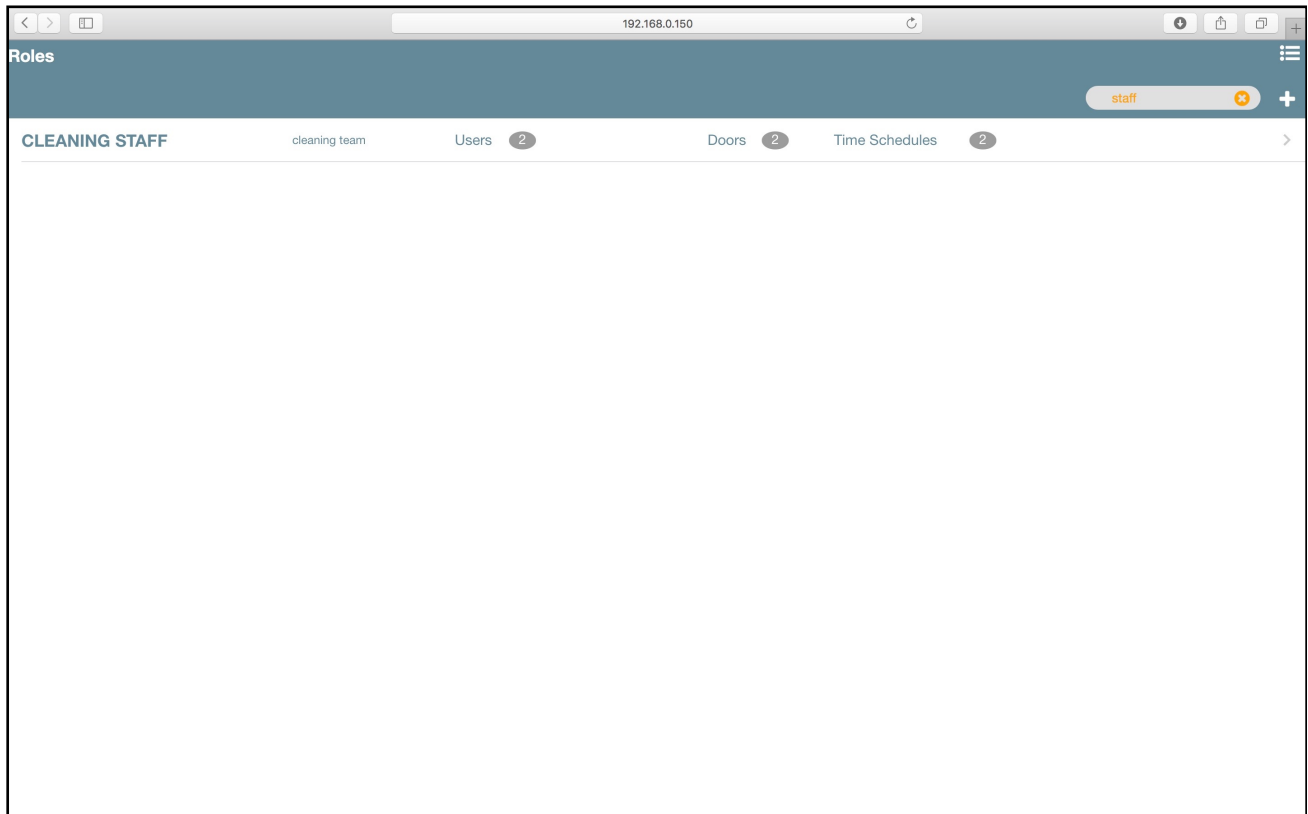
2/2 Elements

25/25 Elements

38

Searching for a Role

1. Click the Menu dropdown and select Access User Management then click on the Roles tab. The roles list displays.
2. Click the Lens search and insert the text for searching in the Role Name or Role description
3. all the roles containing the typed string in the name or description will be displayed. The lens in orange informs that a filtering is active with a specified string



Deleting a Role

Roles which are not assigned to any users can be deleted.

To delete a Role:

1. Click the Menu dropdown and select Access User Management then click on the Roles tab. The roles list displays.
2. Click the name of the Role you want to delete. The corresponding Role details page displays.
3. Click Delete (Trash Bin)

A warning message asks you to confirm that you want to delete the Role

Time Schedules

Time Schedules

Time Schedule are user defined schedules (example: from 8:00am to 5:00pm) that can be applied to a specific person or Role to define when that person has access to a particular door. Any Access User who attempts to access a door during a restricted Time Zone will be denied access.

A Role can allow access to different doors, according to a predefined schedule: it is possible to define access to single door differently for individual user or groups of users (defining it in the Role). For example, the group “Staff” may have access to the “Front Door” according to the schedule “Work Day,” which allows them to access the door, using a valid credential, between the hours of 7:00AM and 6:00PM. At the same door, the group “Cleaning Crew” may have access according to the “Night Shift” schedule, permitting them access only during the hours of 8:00PM and midnight.

The Time Schedule use a 24 hour clock.

- Midnight to Noon is represented as 00:00 to 12:00
- Noon to midnight is represented as 12:00 to 23:59

Browsing the Time Schedules List

To view the list of schedules:

Click the Menu dropdown and select Access User Management then click on the Time Schedule tab. The Time Schedules list displays a list of all schedules currently defined in the system. The list displays the Time schedules listed alphabetically.

Time Schedules		
24H	Time intervals	1
CLEANING STAFF WORKDAY	Time intervals	1
DAY TIME	Time intervals	1

24H (“Always”) is a Time schedules defined automatically when the System is first created.

Details displayed include:

Time schedule name

Intervals: the number of time interval associated with the time schedule

System Administrators with appropriate login permission can:

- Create a New Time schedule
- Edit an existing Time schedule
- Duplicate an existing Time schedule (in order to create a similar one)
- Delete a not used Time schedule

Creating a New Time schedule

1. Click the Menu dropdown and select Access User Management then click on the Time Schedule tab. The Time Schedules list displays.
2. Click Create New Schedule. The Edit Time Schedule page displays with blank fields.

The screenshot shows the 'Time Schedules' interface. At the top, there's a header bar with the title 'Time Schedules', a back arrow, and icons for settings and saving. Below the header, there are two input fields: 'Name' and 'Description'. The main part of the interface is a time schedule graph. It consists of a horizontal timeline from 00:00 to 24:00 with major ticks every 6 hours. Below the timeline, there are seven columns representing the days of the week: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. A red bar is currently set from 08:00 to 18:00 on Monday. Checkmarks are present under the Mon, Tue, Wed, Thu, and Fri columns, while empty boxes are under Sat and Sun. A small input box on the left shows '08:00 - 18:00'.

3. Enter a brief, descriptive Name for the schedule, such as “Night Shift” or “Cleaning Crew.” and a description
 - The first time interval is already proposed and you can modify the begin and end by typing the start and end time or simply moving the slider in steps of 15 minutes.
 - For each day of the week define when the defined interval is active. Active time intervals determine when an access users has access to a door. For each day of the week, monday through Sunday, the time schedule graph indicates the “on” periods for the selected schedule. In other words, when it is assigned to a user, these are the periods during which users may access the door.

- You can add other time intervals with the “add interval” button up to 6 time intervals for each time schedule.
 - To edit a time interval once it is defined, click on the time interval property you want and modify for example use the Start and End fields (or slider) to change the time range.
 - To delete a time interval simply deselect it. When saving the Time Schedule this time interval will be deleted. The time interval is cleared from the Time Schedule graph if you later will edit the Time Schedule from the Time schedule List.
4. Click Save. The Time Schedule Details page displays. This Time schedule can now be used to define access permissions.

Time Schedules over midnight: for example, you might have a schedule called “Cleaning Crew” that is active 6:00 pm through 2:00 am Monday through Friday. But on weekends, you want to limit access to 6:00 pm through 10:00 pm.



Editing an existing Time Schedule

1. Click the Menu dropdown and select Access User Management then click on the Time Schedule tab. The Time Schedules list displays.
2. Click the Time schedule you want to edit. The corresponding Time Schedule Detail page displays.
3. Edit the schedule according to the preceding guidelines for *Creating a New Time Schedule*.
4. Click Save. You are returned to the Schedule detail page.

Duplicating an existing Time Schedule

1. Click the Menu dropdown and select Access User Management then click on the Time Schedule tab. The Time Schedules list displays.
2. Click the Time schedule you want to duplicate. The corresponding Time Schedule Detail page displays.
3. Click duplicate a new Time Schedule copy of the original one
4. Edit the schedule according to the preceding guidelines for *Creating a New Time Schedule*.
5. Click Save. You are returned to the Schedule detail page.

Deleting a Time Schedule

Time Schedules which are not assigned to any users can be deleted.

To delete a Time Schedule:

1. Click the Menu dropdown and select Access User Management then click on the Time Schedules tab. The Time Schedules list displays.
2. Click the name of the Time Schedule you want to delete. The corresponding Time Schedule details page displays.
3. Click Delete (Trash Bin)

A warning message asks you to confirm that you want to delete the Time schedule

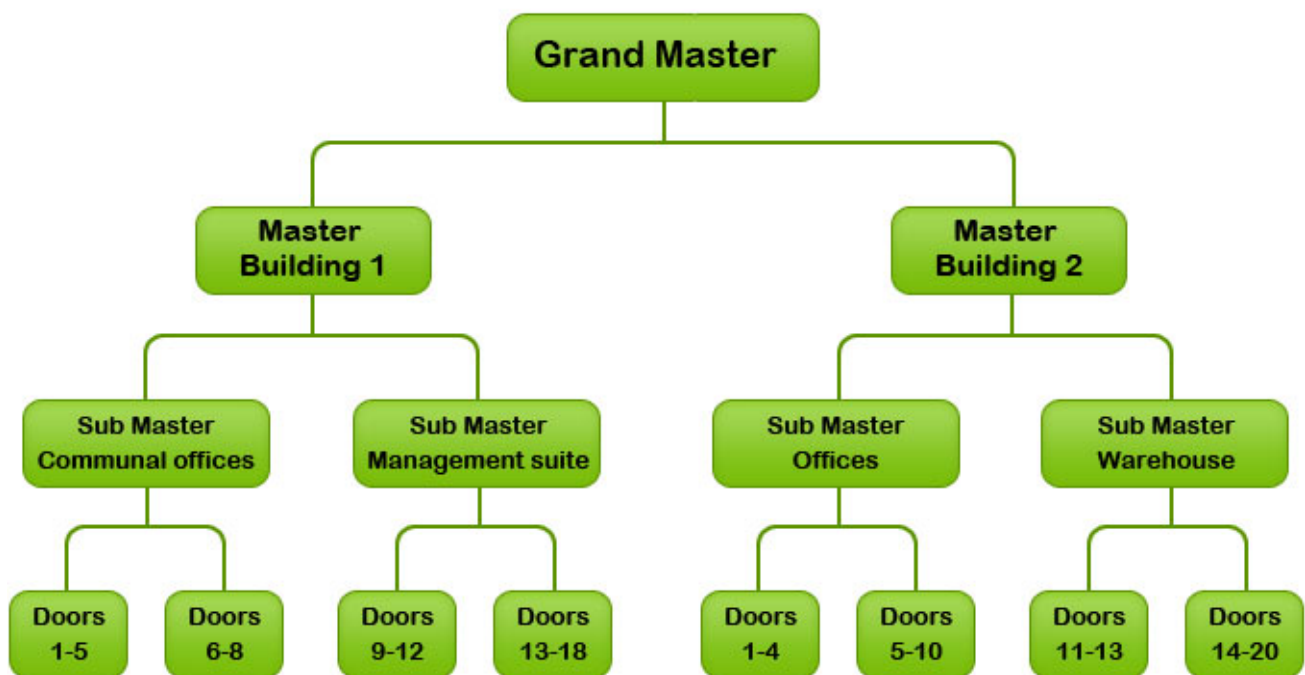
Door Zones

In some sites doors are arranged into geographical area zones or simply Door Zones. In these cases, when creating a Role, it might be useful to select an aggregation of doors that represent a Door Zone instead of selecting individually all the single doors one by one. Therefore a door can have a geographical zone to which belongs to. A door can be assigned only to one zone as the zone represents a geographical aspect of the site installation: obviously a door cannot be in 2 different geographical areas. If the door is not assigned to any zone then when displaying the zones in creating the Role the door is displayed with its name as representative of the zone: it is basically a zone of one single door.

Summary:

- Zones are an aggregation of doors belonging to a geographical area
- A door can be assigned only to one zone
- Door not assigned to zones are shown with their name

Door Zones are very useful when there is a hierarchical structure of the doors:



In this case the creation of a role is much quicker as you do not need to select doors individually but you select an aggregation of doors.

Browsing the Door Zones List

To view the list of Door Zones:

Click the Menu dropdown and select Access User Management then click on the Door Zones tab. The Door Zones list displays a list of all schedules currently defined in the system. The list displays the Door Zones listed alphabetically.

Door Zones				
Labs	Laboratories	gates	11	>
Remote Plants	Plants that are remote sites with a padlock	gates	2	>
Sales	Sales Area	gates	2	>
3/3 Elements				

Details displayed include:

Door Zone name

Doors: the number of doors associated with the Door Zone

System Administrators with appropriate login permission can:

- Create a New Door Zone
- Edit an existing Door Zone
- Delete a not used Door Zone

Creating a Door Zone

To create a Door Zone:

1. Click the Menu dropdown and select Access User Management then click on the Door Zone tab. The Door Zone list displays.
2. Click Add New Door Zone. The Edit Door Zone page displays.
3. Insert a Door Zone Name and a description for it and select the doors you want to include into the Door Zone with the buttons Add and Remove:

Door Zones

<Back New Door Zone

Remote Plants

Plants that are remote sites with a padlock

Assigned Doors Type and Enter Select all

- ☐ Gas Refinery
Gas Refinery Plant
- ☐ Solar Power Plant
Solar Power Plant

Available Doors Type and Enter Select all

- ☐ EEM Office
Electronic Engineering manager Office
- ☐ GM Office
General Manager Office
- ☐ Gym
Gym facility
- ☐ Main Door
- ☐ Meeting Room
Meeting Room
- ☐ MEM Office
Mechanical Engineering Manager Office
- ☐ MKTG
Marketing
- ☐ OPS
Operations
- ☐ R&D
Research & Development
- ☐ Show Room
Show Room
- ☐ SWM Office
Software manager Office
- ☐ Training Room
Main door to enter to Laboratory area

0/2 Elements 13/13 Elements

On the right side you get the list of door that have non yet been assigned to any Door zone yet. While creating the door zones this available door list will become smaller as more and more doors will be assigned to door zones.

If you want to move a door from one zone to another first you have to remove it from a zone and then edit the door zone where you want to add the door, you will see the door on the right available and then you can add.

Note that all credential issued that are impacted from any change in door zone will need to be rewritten at the validators as they are no more in synch with the Atlas Database.

Editing an existing Door Zone

1. Click the Menu dropdown and select Access User Management then click on the Door Zone tab. The Door Zones list displays.
2. Click the Door Zone you want to edit. The corresponding Door Zone Detail page displays.
3. Edit the schedule according to the preceding guidelines for *Creating a New Door Zone*.
4. Click Save. You are returned to the Door Zones list page.

Deleting a Door Zone

Door Zones which are not assigned to any Access users can be deleted.

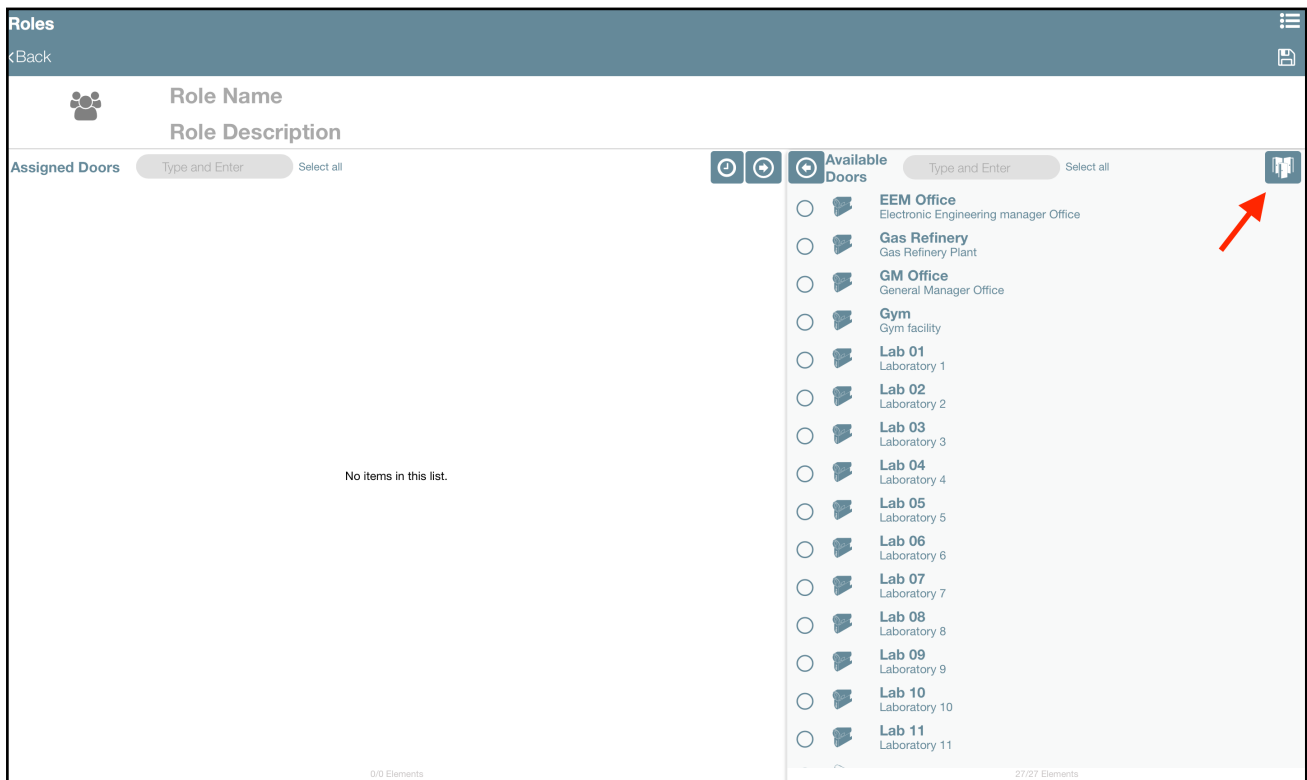
To delete a Door Zone:

1. Click the Menu dropdown and select Access User Management then click on the Door Zones tab. The Door Zones list displays.
2. Click the name of the Door Zone you want to delete. The corresponding Door Zone details page displays.
3. Click Delete (Trash Bin)

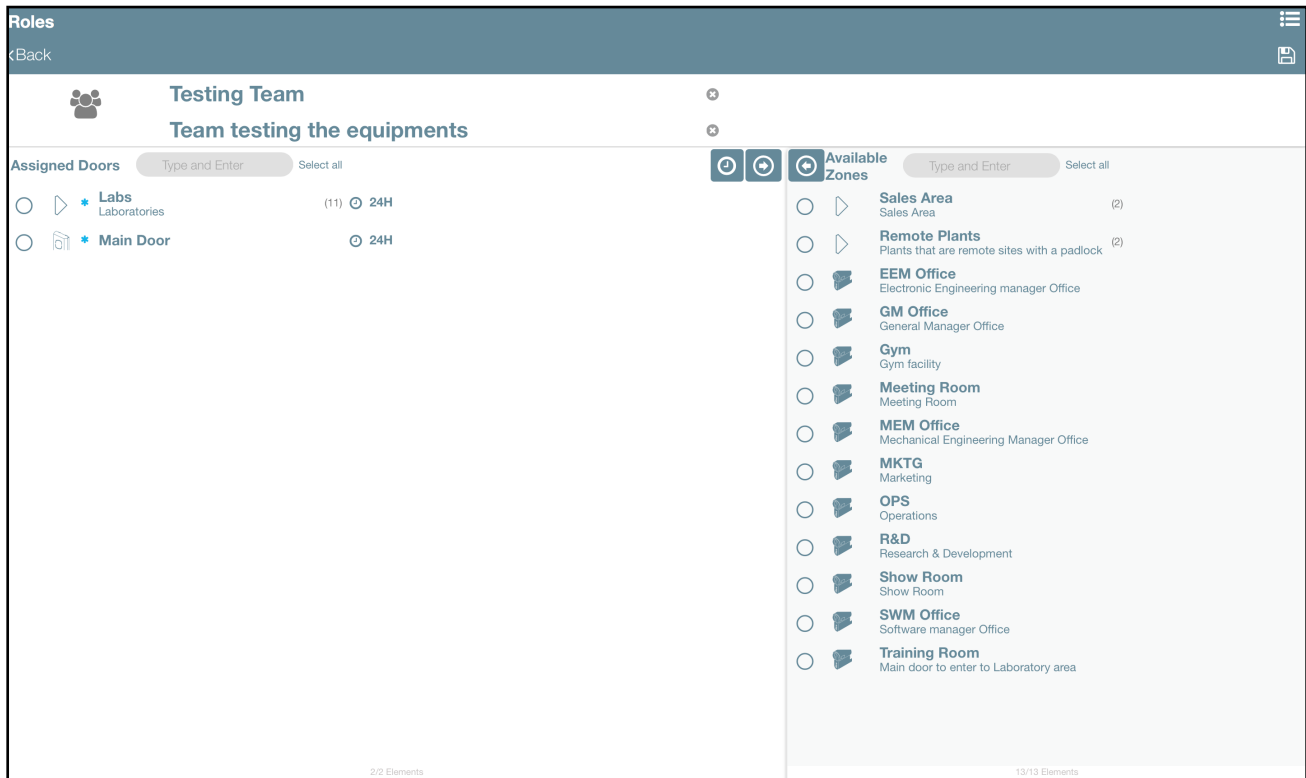
A warning message asks you to confirm that you want to delete the Door Zone

Creating a Role using Door Zones

1. Click the Menu dropdown and select Access User Management then click on the Roles tab. The Roles list displays.
2. From the Roles list, select Add Role and in the edit new role form select “view Zones”



3. The list of the available door zones will appear on the right side:
For each available zone you can see how many doors are in each zone and if you click in the triangle, you see also which are the single doors belonging to the selected Zone.
In case a door does not belong to any Door Zone (single door) you just see the door name.
You can toggle the view back to single doors pressing View Doors.
But if you start selecting a Zone then the view doors will become ADD and you can add a zone:



Adding the door zone will move the item to the right and selecting a door zone from the left you can Edit the Time schedule or Remove the item as a whole. It is not possible to edit a single door within the zone.

Why when you start working with Door Zone you can not go back to the single doors?

One of the important feature of V364 is the capability to assign different Time Schedule to several doors. Suppose you can mix single doors and Door Zones, the following scenario could happen: if you have already selected a Door Zone and you add a particular door which is already into zone you have possible conflicts as the same door might have two different time schedules.

This situation is particularly critical if you already have Roles or Access Users already issued with Single doors and Door Zones and a modification of a Door Zone will need to be checked on all Access Users resulting a long time to wait for a confirmation and when detected need to be properly handled that Iseo will reserve to address in the future.

Access Users

An Access User is any person who requires access to one or more doors of the site. A User has a unique F9000 mechatronic key, that enable entry at the specified doors.

The Access User menu option allows you to enter new personnel, assign credential with access privileges, view the credential status and view the user access history collected by the user credential while opening the doors and uploaded in the validators.

A user can have an assigned role therefore belonging to one group of people.

Activation and expiration dates can be set allowing to enter Access Users information into the system without activating the credential. Access Users can also be imported in the system.

A credential can be assigned to the user with the following processes:

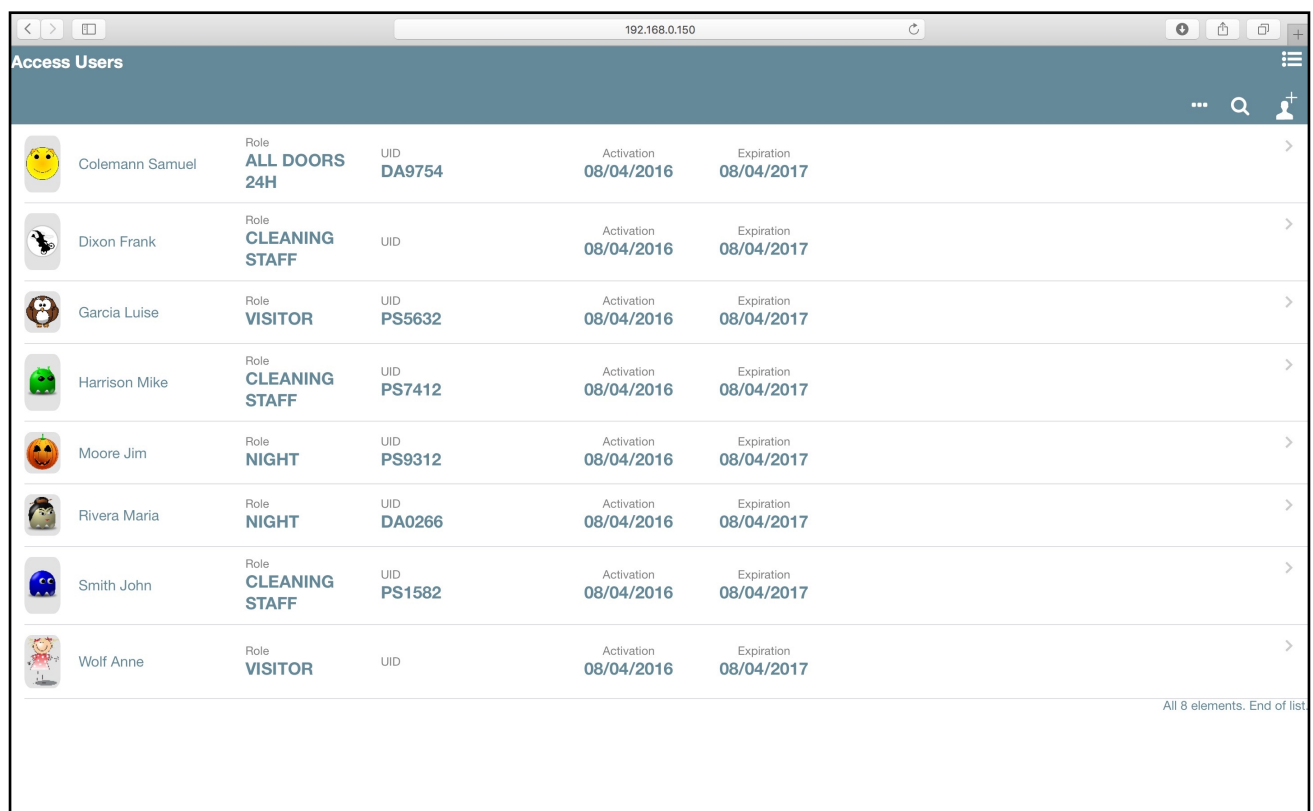
- 1) Credential UID ENROLL: typing the credential UID and giving the credential to the user
- 2) Credential immediate write on a credential reader/writer: writing directly the credentials on the local credential reader/writer

Browsing the Access User List

The Access Users List page displays the list of users active in the system regardless the status of their credential. Users are listed by Last Name alphabetical order in the Access User List.

To view the list of users:

Click the Menu dropdown and select Access User Management then click on the Access Users tab. The Access User List displays.



	Role	UID	Activation	Expiration	
 Colemann Samuel	ALL DOORS 24H	DA9754	08/04/2016	08/04/2017	>
 Dixon Frank	CLEANING STAFF	UID	08/04/2016	08/04/2017	>
 Garcia Luise	VISITOR	PS5632	08/04/2016	08/04/2017	>
 Harrison Mike	CLEANING STAFF	PS7412	08/04/2016	08/04/2017	>
 Moore Jim	NIGHT	PS9312	08/04/2016	08/04/2017	>
 Rivera Maria	NIGHT	DA0266	08/04/2016	08/04/2017	>
 Smith John	CLEANING STAFF	PS1582	08/04/2016	08/04/2017	>
 Wolf Anne	VISITOR	UID	08/04/2016	08/04/2017	>

All 8 elements. End of list

Details displayed include:

Picture : an image associated with the Access User

Name: the user's name. Last Name and First name

Role: the role of the user in the organization (the user group to which the user is affiliated).

Credential UID: if a credential is associate to the Access User the credential Unique Identifier is displayed

Activation Date: set the date that an Access User becomes active. Prior to the activation date, the credential associated to the User will not work.

Expiration Date: set the date that a Access User will expire. After this date, the associated credential will not work.

System Administrators with appropriate login permission can:

- Create new Access Users and assign a credential
- View existing Access User details like access privileges, validity, Credential Status and Access History
- Manage existing access Users: modifying access privileges, suspending user credential, reinstating user credential, revoke user credential (replacing or deleting credential)
- Read a credential and display the associate Access User data on it
- Import Access Users
- Export Access Users list in a .CSV file
- Search for Access User containing a specified string in the Name or Role

Create a new Access User and assign a Credential

To create a new user

1. Select the dropdown menu and select Access User Management and then Access Users. The Access Users list displays.
2. Select Add User and the Edit Access User form with empty fields displays and then you start to insert the fields:

Access Users

<Back

Last Name
First Name

Personal Information Access Permissions Credential Status Access History

Role
Select an item from the list

Credential
 UID

Validity

Activation	08/04/2016		Validation period: minutes	value 1	
Expiration	08/04/2017		Days 366		

Assigned Doors

3. **User Picture:** if you wish to insert a User photo, click on the picture button and the Upload Image popup window displays. You can upload .png images format.
4. **Name:** Enter the user's Last Name and First Name. Last Name is required
5. **Credential UID (Optional) :** the Unique IDentifier of the credential that will be assigned to the Access User - this in case of UID enroll process) If your do not have a credential reader and you know the credential UID , type the UID
6. **Activation Date:** defaults to today's date. Change the date if the user's access permissions should take effect on a later date. It is possible to display also the time for the Activation date (see system preferences enable Display time for activation and expiration)
7. **The Expiration Date field** is automatically calculated considering the system preferences. Enter a date if the user's access permissions should expire on a pre-determined date. It is possible to display also the time for the Expiration date (see system preferences enable Display time for activation and expiration)
8. **Validation Period:** in minutes, hours or days the period of time after which the credential validation expires and must be validated again at the online validators.
9. **Role (optional) :** To assign a role select the desired role from the Available Role list. The group name displays in the In Groups list. To remove Role, click the (x). The user inherits access permissions from the Role to which he or she is assigned. Selecting the role from the list you will see the list of the Assigned doors with the role.
10. **Assign individual doors (optional):** If the user has not any Role then any combination of doors can be assigned to him/her. Instead of using the role, select the "door" button to assign individual doors to the User:

Access Users

Back



Deer

Antony

Personal Information

Access Permissions

Credential Status

Access History

Role

Credential

Select an item from the list

UID

Validity

Activation

14/09/2016

Expiration

13/10/2016

Validation period:

hours

value

8

Days

30

Assigned Doors

Type and Enter

No items in this list.

0/0 Elements

then you will see:

The screenshot shows the 'Access Users' interface. At the top, there's a header bar with a back arrow, the title 'Access Users', and a menu icon. Below the header, the user's profile is displayed: 'Deer Antony' with a profile picture and a 'Personal Information' tab. The 'Access Permissions' tab is active, showing a 'Role' dropdown (set to 'Select an item from the list'), a 'Credential' type (set to 'UID'), and 'Validity' information (Activation: 14/09/2016, Expiration: 13/10/2016, Validation period: 30 days, value: 8). Below this, there are two panels: 'Assigned Doors' on the left (currently empty, showing 'No items in this list.') and 'Available Doors' on the right. The 'Available Doors' panel has a search bar and a list of doors with checkboxes. A red arrow points to the 'Available Doors' panel. The list of available doors includes: EEM Office, GM Office, Gas Refinery, Gym, Lab 01, Lab 02, Lab 03, Lab 04, Lab 05, Lab 06, and Lab 07.

On the right side you see the available doors of the system that you can add to the Access User. You can change the view and select a Door Zones view
If you keep the single door view (available doors) you can:

- select individually some doors
- search for a door (example all doors which contains "Lab") and select ALL door that have been filtered out with the search

As soon as you select a door the "view zones" button disappears and you see the button ADD.

Pressing ADD the selected doors will be assigned to the Access User moving the doors from the right side (available doors) to the left side (assigned doors).

At this point you can still add more doors with a new search or edit the time schedules of the assigned doors.

If you select doors from the assigned doors (on the left side) you can also REMOVE them

- Edit Time Selecting Edit Time you will have on the right side the available time schedule defined in the system. Selecting one of the Time Schedules you can assign it to the selected doors and Define for each door a Time schedule associated up to a maximum of 6 Time schedules for Role. This Time Schedule determines the weekdays and time intervals in which the users with this role will have access to the doors. To specify when the Role will have access to each door:

Access Users

Deer Antony

Personal Information

Access Permissions

Credential Status

Access History

Role

Credential

Validity

Activation

14/09/2016

Validation period:

hours

value

8

Expiration

13/10/2016

Days

30

Assigned Doors

Type and Enter

Select all

Gas Refinery

Gas Refinery Plant

24H ALWAYS

Gym

Gym facility

24H ALWAYS

Main Door

24H ALWAYS

Time Schedules

24H ALWAYS

Working Hours

Week Working Hours

Working Hours with Break

Week Working Hours with break

11. Click Save to save the user and “reserve” the credential for the user in the system. Reserving a credential means that a credential is allocated in the system for the access User, in other words there is a pending credential for the Access Users but the credential is not yet written with the Access data. Until the Access data are not written for the first time the credential will be pending and the administrator might rescind it. At the moment the access data are written in the credential (defined as Credential Provisioning or credential Issuance) the credential becomes Active . At any time prior to the credential provisioning (issuance), the administrator may rescind the pending credential and therefore no credential is assigned to the Access User .

Note:

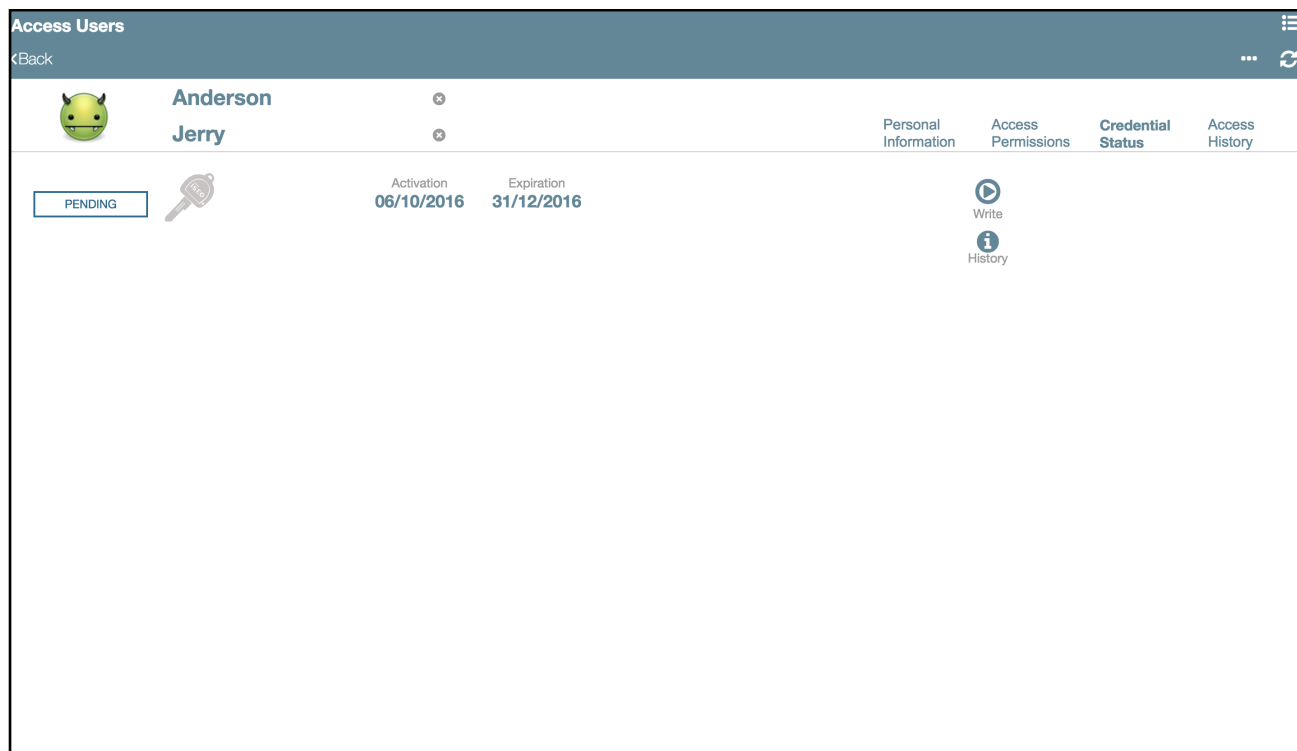
The items with the * are the modified ones based on the previous value of the role
The icon ! on the save warns about the fact the Access User access permissions have been modified and it requires a Save to take effect.

53

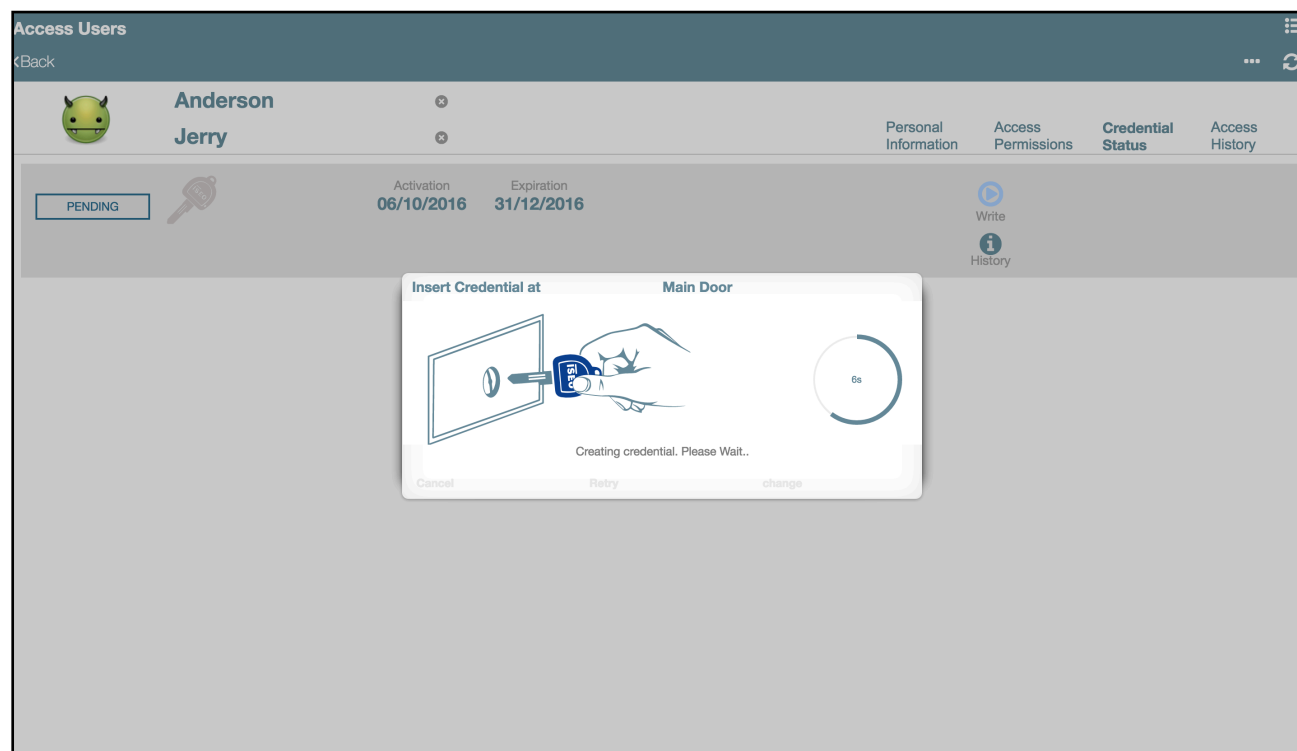
Credential write on a credential reader/writer

In addition to the Credential UID enroll process (typing the credential UID), it is possible to write immediately the F9000 key in a credential reader/writer located near your browser:

1. Insert the Access User without typing the Credential UID and select Save. You will see the credential Status page:



2. Select the **Write Credential** button a reader dialog box will appear



- insert the F9000 key inside the reader/writer: the F9000 key will be written and you will see the credential status:

Access Users

Back

Anderson

Jerry

✖

✖

Personal Information

Access Permissions

Credential Status

Access History

ACTIVE

UID

DA0296

Activation

06/10/2016

Expiration

31/12/2016

Last update

06/10/2016 11:49

Reader Information

Main Door

Validation Expires in

10h 58m

Validation Expire

06/10/2016 22:49

Last validation

06/10/2016 11:49

Main Door

History

Credential Assignment Process summary

		Credential UID	
		Yes	No
Role	Yes	Insert the Role and Type UID then Save. The Access User will program the credential at the validator.	Insert the Role and then Save. The administrator programs the credential at the local reader/writer. The Credential UID will be associated during the writing process.
	No	Insert the individual doors and Type UID then Save. The Access User will program the credential at the validator.	Insert the individual doors and then Save. The administrator programs the credential at the local reader/writer. The Credential UID will be associated during the writing process.

View Access User Details

The Access User Details page displays information for an individual Access user.

To view details for a specific user:

1. Click the dropdown menu and then click on the Access Users tab. The Access Users list displays.
2. Click the Access user you want to view. The corresponding Access User Details page displays.

The screenshot shows the 'Access Users' page with a header bar containing a back arrow, the title 'Access Users', and a menu icon. Below the header is a user profile section for 'Jerry Anderson' with a green devil icon and a dropdown menu. To the right of the profile are four tabs: 'Personal Information', 'Access Permissions' (which is selected), 'Credential Status', and 'Access History'. Below the tabs is a 'Role' section showing 'GM' with a dropdown menu. To the right of the role is a 'Credential' section showing a key icon and the value 'DA0296'. Below the role and credential sections is a 'Validity' section with two rows: 'Activation' and 'Expiration'. The 'Activation' row shows a date of '06/10/2016', a time of '08:00', and a 'Validation period' of '8 hours'. The 'Expiration' row shows a date of '06/10/2016', a time of '16:00', and a duration of '1 Days'. Below the validity section is an 'Assigned Doors' section with a search bar labeled 'Type and Enter'. Below the search bar is a list of six doors: 'Gas Refinery Plant' (Remote Site Area), 'General Manager' (General Manager), 'Main Door', 'Meeting Room' (Meeting Room), 'Operation' (Operation), and 'Research & Development' (Research and Development). Each door has a circular icon with a key and the text '24H ALWAYS'. At the bottom of the page, there is a small text '6/6 Elements'.

The Access User page is divided up into 4 tabs:

- Personal Information,
- Access Permissions
- Credential Status
- Access History

Access Permission

The Access Permissions tab displays a person's access assignments which are inserted when creating the Access User.

Personal Information and User Defined Fields

Personal information shows additional information about the user like Company, Department or other custom fields. These are Custom Fields which are defined at the setup of the system.

User Defined Fields

User Defined Fields are optional additional information about an Access User.

The User Defined Fields are visible in the system for each Access User under the Personal Information tab.

The V364 system allows up to 10 User defined fields (example: company , ID stamped on the credential if different from the UID, department , birth date, and similar other info).

Each field can be defined type as Text or Date or Number.

Text fields can hold up to 255 alphanumeric characters. (Notes is 2024 char)

These fields are optional but they are often used to refine searches in the system and filter users.

There are several functionalities around the User Defined fields that will be developed in several steps:

- Configuration of User defined fields at system configuration by Iseo Technical Support
- Import Access Users including User defined fields

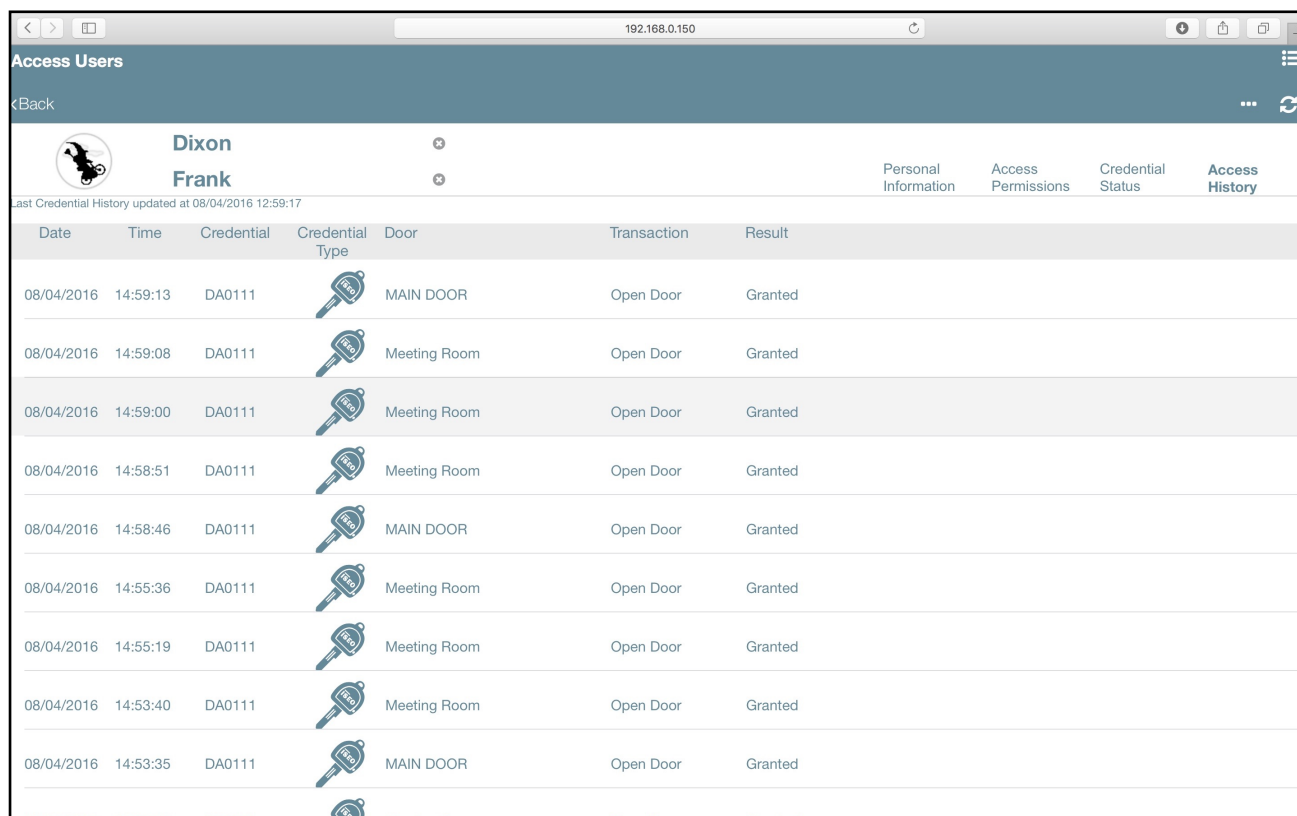
The screenshot displays the 'Access Users' management interface. At the top, there's a header bar with 'Access Users' and a back arrow. Below the header, a user profile for 'Anderson Jerry' is shown with a green alien icon. To the right of the name are two edit icons. Below the profile, there are four tabs: 'Personal Information' (selected), 'Access Permissions', 'Credential Status', and 'Access History'. Under the 'Personal Information' tab, several fields are listed: 'Company' (Green Apple), 'Location' (Milano), 'Department' (Engineering), and 'Notes' (Notes). Each field has an edit icon to its right.

Credential Status

Credential Status shows the status of the Credential assigned to the user as better indicated in the Credential Lifecycle paragraph. This includes also the date and time of the last Update of the access permissions on the credential and the last validation event.

Access History

The Access History tab displays the most recent transactions pertaining to the selected person. This are the events automatically downloaded from the credential at the validators. The Access History tab will only appear after a person has been assigned a credential. The Access events are ordered with the most recent on top.



The screenshot shows a web interface for 'Access Users'. At the top, there's a header with a back button and a menu icon. Below the header, the user 'Dixon Frank' is selected, with a profile picture and a 'More' button. A note indicates 'Last Credential History updated at 08/04/2016 12:59:17'. Below this, there are tabs for 'Personal Information', 'Access Permissions', 'Credential Status', and 'Access History'. The 'Access History' tab is active, displaying a table of access transactions.

Date	Time	Credential	Credential Type	Door	Transaction	Result
08/04/2016	14:59:13	DA0111		MAIN DOOR	Open Door	Granted
08/04/2016	14:59:08	DA0111		Meeting Room	Open Door	Granted
08/04/2016	14:59:00	DA0111		Meeting Room	Open Door	Granted
08/04/2016	14:58:51	DA0111		Meeting Room	Open Door	Granted
08/04/2016	14:58:46	DA0111		MAIN DOOR	Open Door	Granted
08/04/2016	14:55:36	DA0111		Meeting Room	Open Door	Granted
08/04/2016	14:55:19	DA0111		Meeting Room	Open Door	Granted
08/04/2016	14:53:40	DA0111		Meeting Room	Open Door	Granted
08/04/2016	14:53:35	DA0111		MAIN DOOR	Open Door	Granted

Managing Access Users and the Credential Lifecycle

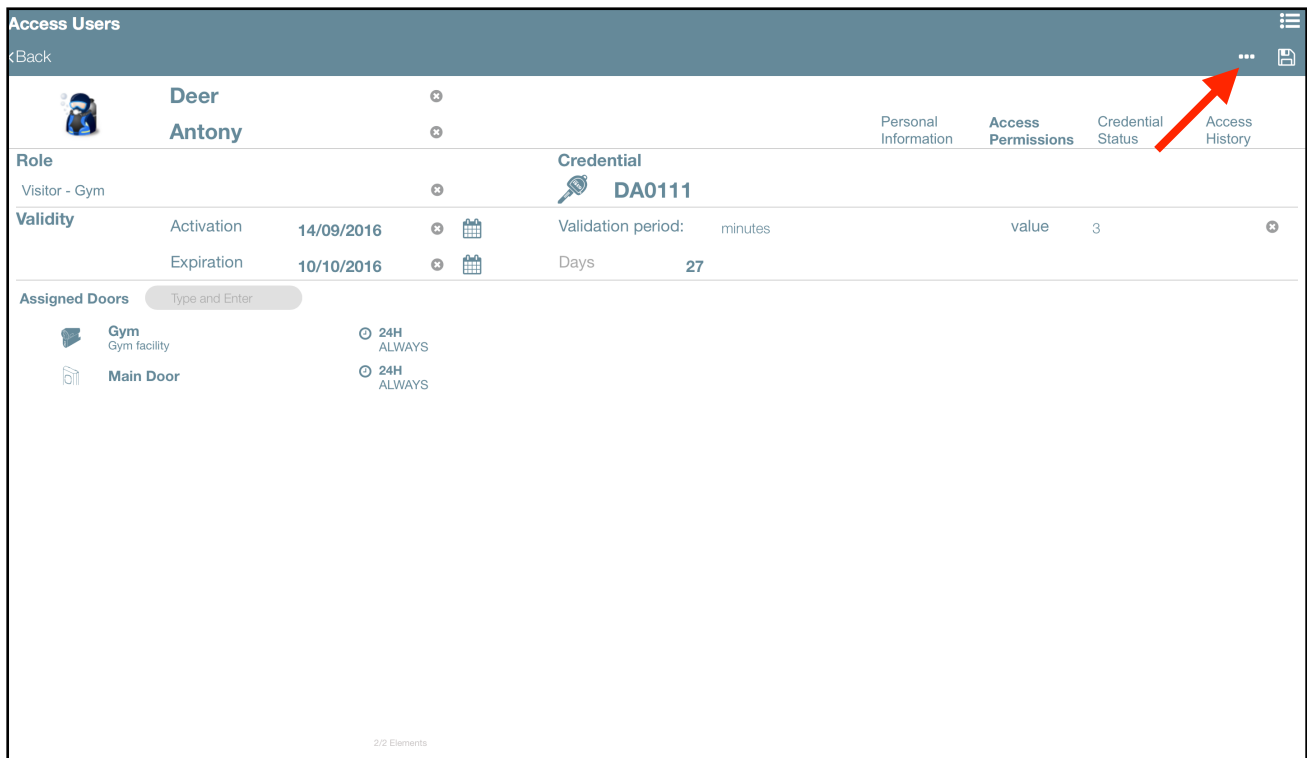
Once a user is created, his/her information can be updated at any time. The Credential can be suspended or revoked from the system and the Access User without an active credential can also be deleted completely from the system.

To edit a user:

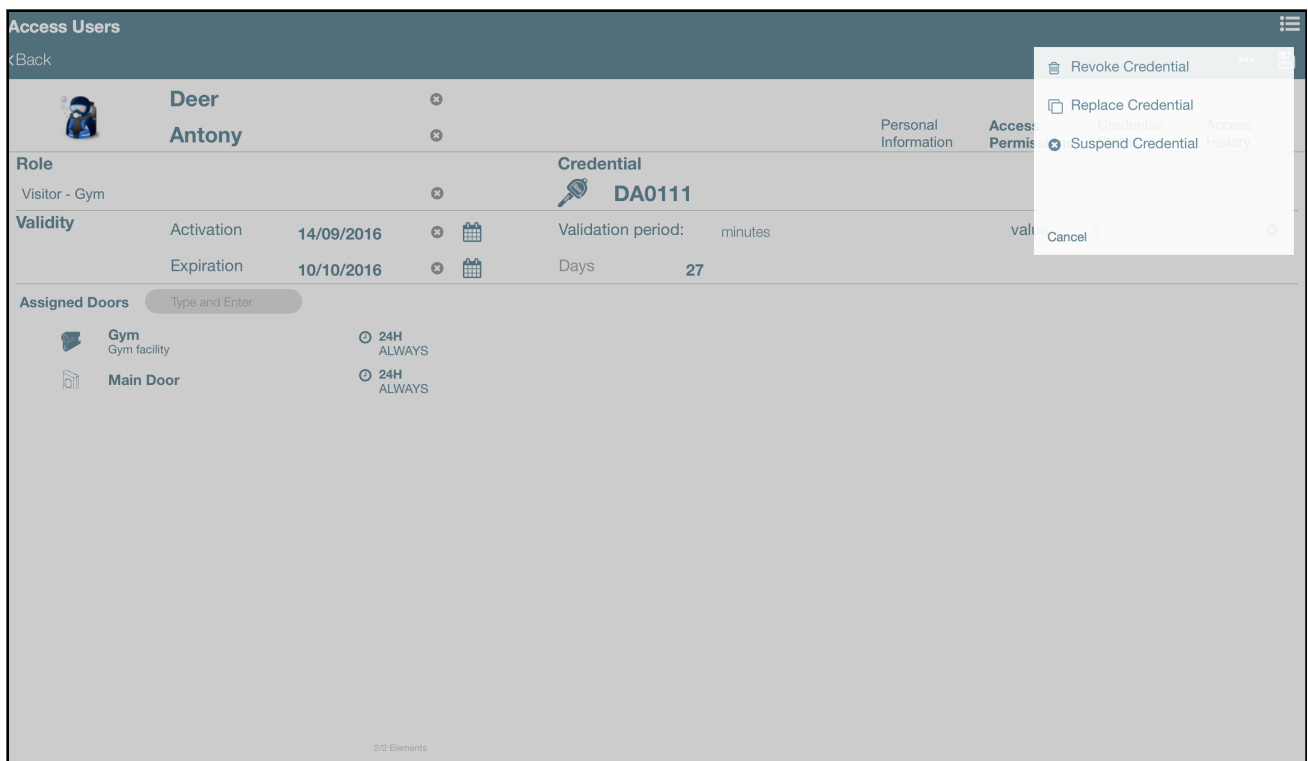
1. Click Access User Management in the dropdown menu then click on the Access Users tab. The Access Users list displays.
2. Click the Access User you want to edit. The Access User Details page displays.
3. All fields on this page can be edited. Enter the desired changes using the guidelines for creating a user, described above.
4. Click Save. You are returned to the User List page.

The changes will be written in the Access User credential at the next validation time. You can check if a user has updated the credential looking into the Credential status. For example To Update means that the credential data are non current with the access permissions modification in the V364 made by the system administrator.

Additional Actions on the user can be performed selecting the More (...) button during Access User editing



obtaining the for example the following options



The possible options are depending from the actual Credential Status in the credential lifecycle.

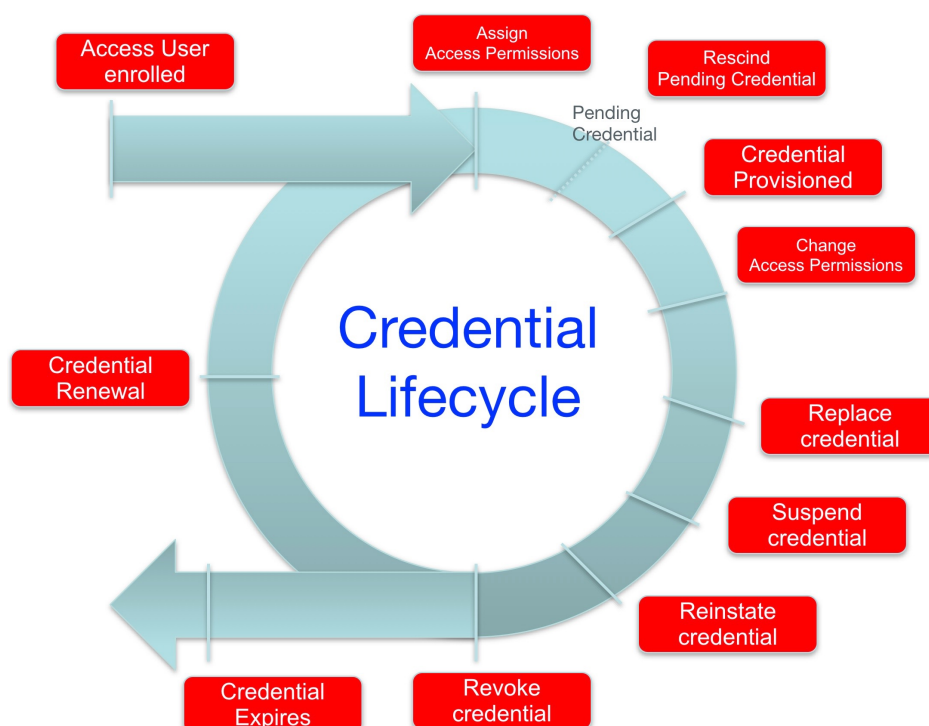
This is the complete list of the Actions on the Access Users and credentials:

Actions	description
Enroll Access User	Access User data entered into the system without defining the access permission (just save the Access user from personal Info or imported from a file .CSV)
Assign Credential	Access user access permission saved in the system (save the Access user from Access permission) : a logical credential has been created but it is not yet written in the physical support
Provision Credential	Access user permission are loaded into the physical credential (the credential data are written in a physical support by the system administrator)
Auto Provision Credential	Access user permission are loaded into the physical credential the credential data are written in a physical support by the User with UID enrollment
Rescind credential	Remove a credential assigned to a user. The physical credential has not yet written for the first time but a logical credential has been allocated in the system. It is the inverse operation of assigning a credential: the user will remain in the database but no credential data is associated to him/her. The system continues to memorize the access permission provided to the user.
Delete Access User	Possible only after rescind or over an expired credential. The User will be removed from the database and will not be shown anymore in the access user list.
Change Access Permissions	The administrator changes the users access permissions. The Access Users need to have access to a different set of doors or different time schedules or a renewal (extend validity) due to expiration The system will not record the update only of the Personal Info.
Suspend	Suspend temporarily a credential
Reinstate	This action will put back in the credential in the system
Revoke	Disable the credential from the Credential database. The credential will not open any ONLINE door The credential might still open the OFF LINE doors if the Revoke action occurred while the credential was active during the validation period. If Revoke occurred during the validation period than optionally you can ERASE the credential (if you have it) or create a Black List credential (if you do not have it = not returned credential)
Replace credential	This credential will replace a lost credential. The replacement card will put in black list the lost credential while opening the door.
Credential Update	The credential access rights are updated
Erase credential	This action will erase the content of a valid credential restoring the credential to Factory mode. A credential can be erased on a reader or also during validation.
Create Black List credential	The Blacklist credential will put in the door lock black list the credential you want to revoke

You can get complete details about the actions reading the credential lifecycle.

The Credential Lifecycle

There is a lifecycle associated within each Access User and Credential created. The V364 system allows access users to be given access to particular areas and the management of the user lifecycle events associated with the credentials by the system administrators.



During the Access User lifecycle the physical credential data should follow any modification made by the system administrator in the V364 database.

However the credential can not be immediately updated, because it cannot be always reached from the system immediately.

The V364 system is able to provide information about the physical credential status by 2 different attributes:

- Credential Lifecycle Status
- Credential Data Synchronization

Credential Lifecycle Status

It is the credential status related to the validity of the access permissions in the system:

Credentials lifecycle status	Description
Active	The credential is Active and validated in the system. The credential can open the doors defined in the access permissions
Not Validated	The credential is active but not validated. The validation period has expired and to open the door the credential needs to be validated again.
Expired	The credential has reached its expiration date
Not yet Active	The credential has been issued but it is not yet active as the activation date is later than the current date
Active to Suspend	A suspension has been requested while the credential is still Active therefore the credential is still valid on the offline doors up to the validation expiration. A residual security risk exists for this credential.
Active to Revoke	A revoke has been requested while the credential is still Active therefore the credential is still valid on the offline doors up to the validation expiration or until a black list credential disables it from all the related offline doors. A residual security risk exists for this credential.
Revoked	The credential has been revoked from the system - the credential is not valid to any door and can be assigned to a different access user
Erased	The credential has been returned to the security manager which has erased the data on it setting the credential to factory mode. If the credential is revoked and is passed into a validator by anyone then it becomes Erased.
Suspended	The credential has been temporarily disabled in the system
Suspended to Activate	A Reinstatement has been requested while the credential is Suspended therefore the credential at next validation will be valid (active) on the offline doors up to the validation expiration.

Credential Data Synchronization

This attribute informs about the synchronization of the data between the credential physical support and the logical credential data inside the V364 system in the Atlas Master. For example the administrator has changed the user access rights but the credential is still in the hands of the user and requires an update at the validator.

Status	Icon	meaning
<i>not assigned</i>		<i>no physical credential has been assigned to the User. It is not possible to have access to the credential status tab</i>
Pending	Pending	A credential as been assigned to the access user but it has not been redeemed by physically writing it into a credential support. The credential is reserved in the system but has not been actually provisioned to the user. The logical credential has been created and saved into the system but it has non yet written into the physical support.
Current	(nothing)	The physical credential is up to date. The system administrator has modified the access permission of the Access user and these modifications have been also written in the credential (Access Permission Updated). The logical credential data has been written in the physical support and the logical and physical credential are synchronized (credential provisioned or issued)
To Update	To Update since "Time"	The physical credential requires an update. The system administrator has modified the access permission of the Access user and these modifications have NOT YET been also written in the credential (Access Permission are to Update). The logical credential has been modified and and the physical support has non been updated. To Update show also the elapsed time since the request of Update: it is the difference from the NOW_Time and the Request_to_update_Time

Therefore to better track all the events on the credential lifecycle we need to consider these actions from the system when a credential is presented to an online reader:

- credential Update
- credential Validation

Following we will see in in detail each administrator action and its impact on the administration transaction database record.

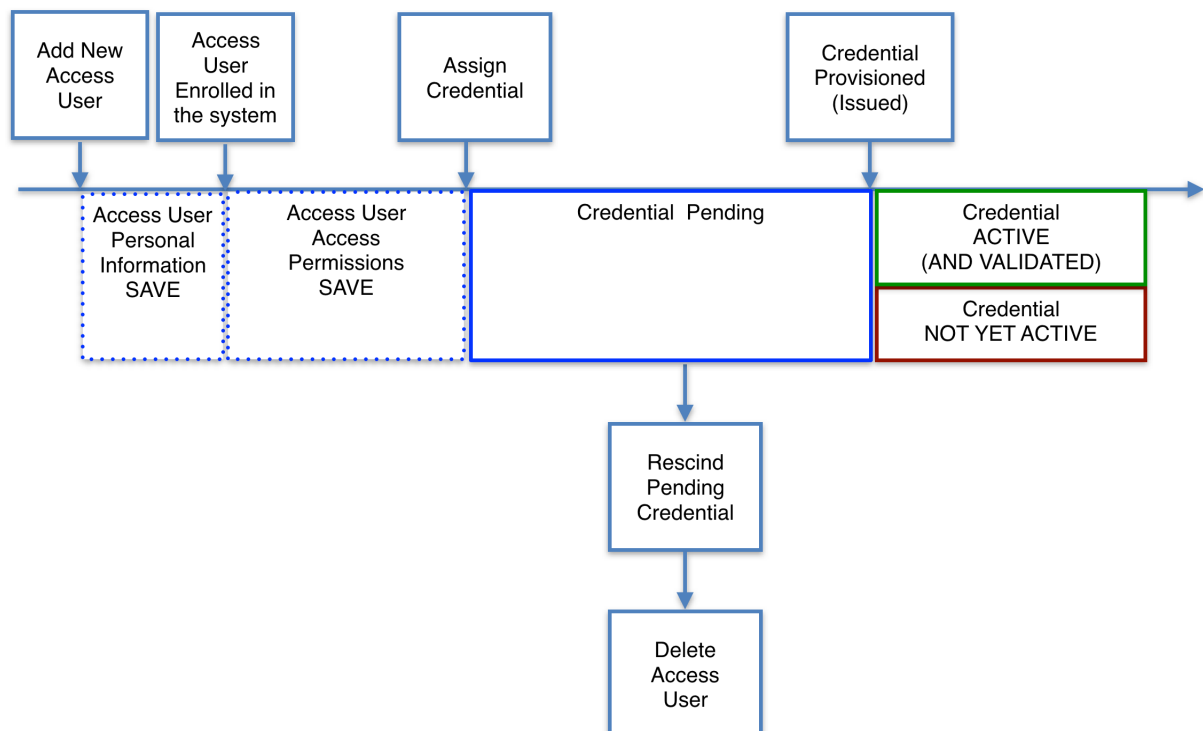
Enroll Access Users

The system administrator **Enrolls an Access User** just entering the user personal information and SAVE from Personal Information or importing a .CSV file just with user personal data.

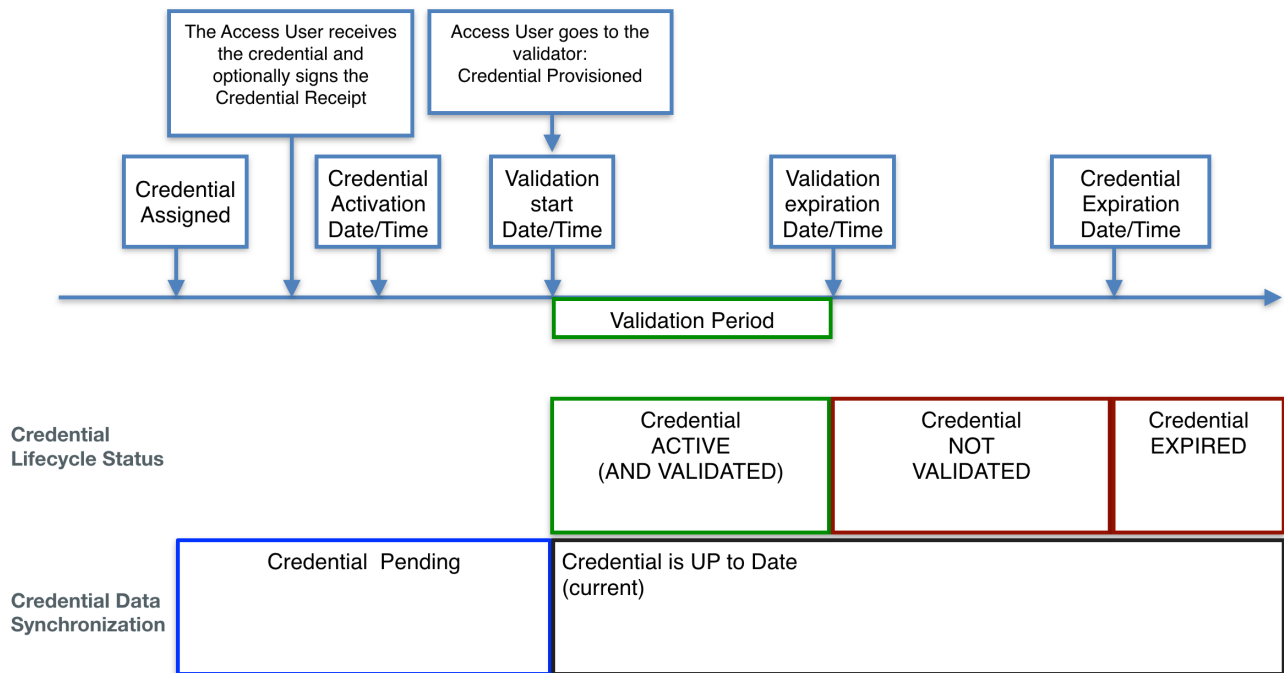
Then system administrator **Assigns a Credential** providing access rights and SAVE from the Access Permission.

At this point there is a logical **Pending Credential** for the Access User: a credential has been reserved into the System for the user but still the Credential Data have not been written into the credential.

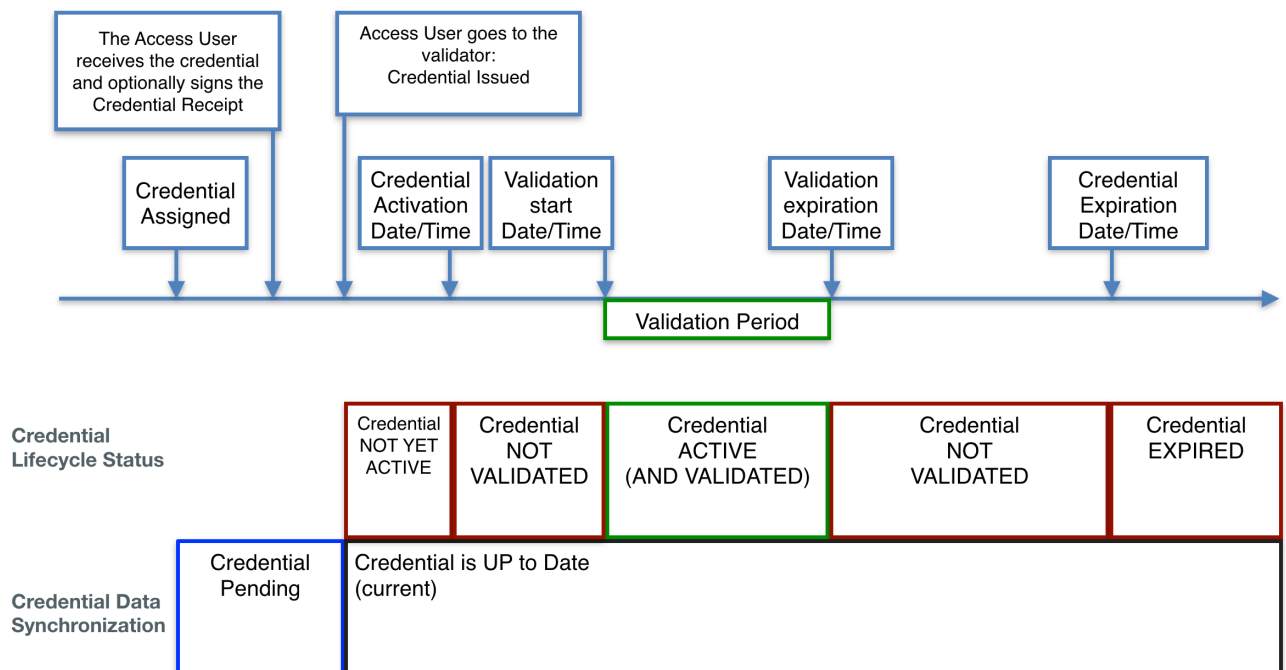
Pending Credential	Actions from administrator	Result
Access User entered into the system but the physical credential is not yet written with the access privileges data. In the database there are access privileges (Credential Data) pending to be actually written into a physical support.	Provision the credential (Write the credential = Issue the credential)	The credential will be written in the Validator or credential programmer and becomes Active (credential is provisioned or Credential Issued). This action can be immediate
	Rescind credential	The Pending credential will be rescinded. The user will remain in the database but no credential data is associated to him/her. The system continues to memorize the access permission provided to the user.
	Delete User	Possible only after rescind. The User will be removed from the database and will not shown anymore in the access user list



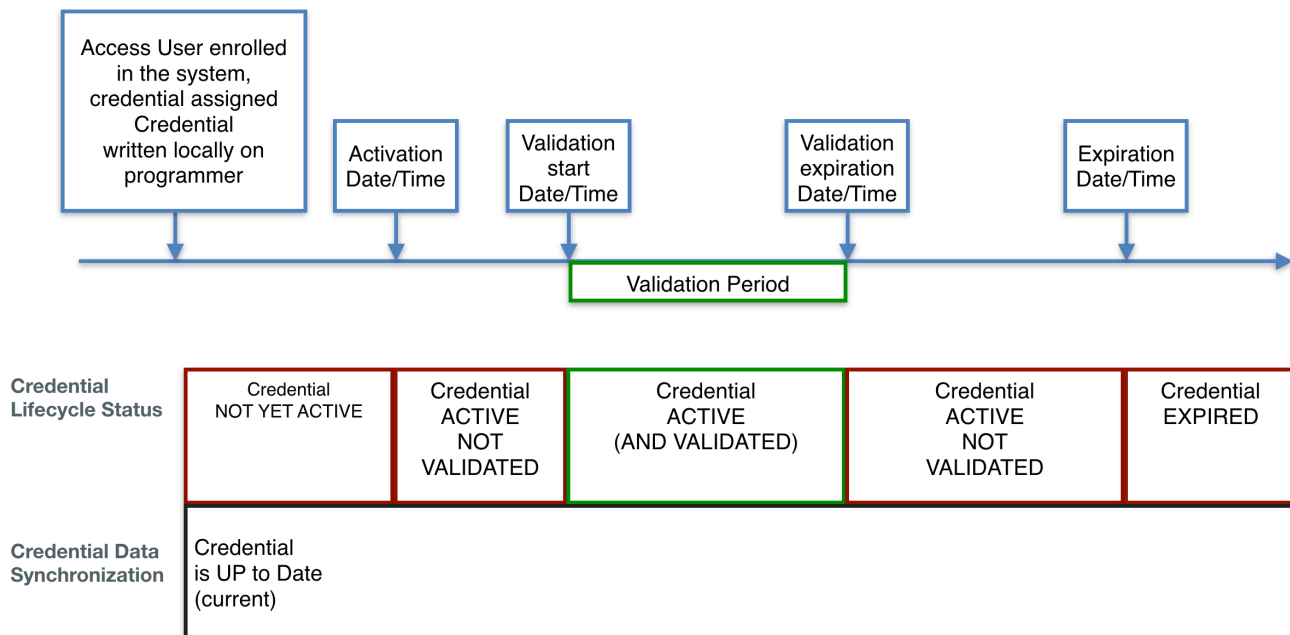
Enroll Access User with UID (case 1)



Enroll Access User with UID (case 2)



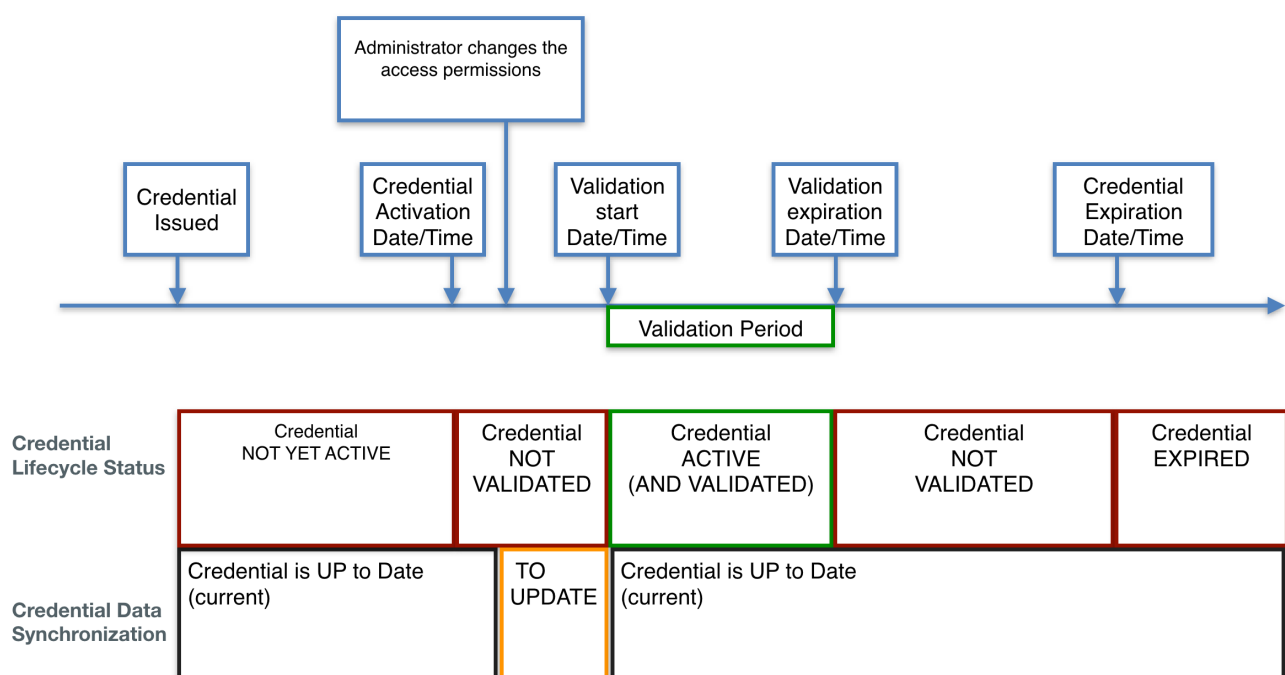
Enroll Access User with immediate write at the programmer



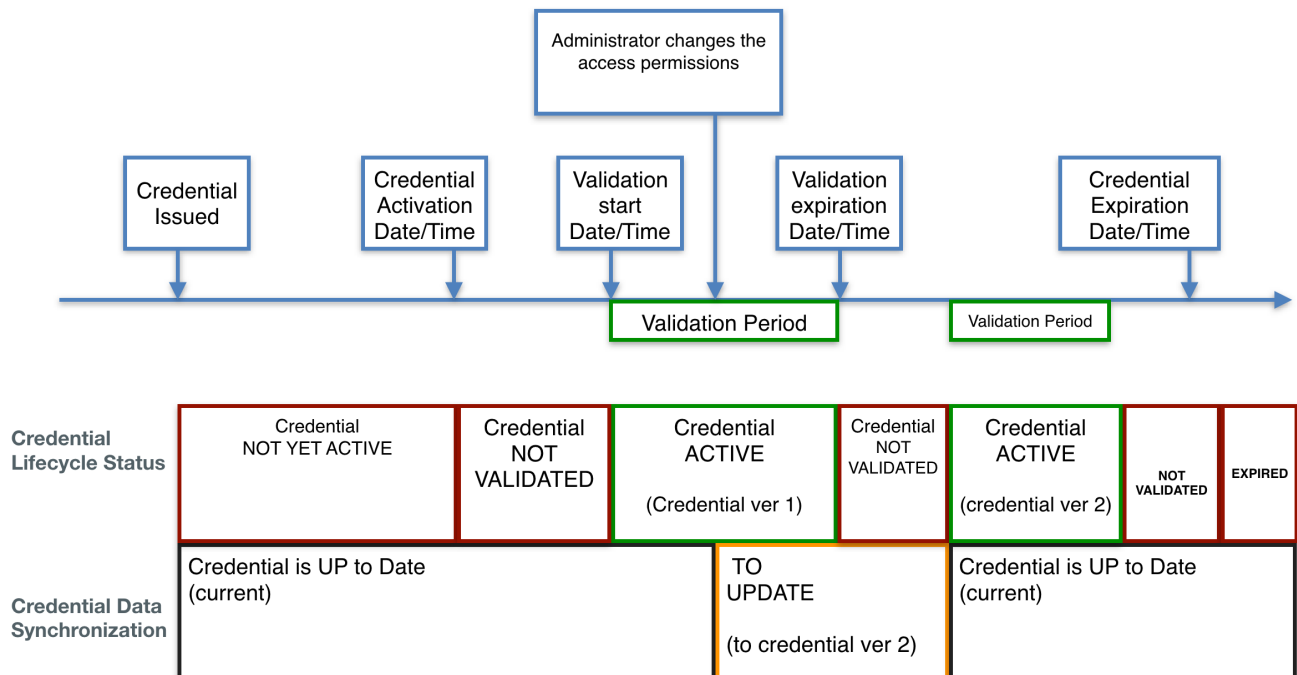
Change Access Permissions

Event	Actions from administrator	Result
Change Access Permission: The Access Users need to have access to a different set of doors or different time schedules	Edit the Access User and modify the access privileges and SAVE	The credential will be updated in the Validator with the new access privileges when the Access User will pass at the validator.

Change Access Permissions outside the validation period



Change Access Permissions during the validation period



Suspend and Reinstate

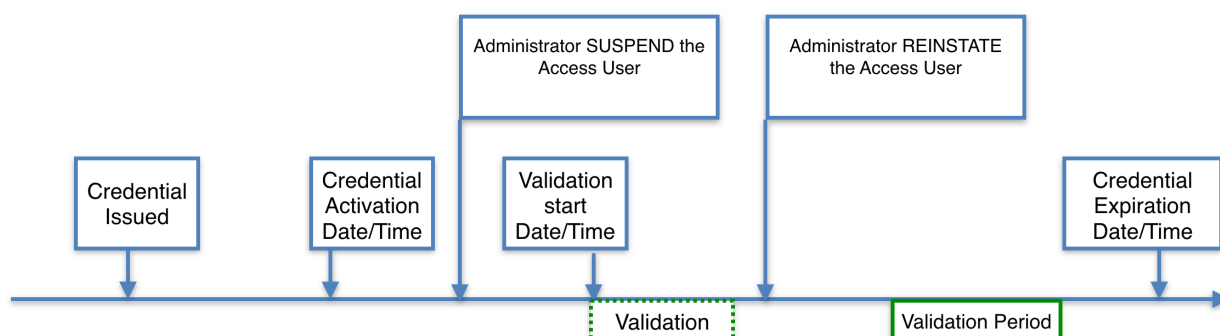
Suspend Access User

Event	Actions from administrator	Result
Suspend means to stop someone for a short period of time - this can happen if the user will be absent from the company for a business trip or similar situations.	Suspend Credentials	If the credential will be presented at the Validator the validation will not take place. Therefore the credential is temporarily invalid (Suspended) until the administrator will not reinstate it (rehabilitate the credential)

Reinstate Access User

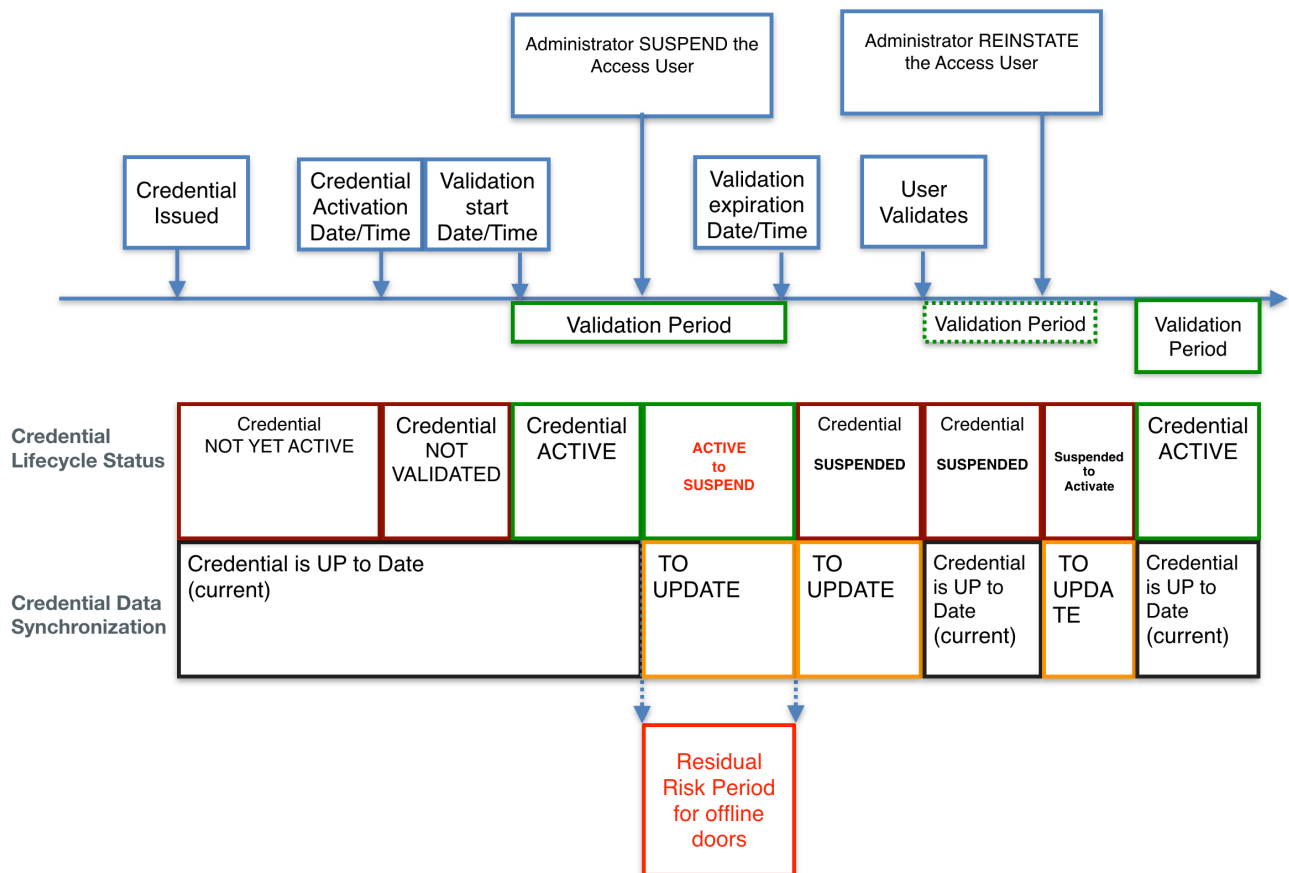
Event	Actions from administrator	Result
Reinstate means to put someone back in a job or position that had been taken away.	Reinstate Credentials	If the credential will be presented at the Validator the validation will occur.

Suspend outside the validation period



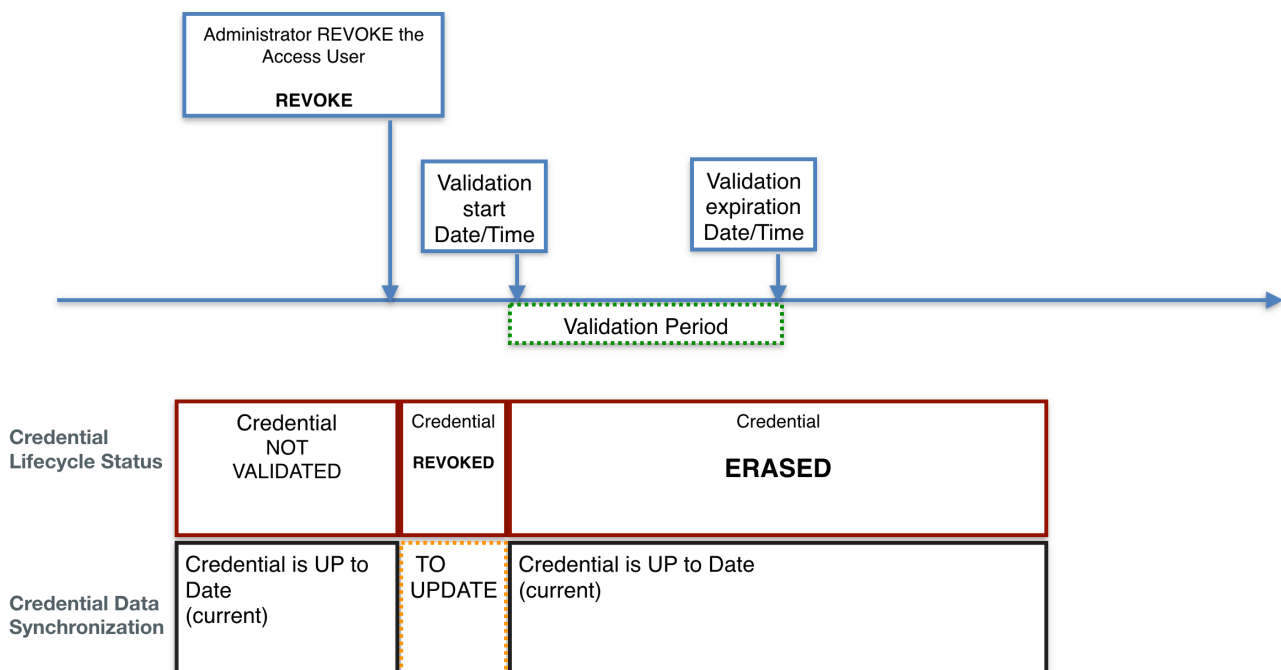
Credential Lifecycle Status	Credential NOT YET ACTIVE	Credential NOT VALIDATED	SUSPENDED	SUSPENDED	SUSPENDED to ACTIVATE	Credential ACTIVE	NOT VALIDATED	EXPIRED
Credential Data Synchronization	Credential is UP to Date (current)		TO UPDATE	Credential is UP to Date (current)	TO UPDATE	Credential is UP to Date (current)		

Suspend during the validation period

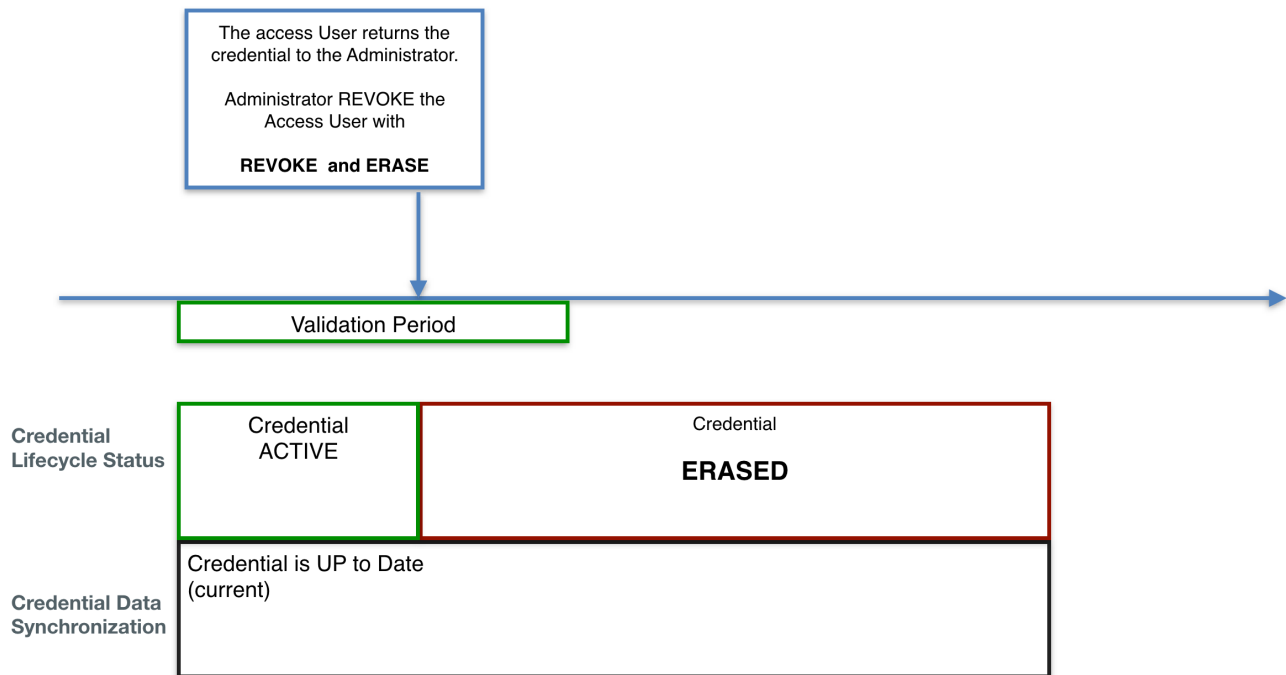


Revoke

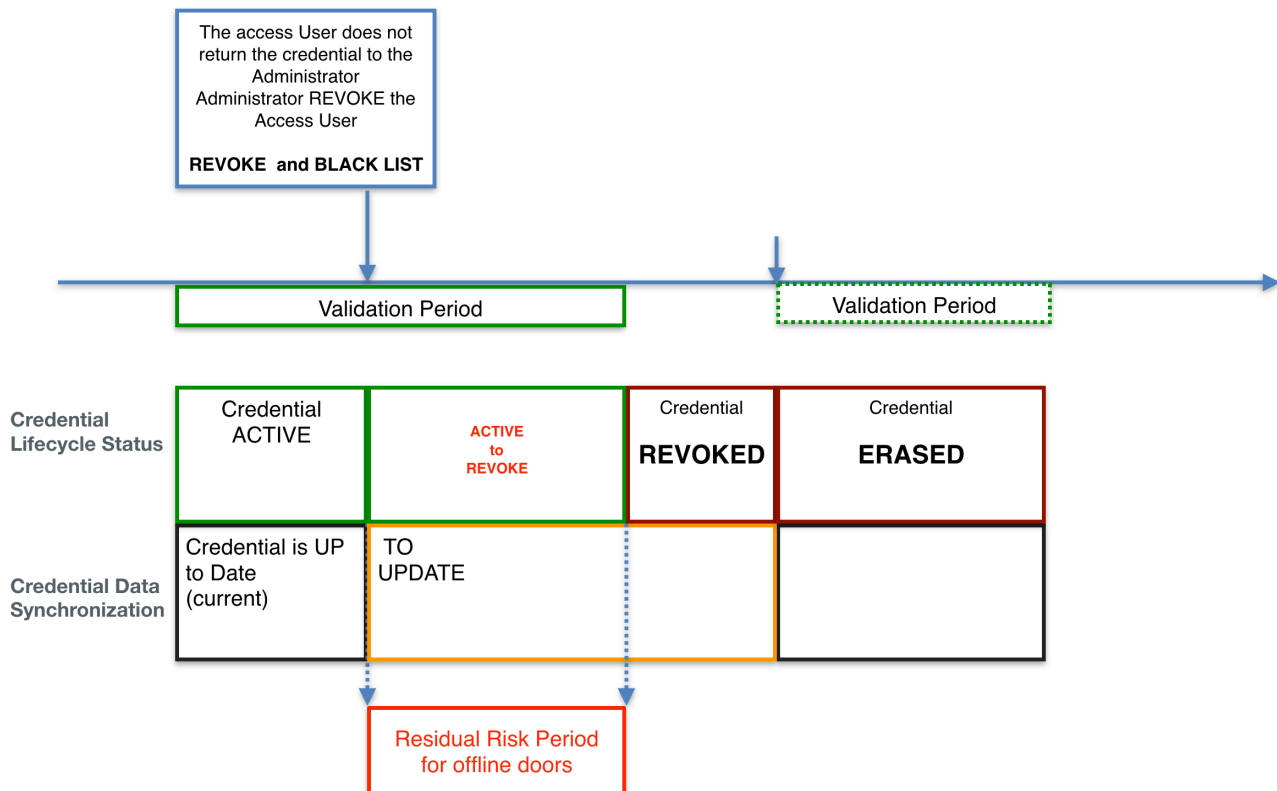
Event	Actions from administrator	Result
The credential status shows the credential is not Active (not validated) then a revoke only can be done.	Revoke Only	This action disable the credential from the database. If the credential is presented to the validator then it will be erased If the credential is returned, then it can be assigned to a new access user.
The Access User has left the organization and <u>has returned the credential</u> to the system administrator. The credential is Active.	Revoke Credential + Erase Credential (clean)	The credential returned can be erased therefore can be assigned to a new access user.
The User has left the organization and <u>has NOT returned the credential</u> . The credential is Active.	Revoke Credential + Black List Credential	This action disable the credential from the Credential database. and will put the NOT Returned credential in the door blacklist. The blacklist credential needs to pass in all offline doors to invalidate the NOT returned credential programming the Blacklist in the door.



Revoke credential during validation period with credential returned



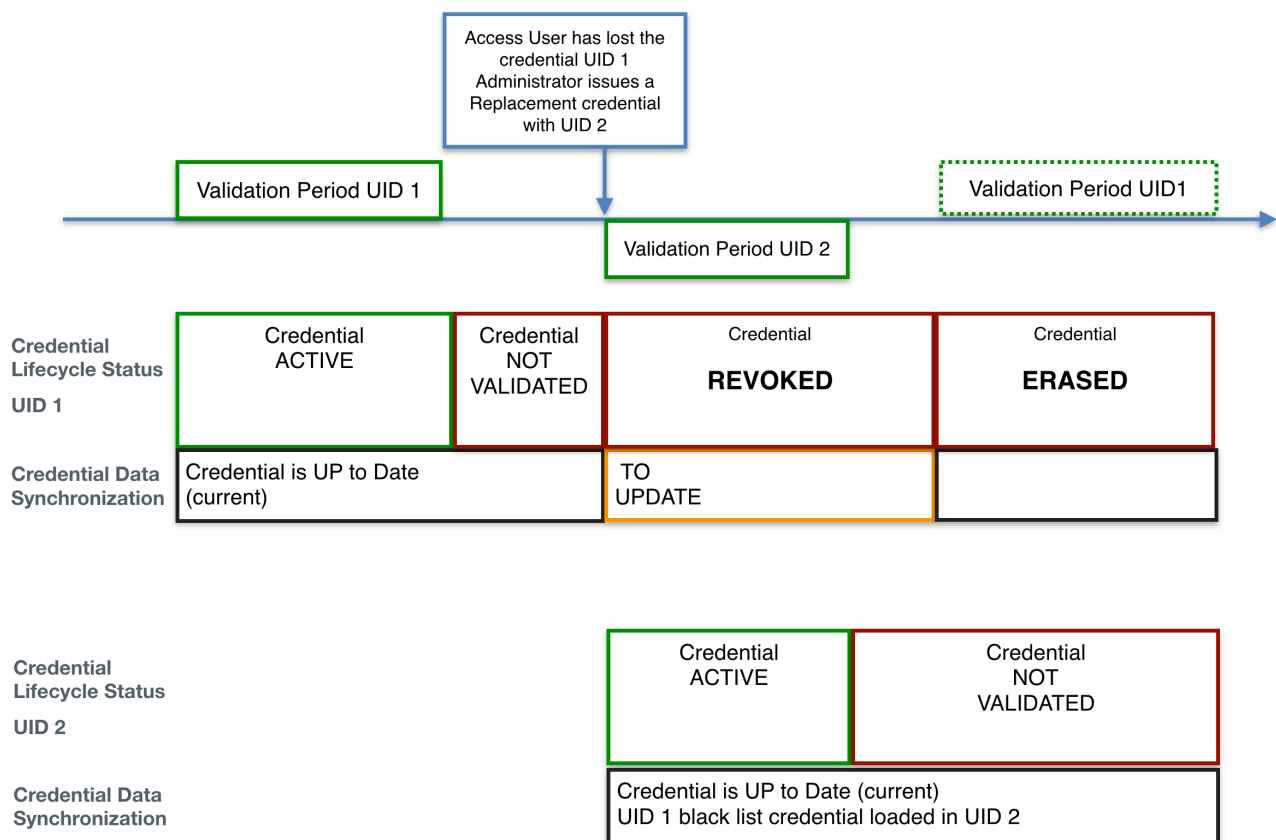
Revoke credential during validation period with credential NOT returned



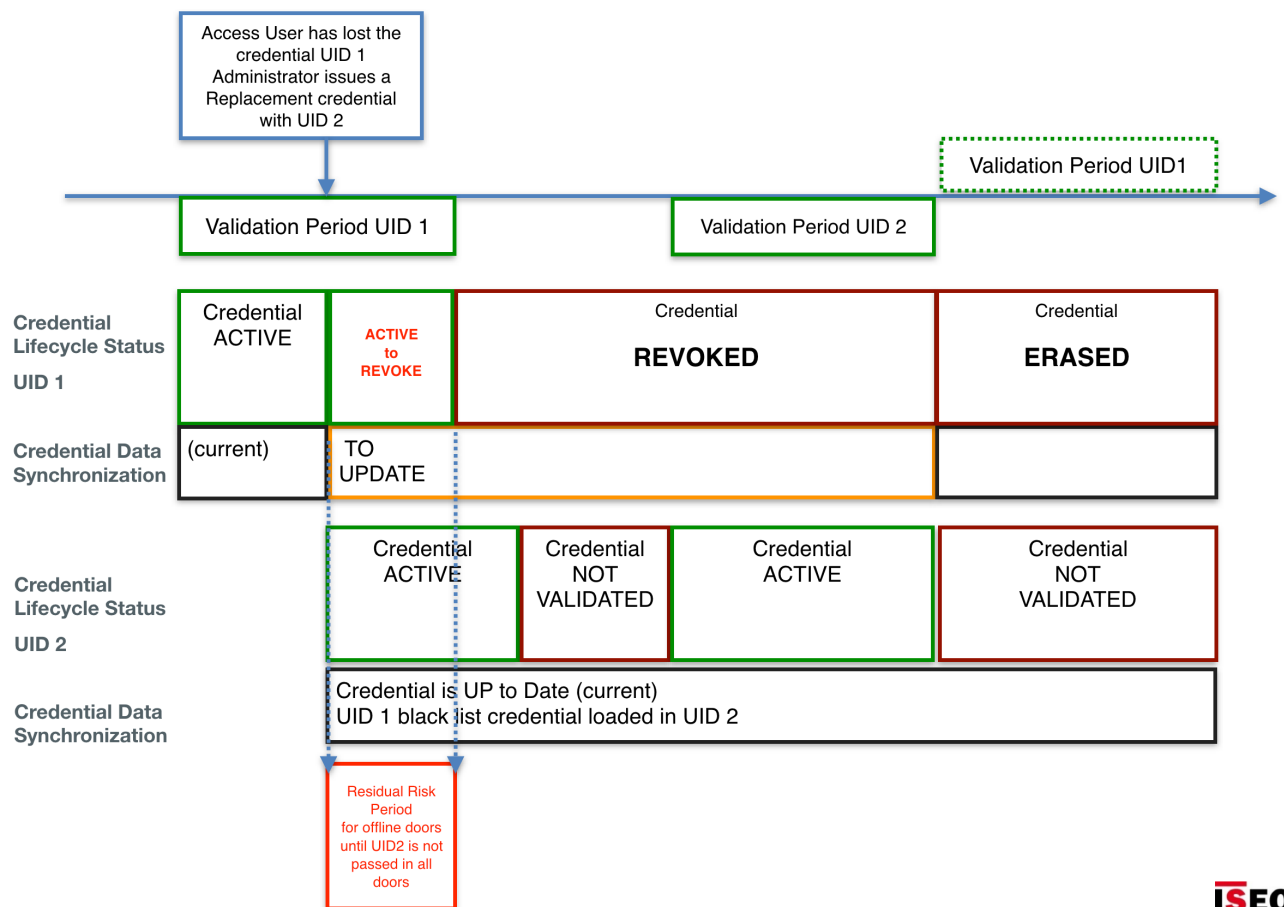
Replace Credential

Event	Actions from administrator	Result
Lost Credential: The Access user has lost the credential. This can happen if someone has stolen it from the user.	Create a Replacement Credential	A new credential will be issued for the User. While the Access user will open the door with the new credential, this will invalidate the lost one putting the lost one in the credentials blacklist.

Replace credential outside the validation period

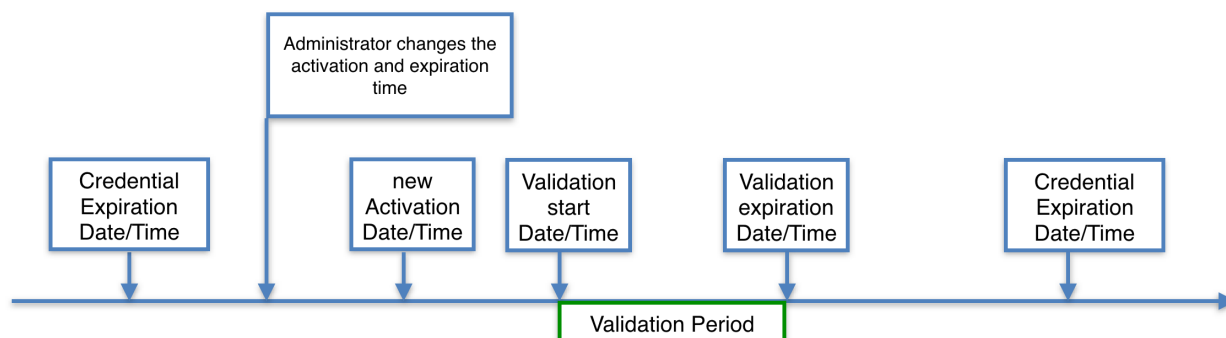


Replace credential during validation period



Expired Credential and Renewal

Event	Actions from administrator	Result
Expired Credential	Renewal Credential Edit the user and modify the expiration Date extending the credential period of Validity	the credential will be updated in the Validator with the new access privileges
	Delete the User	The User will be removed from the database and will not shown in the access user list



Credential Lifecycle Status	Credential EXPIRED	Credential NOT YET VALID	Credential NOT VALIDATED	Credential ACTIVE (AND VALIDATED)	Credential NOT VALIDATED	Credential EXPIRED
Credential Data Synchronization	Credential is UP to Date (current)	TO UPDATE		Credential is UP to Date (current)		

Deleting Access User

User can be deleted from the database only if they do not have a valid credential assigned. Users with expired credential, Revoked Credential or not assigned credential (after rescind) can be DELETED from the database

1. Click the Access Users tab from dropdown menu. The Users list displays.
2. Click the Access User you want to delete. The associated User Details page displays.
3. Select More (...).
4. Click Delete. A warning message asks you to confirm that you want to delete the user.
5. Click OK. You are returned to the Users list with the deleted user removed.

WARNING:

Once a user is deleted, the user cannot be undeleted. To add the user back, he or she must be re-created as a new user.

If the user has a credential (Expired or Revoked) then it will become unassigned and can be assigned to another user at a later date.

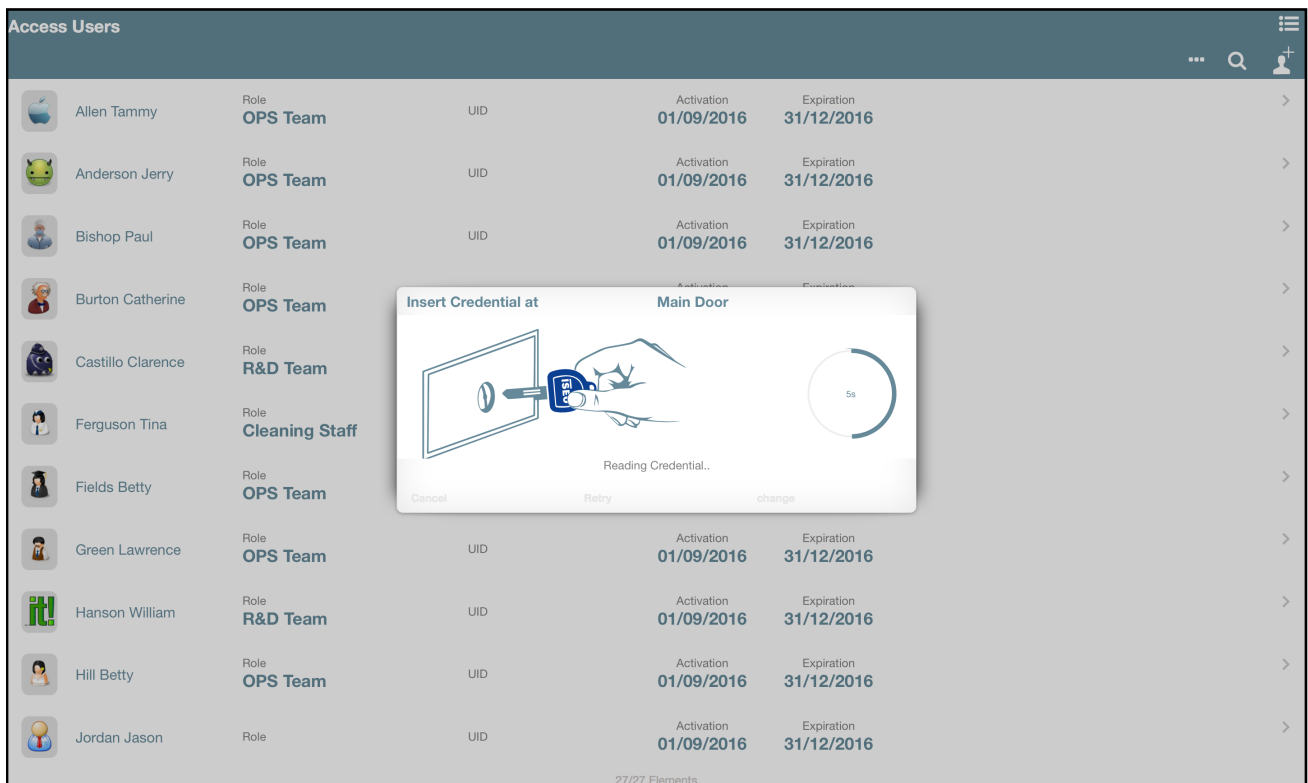
Access User Status in the Database

Status	Meaning	Details
Available in the User List	The User is visible in the User List regardless the credential status assigned to him	Users with Credentials Expired , Revoked or not assigned can be DELETED from the list The users visible in the user list are counted for the credential license user even if they have an expired credential.
Deleted	The user is not visible anymore in the user list.	

Read a Credential

This operation allows you to read the content of a credential and display the associated Access User data.

1. From the Access User management dropdown menu, click on Access Users. The access user list displays.
2. Select Read Credential inside the ... button
3. Put credential into the credential reader/writer



You have 10 seconds for inserting the credential into the reader.

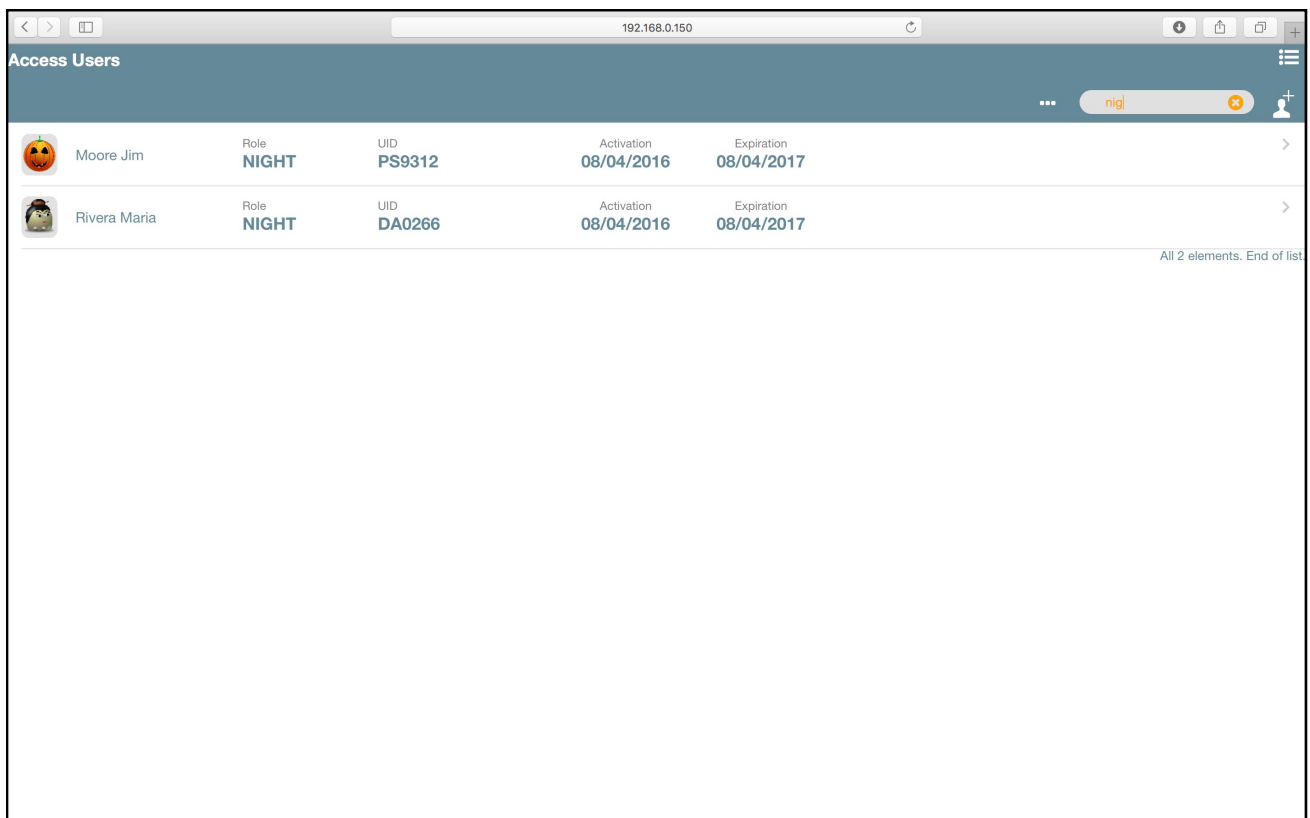
In case you were not able to put it in the reader a timeout will expire and then you can:

- Cancel the operation
- Retry
- Change the reader and select a different one

In case you select a different reader this preference will remain until the end of the session (logout).

Searching for an Access User

1. Click the Menu dropdown and select Access User Management then click on the Access User tab. The Access User list displays.
2. Click the Lens search and insert the text for searching in the any of the Access User Fields (First name, Last Name, Credential UID, Role, Personal Information fields,...)
3. All the Users containing the typed string will be displayed. The lens in orange informs that a filtering is active with a specified string.



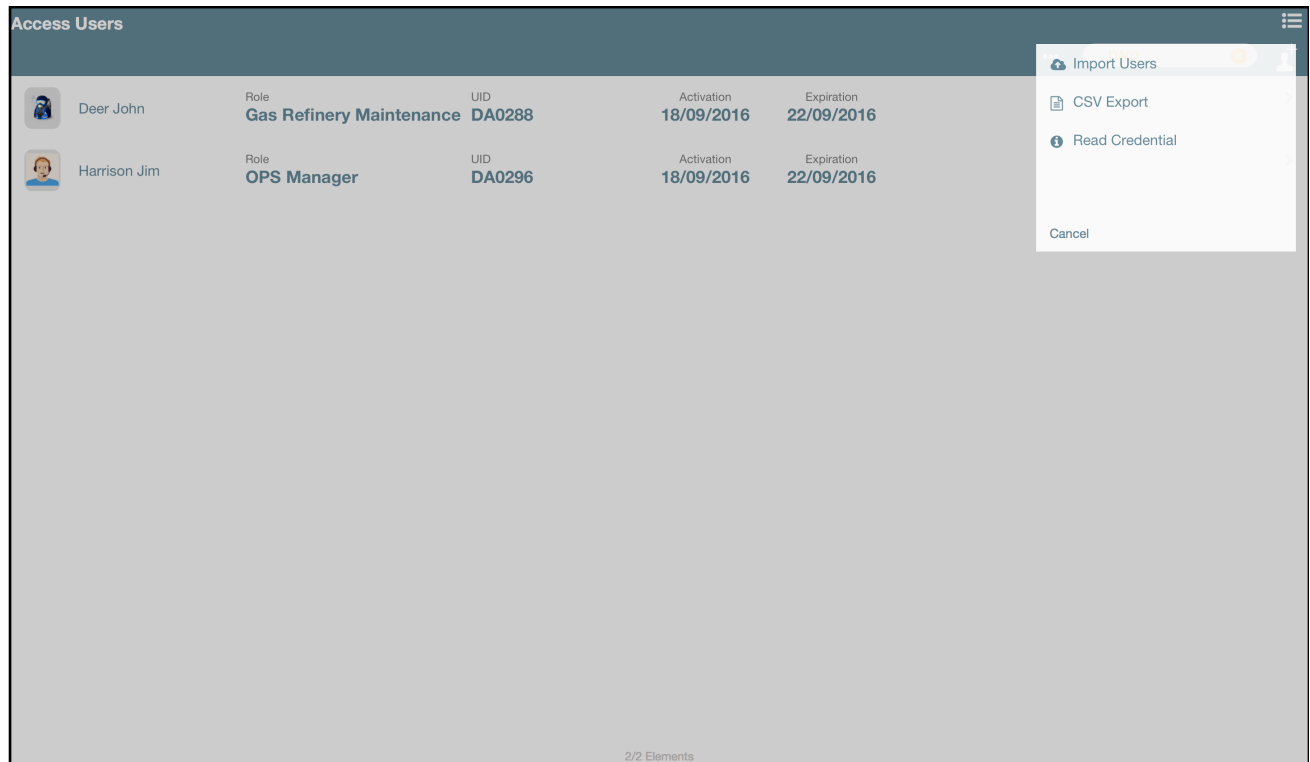
The screenshot shows a web application interface titled "Access Users". At the top right, there is a search bar with the text "nig" entered, highlighted in orange, indicating an active filter. Below the search bar, a table lists two users. The table has columns for a user icon, name, role, UID, activation date, and expiration date. The first user is Moore Jim, with role NIGHT, UID PS9312, activation date 08/04/2016, and expiration date 08/04/2017. The second user is Rivera Maria, with role NIGHT, UID DA0266, activation date 08/04/2016, and expiration date 08/04/2017. At the bottom right of the table, it says "All 2 elements. End of list".

	Role	UID	Activation	Expiration
 Moore Jim	NIGHT	PS9312	08/04/2016	08/04/2017
 Rivera Maria	NIGHT	DA0266	08/04/2016	08/04/2017

The users displayed in the list can be exported into a .CSV file

Export User List in .CSV file

1. Click the Menu dropdown and select Access User Management then click on the Access User tab. The Access User list displays.
2. Click the ... and select .CSV export



The screenshot shows the 'Access Users' interface. It features a table with two rows of user data. A dropdown menu is open on the right side of the table, showing options: 'Import Users', 'CSV Export', 'Read Credential', and 'Cancel'. The 'CSV Export' option is highlighted.

	Role	UID	Activation	Expiration
Deer John	Gas Refinery Maintenance	DA0288	18/09/2016	22/09/2016
Harrison Jim	OPS Manager	DA0296	18/09/2016	22/09/2016

2/2 Elements

3. A .CSV file will be generated containing all the Users in the view.
4. The .CSV will contain the following columns:

Field	Description
&Lastname	Last Name
&Firstname	First Name
&Role	Role
&UID	credential UID assigned to Access User
&email	email
&activationdate	activation date
&expirationdate	expiration date
&validation	Validation mode (0 = no validation, 1 Minutes, 2 Hours, 3 Days)
&validperiod	validation period
&usrfield01	User defined field #1 (Company)
&usrfield02	User defined field #2 (Department)
...	
¬es	Notes
&uniqueid	Unique ID created by the V364 system for the user Used to identify the user in import with UPD
&opeCode	Operation Code (ADD/UPD) for the operation import Users: ADD = creates a new user UPD = Updates User specifying the &uniqueid field
&picture	base64 string image

Import Access User data

The V364 supports importing user data from Comma Separated Value (CSV) File Format files. These files are easily created by many applications, including spreadsheet or simple database applications.

The import of the .CSV allows:

- The creation of new access Users (ADD operation)
- The update of and existing Access User UPD operation)

Be sure to use ; as a field separator when exporting a file from another application or tool for import into the V364.

Format requirements for imported .csv files

Imported files need to be in the following format:

Field	Description
&Lastname	Last Name
&Firstname	First Name
&Role	Role
&UID	credential UID assigned to Access User
&email	email
&activationdate	activation date
&expirationdate	Activation Time
&validation	Validation mode (0 = no validation, 1 Minutes, 2 Hours, 3 Days)
&validperiod	validation period
&usrfield01	User defined field #1 (Company)
&usrfield02	User defined field #2 (Department)
...	
¬es	Notes
&uniqueid	Unique ID created by the V364 system for the user Used to identify the user in import with UPD
&opeCode	Operation Code (ADD/UPD) for the operation import Users: ADD = creates a new user UPD = Updates User specifying the &uniqueid field
&picture	base64 string image

As each column is identified by a field key &fieldname you might avoid to import some columns. The minimum required are &lastname, &firstname, &opecode.

To import Access User .CSV File:

1. From the Access User management dropdown menu, click on Access Users. The access user list displays.
2. Select import user inside the ... button
3. Browse for the .CSV file in your computer ,the first line of the file is used as header describing the fields of the file. If you are importing the Roles these must be already present already in the V364 System



Import Operating codes

Operation Code (ADD/UPD) for the operation import Users:

ADD = creates a new user

UPD = Updates User specifying the &uniqueid field

Credential Receipt

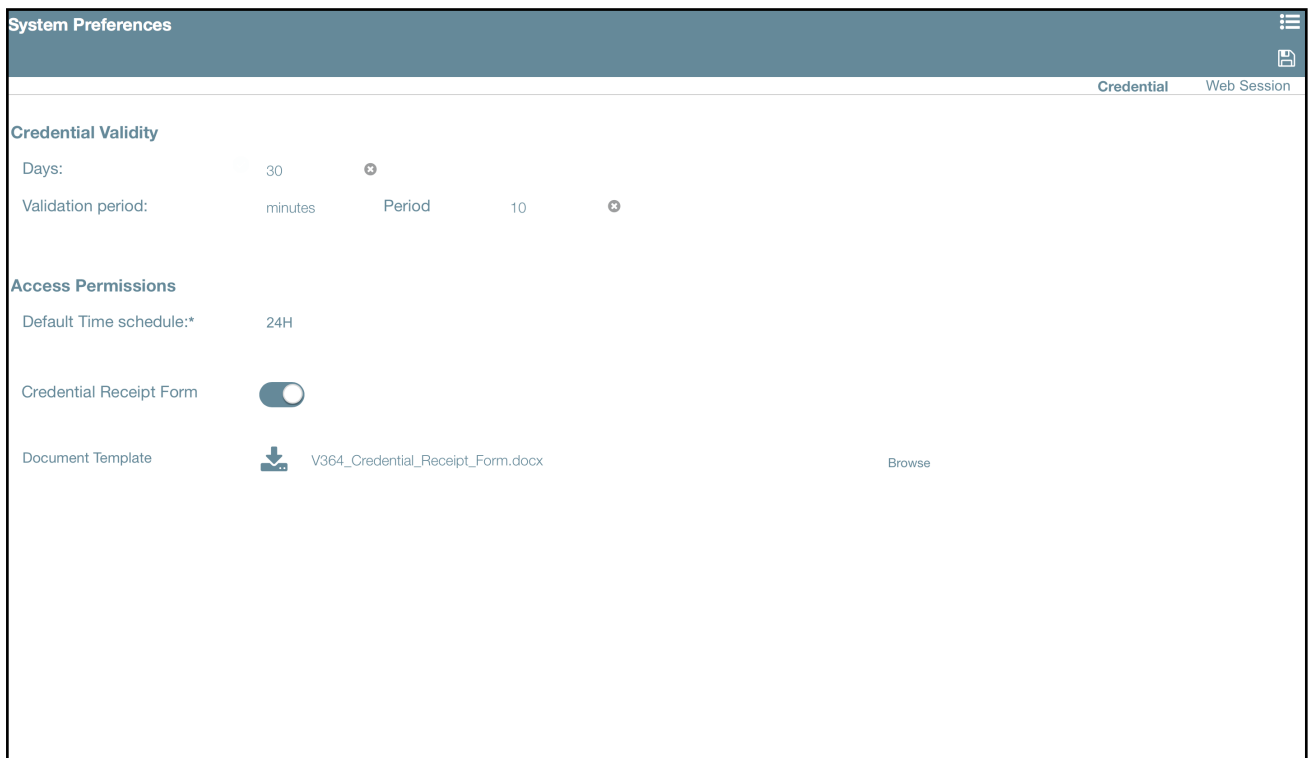
The need of most organization is to have an acknowledge from the Access User of having really physically delivered a credential.

Therefore it is convenient to have the possibility inside the Access User form to print a Credential Receipt Form and ask the signature to the Access User.

The Credential Receipt Form should be customizable in order to allow the organization to write the form upon its own needs.

Credential Receipt Form Configuration

1. From the Access User management dropdown menu, Select the Utilities tab
2. click on from the System Preferences you will get



The screenshot shows the 'System Preferences' window with the 'Credential' tab selected. The 'Credential Validity' section includes 'Days' set to 30 and 'Validation period' set to 10 minutes. The 'Access Permissions' section shows 'Default Time schedule:*' set to 24H. The 'Credential Receipt Form' toggle is turned on. The 'Document Template' field shows a download icon, the filename 'V364_Credential_Receipt_Form.docx', and a 'Browse' button.

3. Enable the Credential Receipt form
4. You will get the possibility to upload a Microsoft Word .docx Document template where some V364 system variables can be used to write the text. Here is an example:

Credential Receipt Form

[&LOCATION], [&TODAY]

I, [&LASTNAME] [&FIRSTNAME] have received the following

Credential UID	Delivery date
[&UID]	[&TODAY]

to access the [&PLANT] of the “COMPANY NAME”.

I do hereby agree to return the above Credential upon request.

“COMPANY NAME” Manager	Credential Recipient

You can download this sample form and modify it and create your own form in .docx and upload it.

The V364 system variables you can use are:

Field	Description
[&PLANT]	Plant name
[&LOCATION]	Location of the V364 installation
[&TODAY]	Current date
[&Lastname]	Last Name
[&Firstname]	First Name
[&Role]	Role
[&UID]	Credential UID assigned to Access User
[&email]	email
[&activationdate]	Activation date
[&expirationdate]	Expiration date
[&validation]	Validation mode (0 = no validation, 1 Minutes, 2 Hours, 3 Days)
[&validperiod]	validation period
[&usrfield01]	User defined field #1 (Company)
[&usrfield02]	User defined field #2 (Department)
...	
[¬es]	Notes
[&picture]	base64 string image associated with the User

Print a Credential Receipt

When the credential is issued then you can print the Credential Delivery Form selecting the option Print Credential receipt:

The screenshot displays the 'Access Users' interface. At the top, there's a header bar with 'Access Users' and a back arrow. Below this, a user profile for 'Burton Catherine' is shown, including a role of 'OPS Team' and a credential 'DA0111'. The 'Validity' section shows activation and expiration dates (01/09/2016 and 31/12/2016) and a validation period of 122 days. The 'Assigned Doors' section lists various locations like 'Gas Refinery Plant', 'Main Door', 'Meeting Room', and 'Operation', each with associated working hours. A context menu is open over the user profile, showing options: 'Revoke Credential', 'Replace Credential', 'Suspend Credential', and 'Credential Receipt' (which is highlighted). The menu also includes 'Cancel' and 'OK' buttons.

You will get the Credential Delivery form already compiled like this in .docx format (on which you can still make modifications) or print:

Credential Receipt Form

Rome, 22/04/2016

I, Burton Catherine have received the following

Credential UID	Delivery date
RH1143	01/09/2016

to access the **Roma_01** of the "COMPANY NAME".
I do hereby agree to return the above Credential upon request.

"COMPANY NAME" Manager	Credential Recipient

System Administrators

The System Administrators menu option is used to set up V364 system administrators accounts.

System Administrators (or simply Administrators) are those individuals that administer or manage the V364 system. The System Administrators option is only visible to administrators with the right authorization level, in other word with an Administrator Role which authorize them to manage Administrator account.

It is possible to setup different Administrator Roles with different access level permissions (or system authorizations)

System Administrator Roles

There are 3 types of Administrator Role:

Technical Support role: this role is reserved to the Iseo Technical Support and allows to initially configure the V364 System (Network setup and Doors setup). The Technical Support creates the System Administrator.

System Administrator role: this role is the actual Administrator of the system in operation and has full right to administer the system in the day to day operation such as create other System administrators, create roles, time schedule,

Manager role: this role has access only to a subset of the functions example they cannot manage other administrators or create Access User roles.

Here is the detailed list of the V364 functionalities:

V364 System			
Administrators Roles	Technical Support	System Administrator	Manager
Access User Management	Y	Y	Y
Access Users	Y	Y	Y
Roles	Y	Y	
Time Schedules	Y	Y	
Door Zones	Y	Y	
System Administrators	Y	Y	
Login Preferences	Y	Y	Y
Door Events	Y	Y	
System Configuration	Y		
Network setup	Y		
Doors setup	Y		
Software Upgrade	Y		
Configuration Utilities	Y		
Reset to factory	Y		
System Shutdown	Y		
Credential Technology configuration	Y		
License Upgrade	Y		
Utilities	Y	Y	
Download Backup	Y	Y	
System Preferences	Y	Y	
System Information	Y	Y	
Logout	Y	Y	Y

System Administrators vs. Access Users

Throughout V364, the term *Administrator* refers to an individual who has access permissions to the V364 interface. Administrators manage the interface itself.

The term *Access user (or User)*, on the other hand, refers to an individual who has access privileges to some doors or all doors of a building. Users do not have access to the V364 System.

Instead, Administrators add and manage user-related information and assign credentials to users.

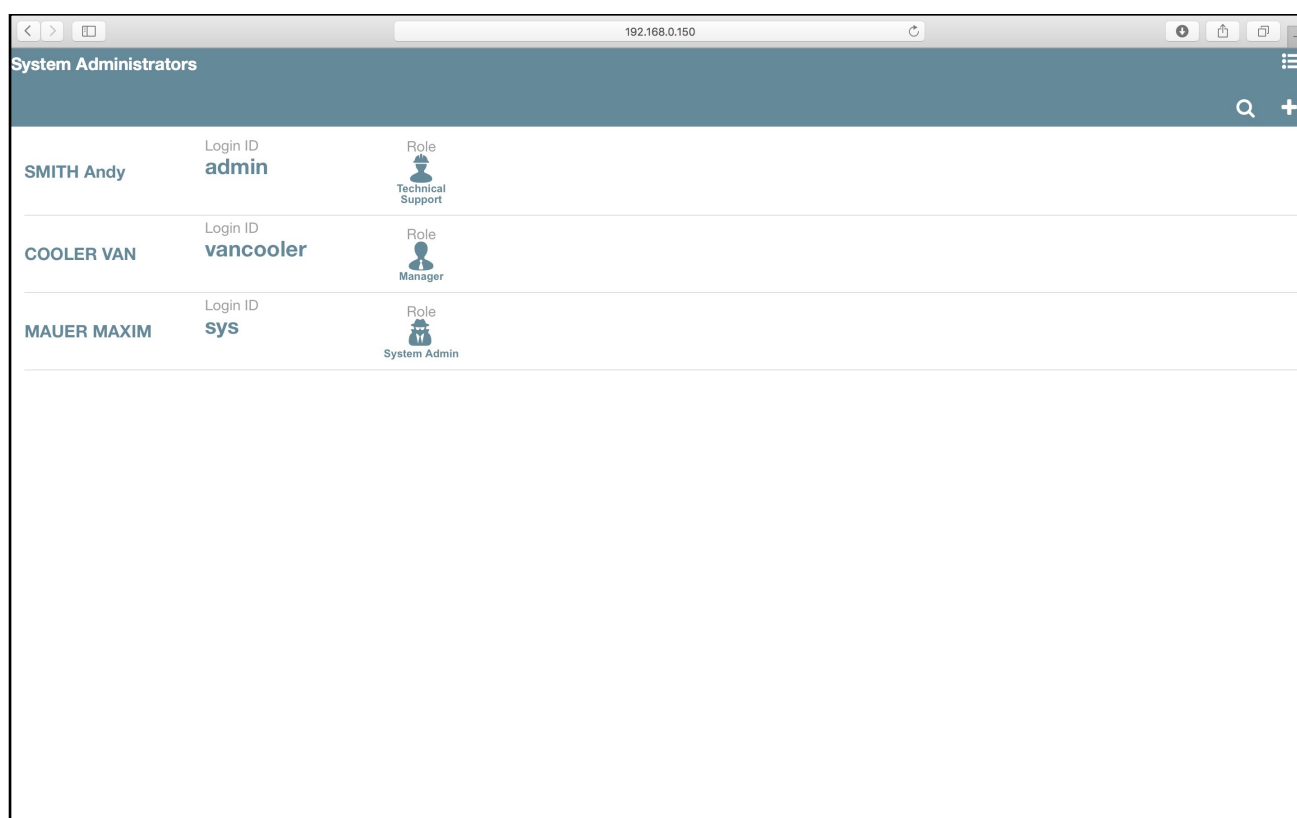
If an Administrator requires also access to doors then he/she must be defined also as Access users in the V364 system and a credential should be assigned to him/her.

Browsing the System Administrators List

The System Administrators List page displays the list of the system administrators. Administrators are listed by Last Name alphabetical order in the Access User List.

To view the list of Administrators:

Click the Menu dropdown and select System Administrators. The System administrators List displays.



	Login ID	Role
SMITH Andy	admin	Technical Support
COOLER VAN	vancooler	Manager
MAUER MAXIM	sys	System Admin

Details displayed include:

Name: the System administrator name. Last Name and First name

Login ID: the Login Identification used by the administrator to login to the V364 system

Role: the role of the Administrator which represent the authorization level in managing the V364 system .

Administrator with appropriate roles can

- create a new administrator
- edit an existing administrator
- delete an existing administrator

Every Administrator can

- change the own login preferences

Creating a new Administrator

To create an Administrator:

1. Click the Menu dropdown and select system administrators. The System administrator list displays.
2. Click Add New Administrator. The Edit administrator page displays with blank fields.

The screenshot shows a web browser window with the address bar displaying '192.168.0.150'. The page title is 'System Administrators'. Below the title bar, there is a '<Back' link and a document icon. The main content area is divided into two columns: 'LAST NAME' and 'FIRST NAME'. Below these columns, there is a 'Login Information' section. This section contains several fields: 'Administrator Role' with a dropdown menu showing 'Select an item from the list'; 'Login ID' with a text input field containing 'login id'; 'Password' with a text input field containing 'password'; 'Password confirm' with a text input field containing 'password confirm'; 'Language' with a dropdown menu showing 'Select a language from list below'; 'Date format' with a text input field containing 'dd/mm/YYYY'; and 'Credential Reader/Writer' with a dropdown menu showing 'Select an item from the list' and a checkbox.

3. insert the The System administrator name. Last Name and First name
4. select the Role of the Administrator which represent the authorization level in managing the V364 system
5. Enter the LoginID the Administrator will use to log into the system.
6. Password. Enter a password for the Administrator.
7. password confirm: Re-enter the exact same password in the (again) field. Both of these fields are required when creating an administrator or when changing the password. Otherwise they are optional fields.
8. Language. Select a preferred language from the drop-down list.

9. Date format : select a preferred date format from the drop-down list.
10. Credential Reader/Write. select from the drop-down list the preferred credential reader writer where the Administrator will read and write the credentials. Normally it is the one located close to the administrator browser.
11. save the administrator. You are returned to the administrator List page.

Managing Administrators

Once an administrator is created, this can be edited by any Administrator with appropriate level of authorization.

To edit an administrator:

1. Click in the dropdown menu then click on the System Administrators. The administrators list displays.
2. Click the administrator you want to edit. The administrator Details page displays.
3. Click Edit. The Edit User page displays.
4. All fields on this page can be edited. Enter the desired changes using the guidelines for creating an administrator, described above.
5. Click Save. You are returned to the administrator List page.

Deleting Administrators

Administrators can be DELETED from the database, therefore they will not be able to manage the V364 system anymore.

1. Click the System Administrators tab from dropdown menu. The System administrators list displays.
2. Click the System Administrator you want to delete. The associated System Administrator details page displays.
3. Click Delete. A warning message asks you to confirm that you want to delete the user.
4. Click OK. You are returned to the System administrator list with the deleted administrator removed.

WARNING:

Once an administrator is deleted, the administrator cannot be undeleted. To add the administrator back, he or she must be re-created as a new administrator.

Searching for an Administrator

1. Click the Menu dropdown and select System Administrators. The System Administrators list displays.
2. Click the Lens search and insert the text for searching in the Administrator First Name, Last name.
3. all the Administrators containing the typed string in the Name will be displayed. The lens in orange informs that a filtering is active with a specified string.

System Administrator Transaction Log

It is possible to display all the transactions made by an administrator.

1. Click the System Administrators tab from dropdown menu. The System administrators list displays.

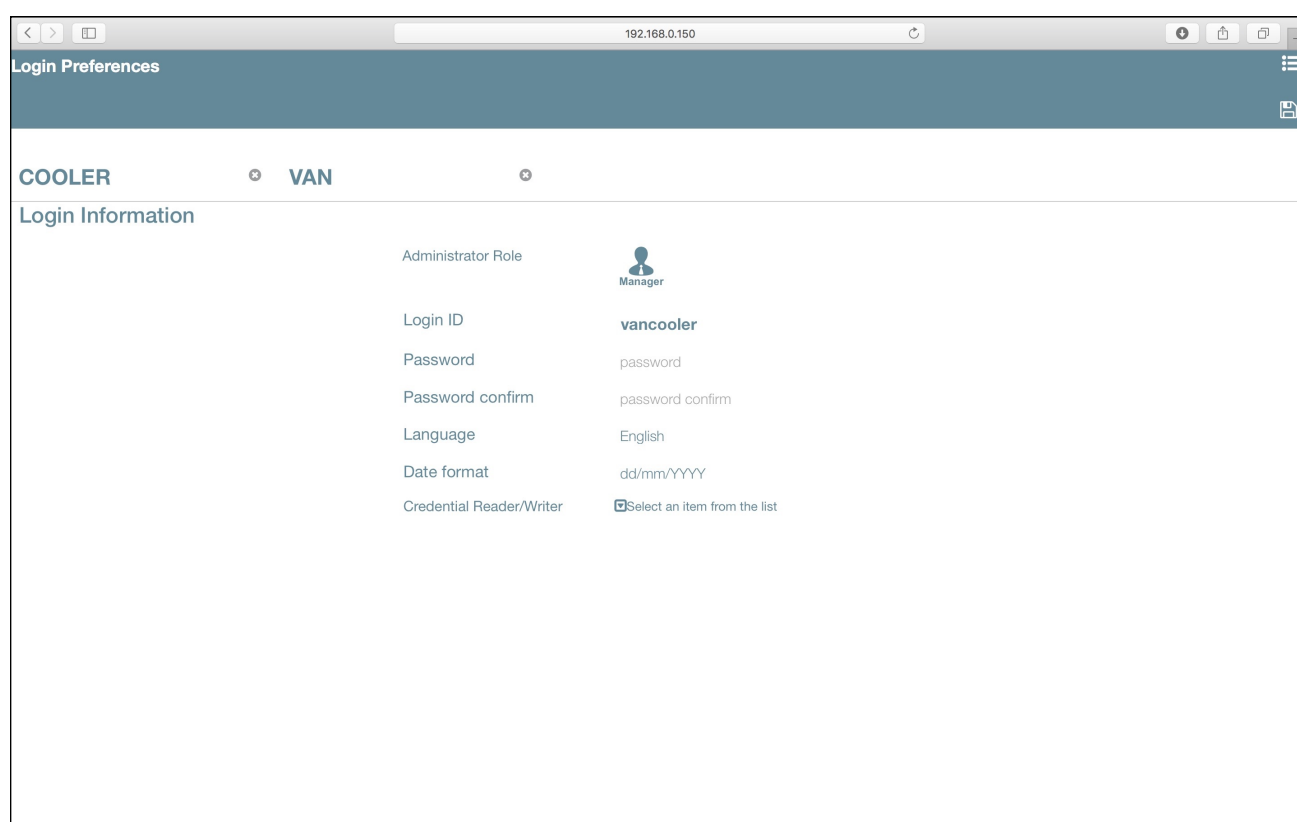
2. Click the System Administrator you want to look. The associated System Administrator details page displays.
3. Click on the Transaction log page.
4. Click not the .CSV icon to export the operations in a .CSV file.

Changing Administrator Login Preferences

Each Administrator manages his or her own login preferences such as password, preferred language, etc.

To change the login preferences:

1. Click the Menu dropdown and select Change Login Preference.
2. the page with your current Login preference displays.
3. you can change



The screenshot shows a web browser window with the address bar displaying '192.168.0.150'. The page title is 'Login Preferences'. Below the title bar, there are two tabs: 'COOLER' and 'VAN'. The 'VAN' tab is active. The main content area is titled 'Login Information' and contains a table of preferences:

Administrator Role	Manager
Login ID	vancooler
Password	password
Password confirm	password confirm
Language	English
Date format	dd/mm/YYYY
Credential Reader/Writer	Select an item from the list

- Password: enter a new password in both the New Password and Confirm New Password fields.
- Language. Select a preferred language from the drop-down list.
- Date format : select a preferred date format from the drop-down list.
- Credential Reader/Writer. select from the drop-down list the preferred credential reader writer where the Administrator will read and write the credentials. Normally it is the one located close to the administrator browser.

Events

In the Events menu you can display:

- **Door Events:** view latest events in the doors showing when individual doors were accessed and by whom.
- **System Administrators Transactions:** shows all the operation made by the system administrators

Door Events

The door Events menu displays the Access Events (history of the access) for the doors of the system either online, either offline (the F9000 cylinder).

For each event, the report shows the date and time, the user name, the operation and its result.

From the Online doors the events are collected automatically and from the offline doors (the F9000 cylinders) the events are collected with the programming key (red key).

Browsing the Door Events

The door events page displays the list of all the doors of the system. You can see the Online and the Offline doors in 2 different tabs.

Display events from online doors

To readout events from the online door :

1. Click the Menu dropdown and select Door Events. The Door events page will display
2. Select the Online tab and the list of the doors will appear
3. Select the Door you want to check for events. The events at the online door appears.

Door Events						
<Back BackDoor Start Log 04/11/2016 End Log 11/11/2016						
Logs into the system						
Date	Time	Credential	Credential Access Users Type	Transaction	Result	
11/11/2016	14:39	DA0288	 Fred Sanchez	Open Door	with Success	
11/11/2016	14:39	DA0111	 Paul Bishop	Open Door	with Success	
11/11/2016	14:39	DA0296	 William Hanson	Open Door	with Success	
11/11/2016	14:38	DA0288	 Fred Sanchez	Open Door	with Success	
11/11/2016	14:38	DA0288	 Fred Sanchez	Open Door	with Success	
11/11/2016	14:38	DA0111	 Paul Bishop	Open Door	with Success	
11/11/2016	14:38	DA0296	 William Hanson	Open Door	with Success	
11/11/2016	14:38	DA0296	 William Hanson	Open Door	with Success	
11/11/2016	14:34	DA0288	 Fred Sanchez	Open Door	with Success	

Display events from offline doors

To readout events from the offline door :

1. Click the Menu dropdown and select Door Events. The Door events page will display
2. Select Offline tab and the list of the doors will appear
3. Select the Door for which you want to read the events
4. Create the Credential to download Events (use the Red key = programming key)
5. Go to the offline door and download the events on the key
6. Go to V364 and read the download events key or insert it in any validator which will automatically download it. You can read events from different doors.
7. Events will be displayed with the most recent event on the top
8. Events can also be filtered by date selecting a time interval

Door Events						
Meeting Room						
Meeting Room						
Start Log						
04/11/2016						
End Log						
11/11/2016						
Logs into the system						
Date	Time	Credential	Credential Access Users	Transaction	Result	
11/11/2016	14:34	DA0111	Paul Bishop	Open Door	Not Validated	
11/11/2016	14:34	DA0288	Fred Sanchez	Open Door	with Success	
11/11/2016	14:31	DA0111	Paul Bishop	Open Door	with Success	
11/11/2016	14:31	DA0288	Fred Sanchez	Open Door	Not Validated	
11/11/2016	14:31	DA0296	William Hanson	Open Door	with Success	
11/11/2016	14:30	DA0111	Paul Bishop	Open Door	with Success	
11/11/2016	14:30	DA0288	Fred Sanchez	Open Door	with Success	
11/11/2016	14:30	DA0296	William Hanson	Open Door	Wrong Door	
11/11/2016	14:27	DA0288	Fred Sanchez	Open Door	with Success	

CSM ACCESS CONTROL SYSTEM TIME: 11/11/2016 14:31:00

List of Door Events

Every event is made by a Transaction (operation on the door) and a Result.

Transactions

Transaction	Description
Open Door	The credential is presented at the door
Credential Loaded into Black List	The credential is loaded into the black list.
Door Scheduled Passage Mode ON	The Door enters in passage mode at accordingly the loaded Door Schedule Time (only for online doors)
Door Scheduled Passage Mode OFF	The Door enters in passage mode at accordingly the loaded Door Schedule Time (only for online doors)

Results

Result	Description
with Success	operation executed with success
Wrong Plant	The credential belongs to a different Plant
Wrong Door	The credential has not the access right for the door
Out Validity	The credential is Not Yet Valid or Expired
Not Validated	The validation period has expired
Suspended	The credential is suspended
Out of time schedule	The credential is presented out of the Time schedule for the door
Credential Black Listed	The credential is in the door black list
Black List Full	The credential can not be loaded in the black list because it is full. The black list has records and automatically the expired credential are deleted.
Error in writing events in the credential	There has been an error while writing the events in the credential due to the credential has been removed before the completion of the operation
Full Credential Events Log	the credential has the event log full: you need to download the events at the validator

System Administrators Transactions

The System Administrators Transactions shows all the operations made by the system administrators.

The System Administrators Transactions displays the last operation on top. For each action, the view shows the Date/Time, details of the Action, and the Administrator who performed the action.

It is possible to export the Administrator transactions in .CSV file for advanced search with external software tools.

System Administrators Transactions										
Date	Time	Administrator	Type	UID	Action	Name of User	Validation Date	Expires at Time	Version Atlas	Residual Risk Credential
11/11/2016	14:34	sys		DA0288	Reinstate	Fred Sanchez			5	4
11/11/2016	14:33	sys		DA0288	Suspend	Fred Sanchez	11/11/2016	14:43	4	1
11/11/2016	14:32	sys		DA0288	Reinstate	Fred Sanchez			3	1
11/11/2016	14:31	sys		DA0288	Suspend	Fred Sanchez	11/11/2016	14:41	2	1
11/11/2016	14:30	sys		DA0296	Change access permission	William Hanson	11/11/2016	14:40	2	1
11/11/2016	14:29	sys		DA0296	Assign Credential	William Hanson			0	
11/11/2016	14:27	sys		DA0111	Change access permission	Paul Bishop	11/11/2016	14:31	2	1
11/11/2016	14:24	sys		DA0111	Revoke Credential	One 1	11/11/2016	14:34	3	3
11/11/2016	14:23	sys		DA0296	Revoke Credential	Thirteen 13	11/11/2016	14:33	2	2
11/11/2016	14:22	sys		DA0111	Assign Credential	Paul Bishop			0	
11/11/2016	14:20	sys		DA0288	Assign Credential	Fred Sanchez			0	
11/11/2016	14:18	sys			Login					

ACM ACCESS CONTROL SYSTEM TIME 11/11/2016 14:18:30

Utilities

Download Backup

Your database should be backed up on a regular basis.

The frequency of system backups depends on the amount and regularity of changes to the data on your V364 System. As a rule, it is strongly recommended that backups be taken, to preserve data against unintentional or catastrophic loss.

To create a backup of your database:

1. From the System dropdown menu, select Utilities and the Download Backup.
2. The Backup will automatically downloaded into your download folder

For security purposes the restore is only available to the Technical Support.

System Preferences

You can set system parameters values that will make more convenient the management of the system and the data entry when creating a new Access users.

To manage System Preferences

1. From the System dropdown menu, select Utilities and then System Preferences
2. The system preference page will display
3. Selecting the **Credential** tab you can modify:

Credential Validity

- Default Days : the default number of days the credential will be valid
- Default Validation Period: the default period of validation in minutes or hours and the related value
- Display time for activation and expiration (Switch) ; if this is selected then you can set
 1. Default activation time
 2. Default expiration time

Access Permissions

- Default Time Schedule: the default time schedule associated with each door assigned to the access User or the Role.
- The credential receipt form configuration

4. selecting the **web session** tab

Save your new preferences. At the next Access User data entry they are available.

System Information

You can view some information about your system

1. From the System dropdown menu, select Utilities and then System Informations
2. The system information page will display:



1.0.x.x
Platform
2.07.05.02441
Application
0.9.8.9.40

Atlas

MAC Address

License ID

Processor Board

Credential type

IP Network Address

Subnet Mask

Gateway

Date

Time

Time Zone

Master

00 15 42 01 35 FE

IseoDemoLicense

3.10.17-80707-gdac46dc-dirty

F9000 V2

192.168.0.184

255.255.255.0

192.168.0.1

11/11/2016

11:03:54

(GMT+01:00) Amsterdam, Berlin, Rome, Vienna

License valid: max 5000 users enabled

3001

Change Network

Software versions:

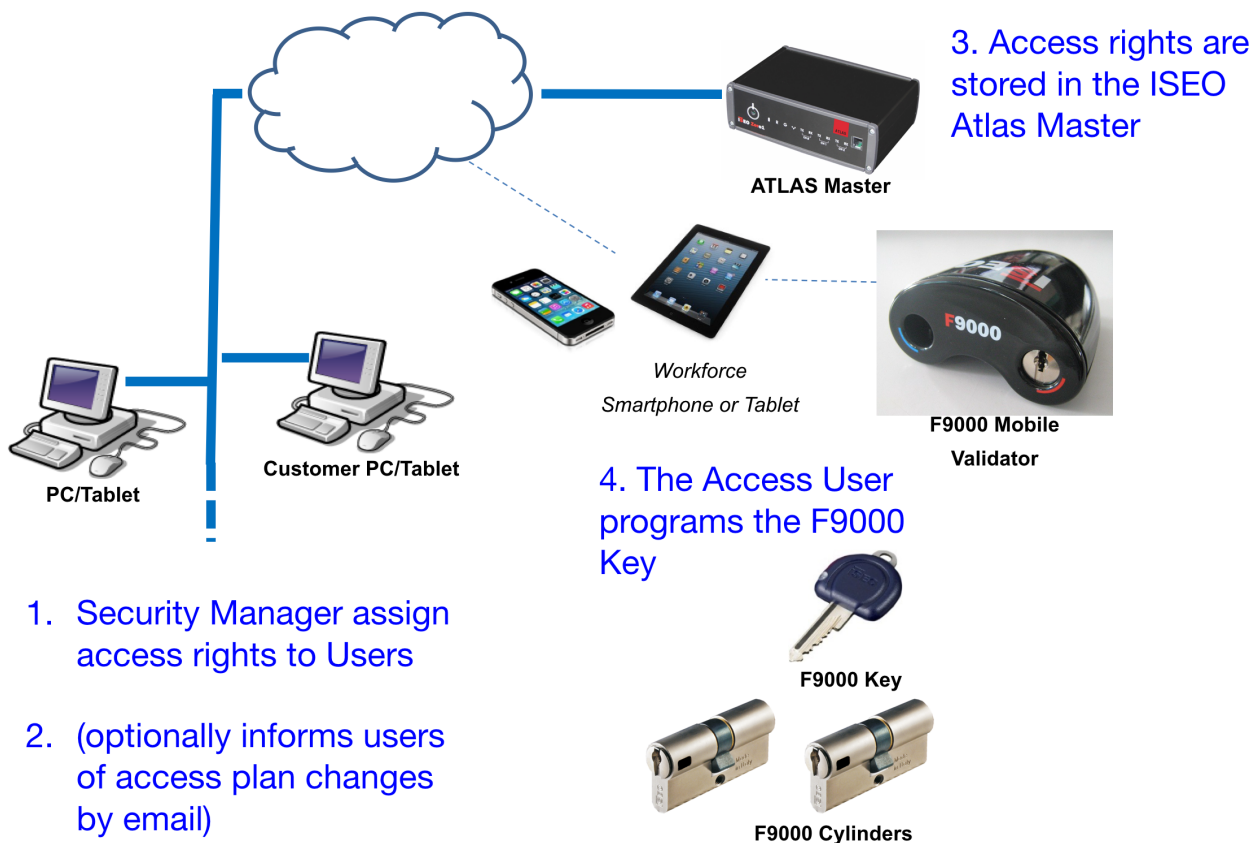
- **V364 Version:** it is the version of the V364 Solution package released which includes the all bundle of software and device firmware to run the V364 system solution (1.0.x.x)
- **Platform version:** it is the V364 platform engine that manages all the network infrastructure including the credentials reader/writer connection and provides low level services to the V364 Software.
- **Application version:** it is the version of the V364 Application running in the Atlas Master and slave controllers.

Information about the Atlas Master controller status:

- **MAC Address:** MAC stands for Media Access Control and basically identifies univocally the Atlas as it is hard-coded onto the Atlas.
- **Licence ID :** the V364 license number of your system and the maximum number of active users allowed
- **Processor Board:** the hardware electronic board of the Atlas controller
- **Plant Type:** identifies the type of credential in use in your system. In your case F9000 V2
- **Network configuration:** IP Network Address and network configuration of the Atlas Master
- **Date Time and Time zone:** current date and time of the Atlas Master

V364 Smartphone App

The V364 App is able to manage the F9000 Mobile Validator in order to validate the F9000 key typically for a mobile work force. The V364 App for smartphone or tablet is available for Android and iOS. This operation allows to provide access authorization to remote unmanned sites to a Mobile Workforce of technicians always on the move connected to the office with smartphones.

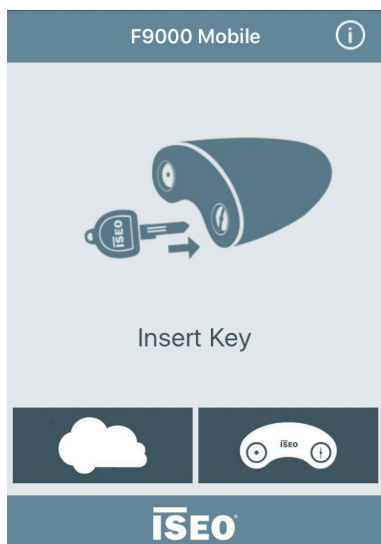


Using the V364 App

The V364 mobile App for Android and iOS allows the communication between the Atlas Master and the F9000 key via the F9000 Mobile Validator in order to accomplish a mobile validation of the mechatronic key. Therefore the functionalities of the mobile validator are the same of any validator connected directly to the Atlas.

Once installed the V364 APP in your smartphone or Tablet:

1. Start the V364 APP
2. You will see the following screen:



The bottom images show you the status of the Atlas connection (the cloud on the left) and the connection with the F9000 Mobile Validator (on the right).

If the background color is:

DARK GRAY then the V364 is connected

BLUE an operation of key programming is in progress

RED there is no connection

3. Insert the key into the F9000 Mobile Validator and the programming starts and remove the F9000 at the end:

