



VAULT CLOUD/SITE ENTERPRISE
USER MANUAL

Description



**System
Overview**

controllers



- **Power Source Built:**
- **The CF Falco-controlling interests have a source capable of charging your battery propria.**
- **autonomy:**
- **Controllers to be capable of supplying power to the entire system of locks and readers eletromagnéticas.**
- **PoE Power System Option: The SCAIP-CF-POE controller is the only controller PoE in the world, capable of powering 2 locks and 4 readers directly without auxiliary power supply and battery charger with built-in; (Using Hi PoE - 30W) ***
- **Energy Monitoring:**
- **Monitor power AC / DC, and alerts the software. What a special dispensation installing energy backbone for access control.**
- **Pear to Pear Technology:**
- **The controllers are devices P2P network. This allows controllers to talk to each other and in turn save money when integrated installation of fire systems, for example.**
- **Among several other advantages, P2P technology becomes operable controller offline 99.9%, not depending on the communication with the server even for the proper functioning of the Global Anti passback.**
- **Native TCP / IP:**
- **They are native controllers IP, which does not require wiring connecting placase together by RS 485.**

Description



Transaction Server
Service Site



VAULT Enterprise Site



SQL Server



Softwares



Program interface between controllers and the database. The application is in us any site that has installed the Enterprise Vault software.

He "sent" to the Database transactions, and there are recorded. When the TS is "closed" transactions are stored in the controllers, so that this information remain inaccessible to users. After reset "communication", transactions are automatically sent to the Data Bank.

Note: The application is a service and it can work with windows on Logoff.

Program interface between the user and the local database.

Through this program, we conduct registration cards, create rules, issued reports and visualize local transactions.

Place where ALL the registered information store site:

Registration data

Cards

Rules (Access Group, Elevator, Antipassback ...)

drivers

schedules

transactions

Note: MS SQL Database Server

Description

Softwares



Transaction Server Service Cental

*Program interface between the Enterprise Vault site and the central database. The application is installed only on the center handle.
Note: The application is a service and it can work with windows on Logoff.*



VAULT Enterprise Central

Program interface between the user and the Central bank data.

Through this program, we conduct registration cards, create rules, issued reports and visualize all transactions local. At the core software as we veer all transactions other sites and make any record .



Central Database

Place where ALL the information recorded from all sites are stored:

*Registration data
Cards
Rules (Access Group, Elevator, Antipassback ...)
drivers
schedules
transactions*

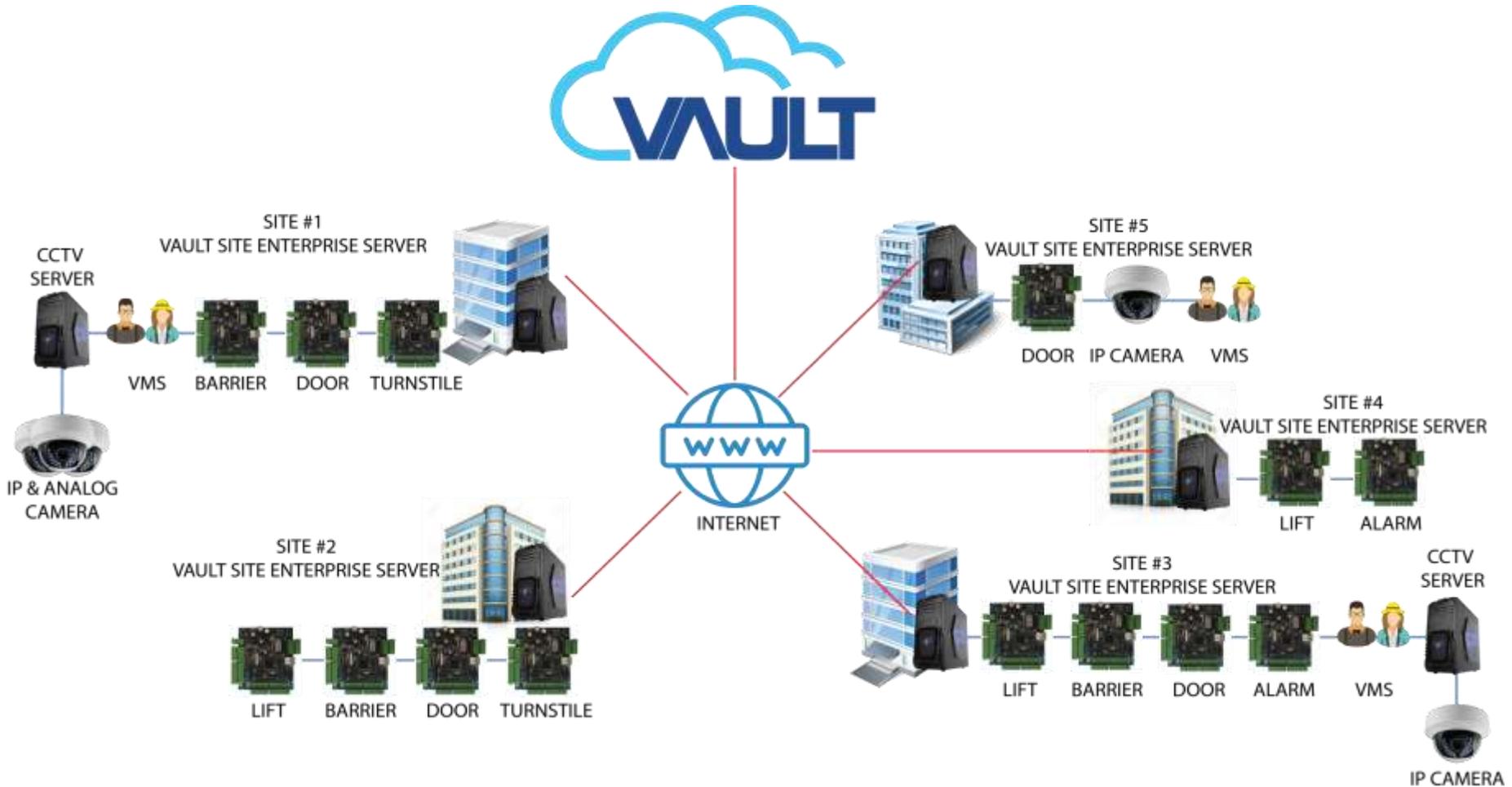
Note: Database MS SQL Server

Topology



Topology

Topology



This document uses the following definitions for central site and regional site:

Term	Definition
Cloud/Central	The cloud website that hosts and install the central application. Corporate servers at the central site are typically contained within a data center control.
Reginal Site	<p>A location or place that hosts and install a subset of site application, computers connected together by using a combination of LAN/VLAN and Intranet links. A regional site is connected to a central corporate site by using a Internet.</p> <p>For purposes of this paper, a regional site can be one of the following: A site located in a different region or country. A site physically separated from the central site but otherwise well-connected (such as a government agency or branch office).</p>



Determine your project size / scope

When planning the installation , make sure you understand the no of site/branch to be link up , door controller , hardware , software and etc to be connected back and link to the central software.

VAULT Enterprise Central						
Central Name	No Of Site	No Of Controller	No Of Card	UTC Time Zone	Server IP Address	Country
Central	3	(Based on site controllers)	(based on total site cards)	UTC +8 Malaysia	10.52.122.10	Malaysia
<ul style="list-style-type: none"> •Default central software login id = admin , password = admin , and the Site Name = Central •You are not allowed to change and update the site code after link the Site/Central software together. 						

VAULT Enterprise Site						
Site Name	No Of Controller	No Of Card	UTC Time Zone	Server IP Address	Country/Location	Userr Login
BANGSAR	50	500	UTC +8 Malaysia	20.55.122.11	Malaysia	BSR
JAKARTA-V1	100	1500	UTC +7 Indonesia	30.52.122.12	Indonesia	JKT1
JAKARTA-V2	60	1000	UTC +7 Indonesia	40.52.122.13	Indonesia	JKT2
<ul style="list-style-type: none"> •The Site Name & User Login ID must be unique during the planning stage for the software installation. •Proper setup and configuration are required before link up the site to the central software. 						



Determine your project size / scope

When planning the installation , make sure you understand the no of site/branch to be link up , door controller , hardware , software and etc to be connected back and link to the central software.

VAULT Enterprise Central						
Central Name	No Of Site	No Of Controller	No Of Card	UTC Time Zone	Server IP Address	Country
<ul style="list-style-type: none"> •Default central software login id = admin , password = admin , and the Site Name = Central •You are not allowed to change and update the site code after link the Site/Central software together, make sure you 						

VAULT Enterprise Site						
Site Name	No Of Controller	No Of Card	UTC Time Zone	Server IP Address	Country/Location	Userr Login
<ul style="list-style-type: none"> •The Site Name & User Login ID must be unique during the planning stage for the software installation. •Proper setup and configuration are required before link up the site to the central software. 						

Central with regional Vault Cloud/Site Architecture



Vault Cloud Enterprise architecture and governance across your environment in the following ways

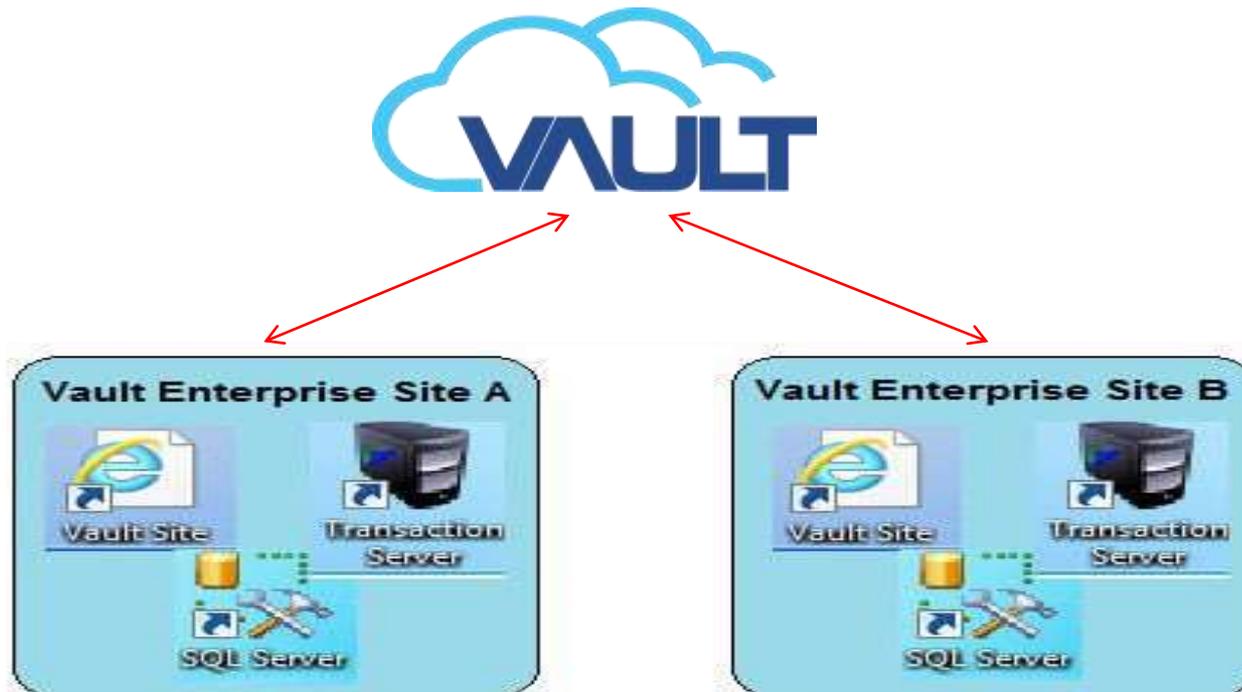
- On Vault Cloud Enterprise application, monitor and control all data from site or data control centre.

Vault Site Enterprise architecture and governance across your environment in the following ways

- On each site application, create parallel channel for collaboration, published data control, and door access information.

For example, RFID card registered (Created/Edited/Deleted) information or alarm at regional site more often will auto update back to the cloud application.

The following illustration shows a two **regional site server** .





Central Software License

Software License

Vault Enterprise central software license are control based on the site server and module available. Module here refer to feature available. Site Server here refer to Vault Enterprise Site per server instance. Make sure you understand how and what the module you need in order to enable and purchase the feature you want .

Module	Description
Site Server	No of Site Server to be linked at central system
Door Controller	Door controller <= 10 per site are free of charge, above 10 door controller , license are required per controller
Fire Alarm Module	By feature to be enable or disable
Global Antipassback	By feature to be enable or disable
Fingerprint Alarm	By feature to be enable or disable (ZK/VIRDI) limited model only By feature to be enable or disable
LCD Module Lift Module	By feature to be enable or disable By feature to be enable or disable
Car Park Module	By feature to be enable or disable (Nuuo, Milestone, Digifort, HIK, Infinova, Geovision, ISS, Securos, Meritlili n, Exaqvision, Dahua)
Video Integration	By feature to be enable or disable
IO Module	

Port
Requirement



Port
Requirement

FIREWALL USED DOORS



TCP DOORS = 1003, 1007, 1008, 2011, 2012

UDP DOORS = 2003, 2007, 32767, 2011, 2012



Port Requirement

When planning the infrastructure, ensure that port numbers used by Vault Enterprise Application, MSSQL, and IIS are free to enable communication between those components.

The following is the list of default ports used by the Vault Enterprise application.

Port Used	
Port No.	Description
1433	MSSQL Server
80	Web access port to web door access system
1003, 1007, 1008, 2011, 2012	Controller event tracking
2003, 2007, 32767, 2011, 2012	UDP port use for command communication with door controller
32767	Use for device health check and security access
ICMP PORT	Communication with controller

**Fail Over
/ High availability**

Fail Over / High Availability

The purpose of Fail Over / High Availability is to provide resiliency within the primary system and planned downtime. Switching to a redundant or standby system component (server, hardware component, etc.) upon the failure or abnormal termination of the previously active system component.

You may want consider to provide this window clustering solution to your client depend on the project request and needs.

In clustered environment, vault central can be hosted on more than one server to provide redundancy. If a server within the cluster crashes, you will not lost the control or access to the system, other available server will take up the role of the server that are down.





Proposed Solution & Diagram

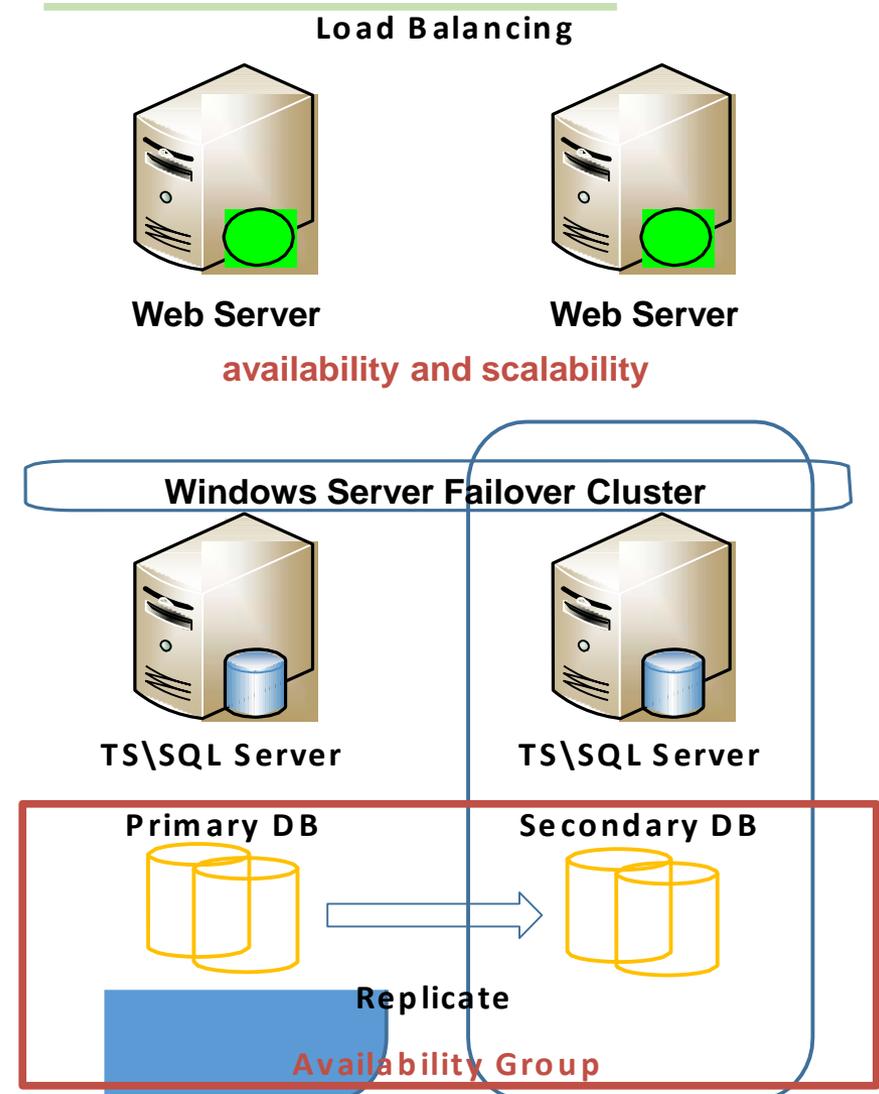
Enterprise Vault Central

Web Server (Front-End) - Two servers form as a single virtual cluster with NLB to bring the availability and scalability of Internet server applications.

SQL Server (Back-End) – Two servers in group of failover cluster farm provide high availability and scalability to Microsoft SQL Server, and TS servers. If one or more of the cluster nodes fail, other nodes begin to provide service (a process known as failover). In addition, the clustered roles are proactively monitored to verify that they are working properly. If they are not working, they are restarted or moved to another node.

Note : Try to contact the local microsoft certified solution provider and share with them the environment setup you need or contact us for further information.

Tag : Enterprise Class Server, Storage & Networking Solutions provider



specifications



Hardware Specification

Hardware Specification



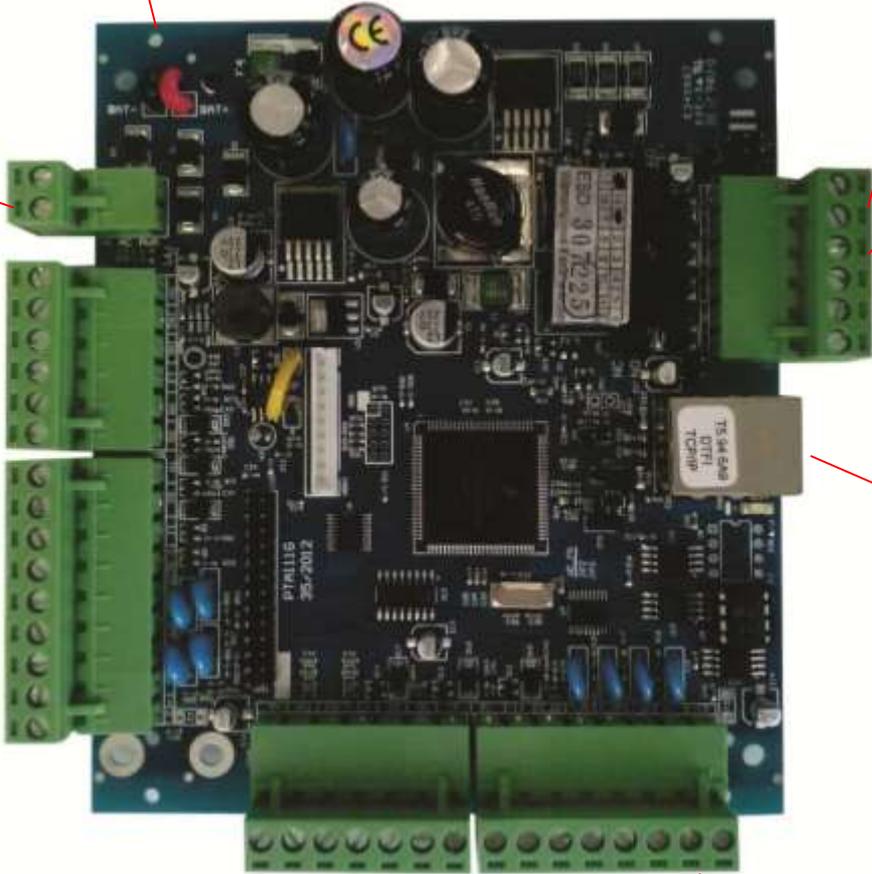
specifications

Battery Charger 12V / 7Ah (Max.)

Food for Lock
Max. 12VDC / 1A

VAC power input
Range: 14 ~ 15 VAC

Relay - Dry Contact
- N.A - 250Vac / 10A
- N.C - 250 VAC / 7A



10Mbps Full Duplex

Feed Readers
Max. 12Vdc / 500mA

Feed Readers
Max. 12Vdc / 500mA

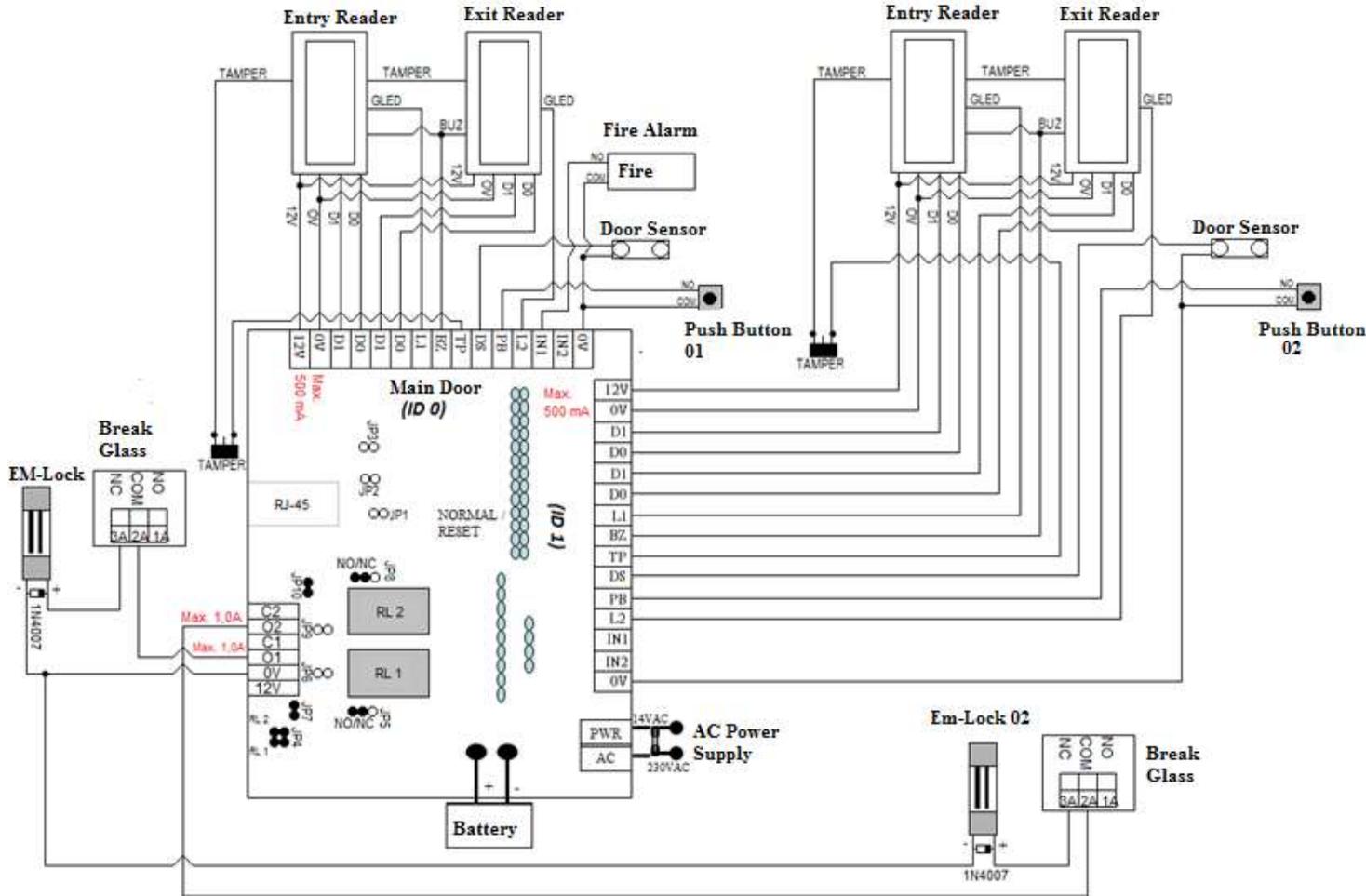


Connection
Diagram



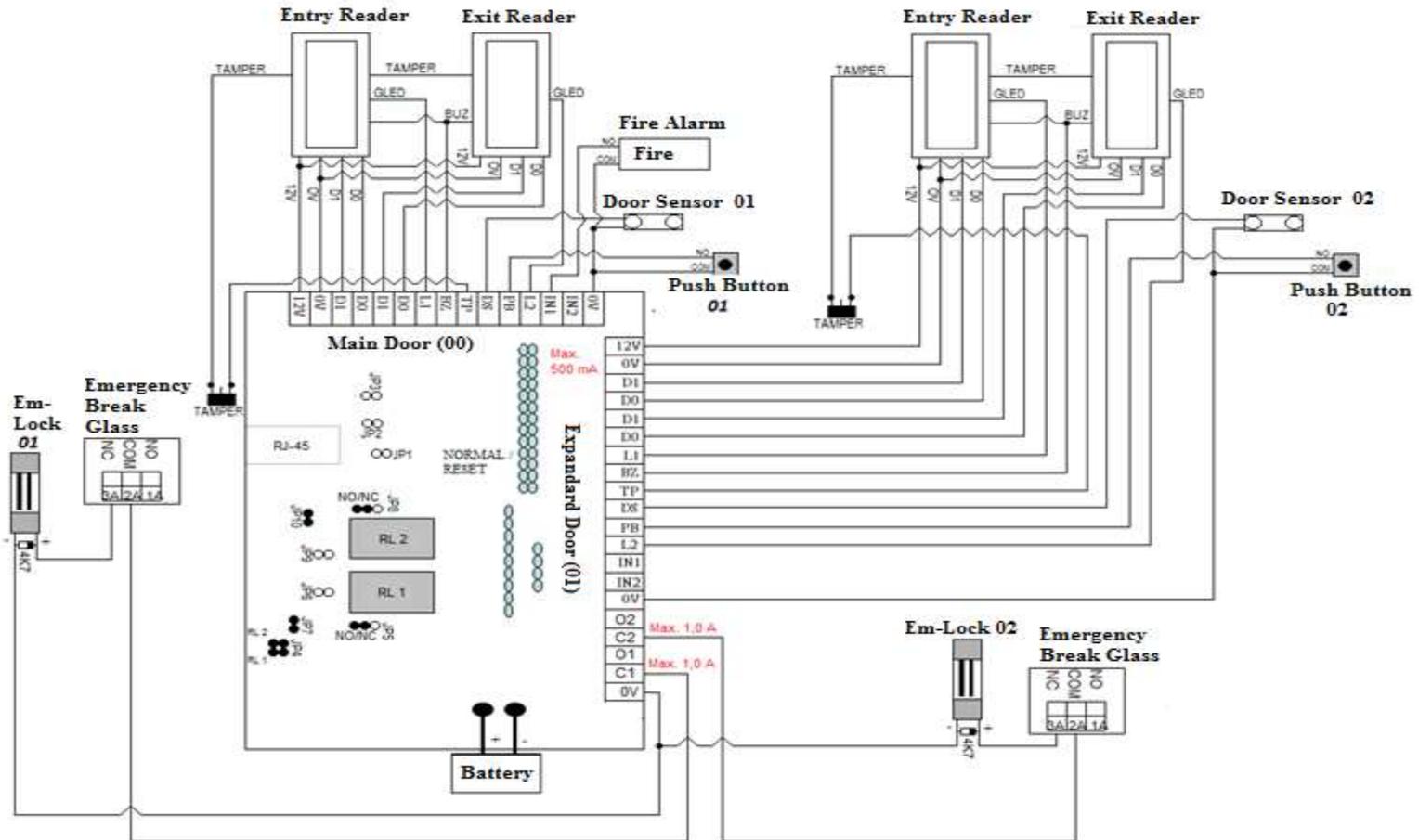
Connection
Diagram

Two Door Controller



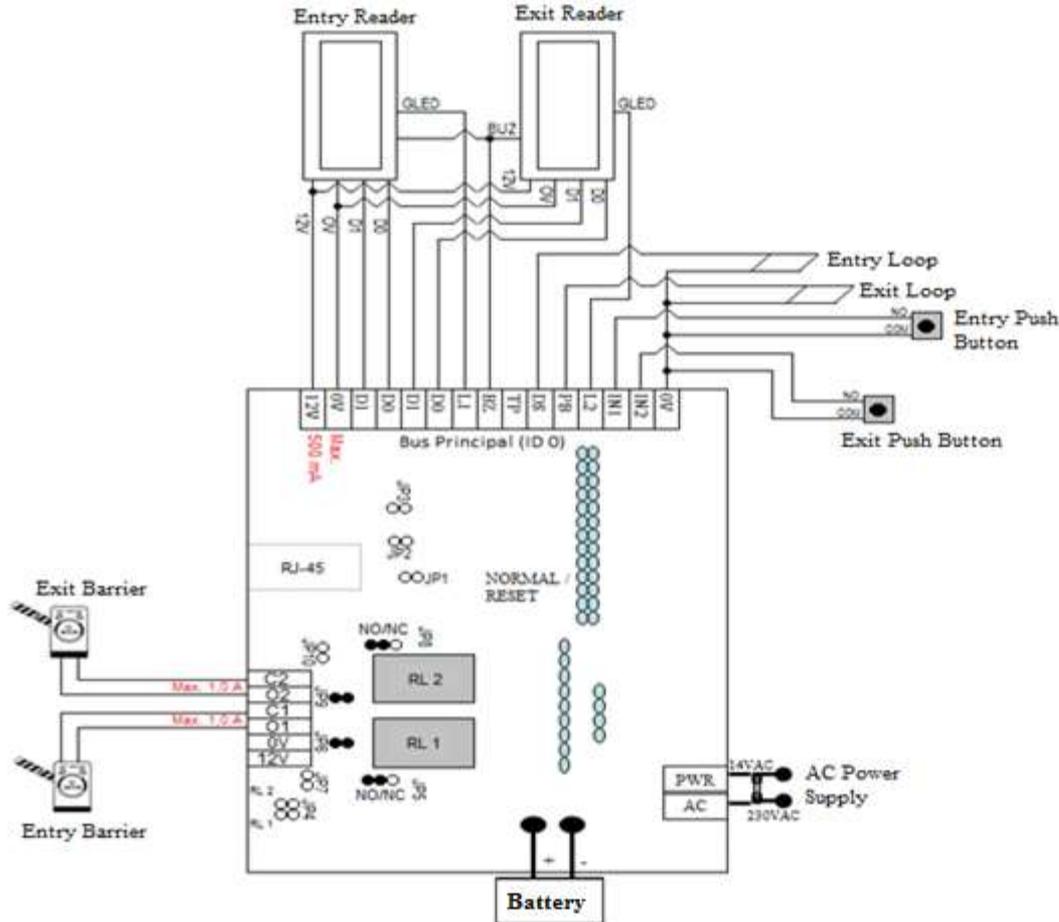
Observation: the total current of the controller must not exceed 12V @ 2A, independent of the output current of each circuit

Controller POE Two Doors



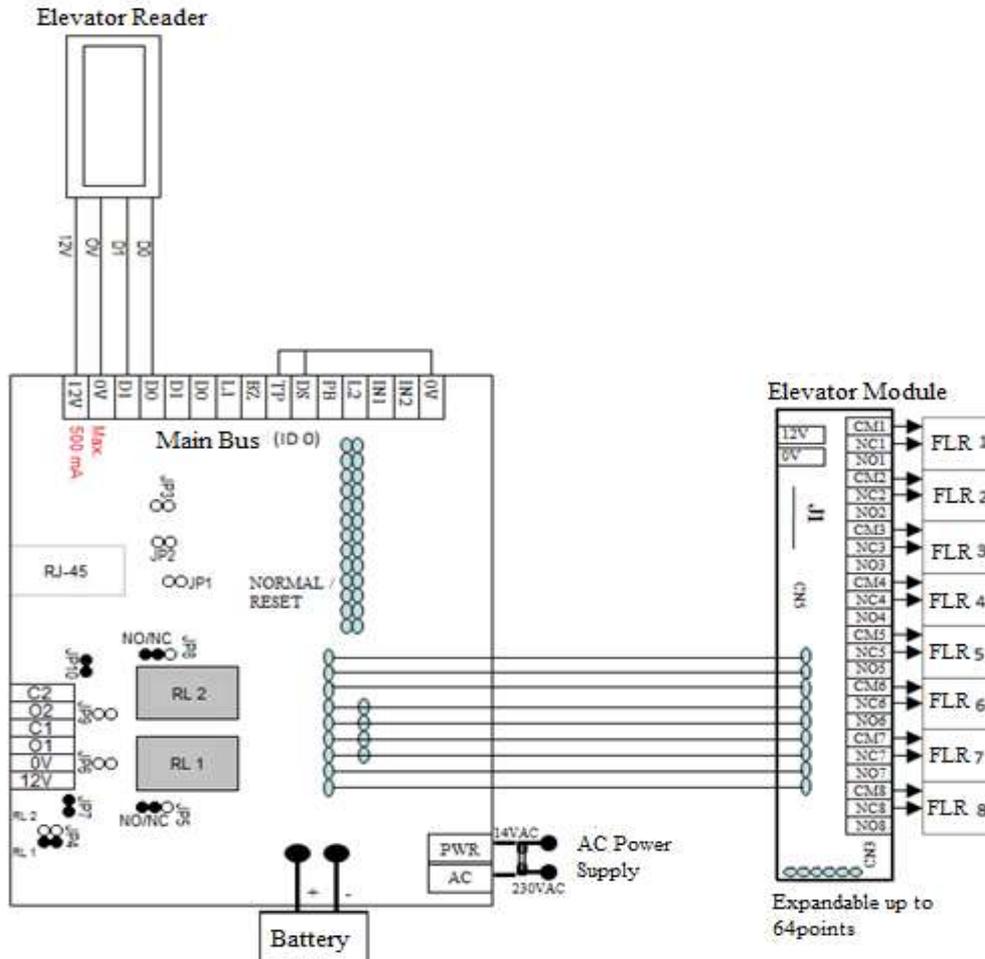
Observation: the total current of the controller must not exceed 12V @ 2A, independent of the output current of each circuit

Car Parking Controller



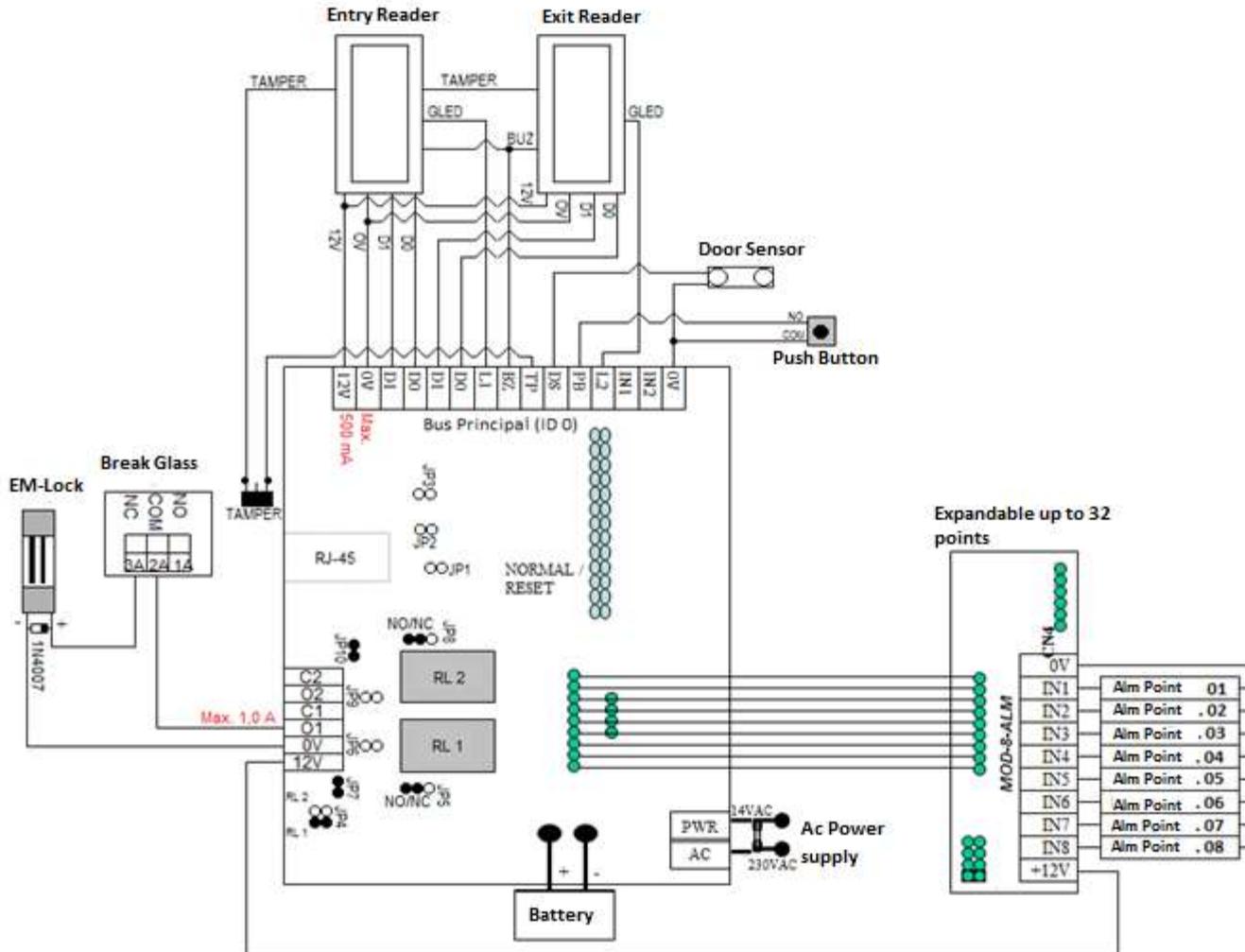
Observation: the total current of the controller must not exceed 12V @ 2A, independent of the output current of each circuit

Elevator controller



Observation: the total current of the controller must not exceed 12V @ 2A, independent of the output current of each circuit

Alarm controller



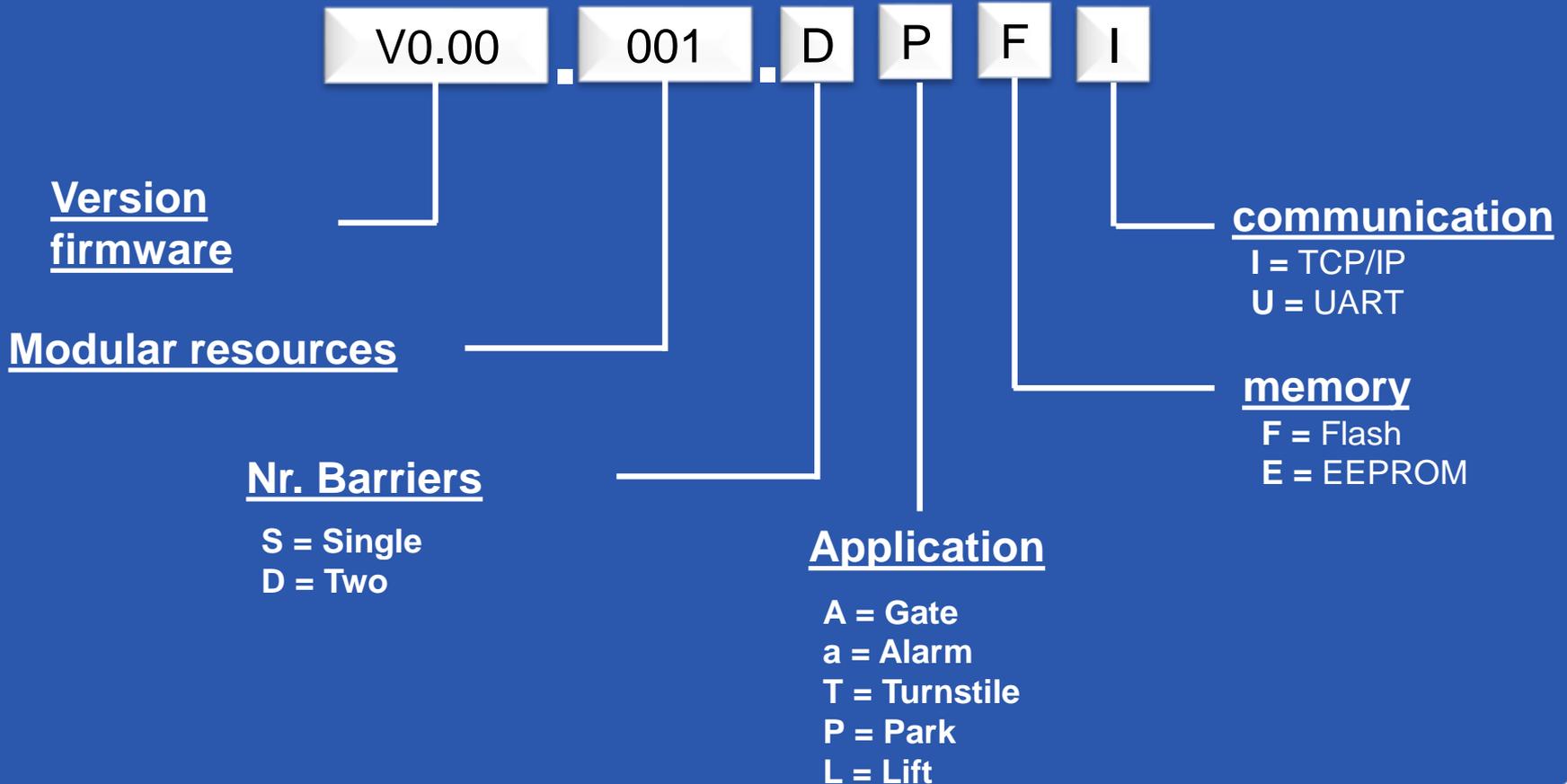
Observation: the total current controller must not exceed 12V @ 2A, independent of the output current of each circuit

Firmware



Firmware

Identifying the Firmware controller



Requirements

Software Requirements

Application Server - Site



Application Server - Server Transaction Service and Enterprise Vault Site					
controllers	Simultaneous Hits on the web	Processors' (upper)	Memory RAM	Operating System Recommended	Storage***
Up to 10 *	2	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows 7 Professional (x64)	250GB
11 a 30*	2	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows Server 2008 R2 (x64)	250GB
31 a 90 **	5	Intel Xeon E3-1280 @ 3.50 Ghz Intel Xeon W3680 @ 3.33Ghz Intel Core I7-970 @ 3.20Ghz Intel Core I7-2700K @ 3.50Ghz Dual Xeon E5620 @ 2.40Ghz	8GB	Windows Server 2008 R2 (x64)	500GB
superior a 99 **	5	Intel Xeon E5-2670 @ 2.60 Ghz Dual Xeon E5-2670 @ 2.60Ghz Dual Xeon E5-2640 @ 2.50Ghz	16GB	Windows Server 2008 R2 (x64)	2 TB

•For sites with up to 30 controllers can use a single server for database and application.

** For sites with more than 30 controllers must use a server to the database server and one for the application.

*** Disk capacity must be topic under analysis case by case.

Server Database - Site



Database Server for Enterprise Vault Site Software

controllers	Simultaneous Hits on the web	Processors' (upper)	Memory RAM	Operating System Recommended	Database	Storage***	
						Sist.Op	Database
Hasta 10*	2	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows 7 Professional (x64)	Microsoft SQL Express (freeware)	250GB	250GB
11 a 30*	2	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows Server 2008 R2 (x64)	Microsoft SQL Server 2008 R2 Standard	250GB	250GB
31 a 90 **	5	Intel Xeon E3-1280 @ 3.50 Ghz Intel Xeon W3680 @ 3.33Ghz Intel Core I7-970 @ 3.20Ghz Intel Core I7-2700K @ 3.50Ghz Dual Xeon E5620 @ 2.40Ghz	8GB	Windows Server 2008 R2 (x64)	Microsoft SQL Server 2008 R2 Standard	250GB	500GB
superior a 99 **	5	Intel Xeon E5-2670 @ 2.60 Ghz Dual Xeon E5-2670 @ 2.60Ghz Dual Xeon E5-2640 @ 2.50Ghz	16GB	Windows Server 2008 R2 (x64)	Microsoft SQL Server 2008 R2 Standard	500GB	2 TB

*For sites with up to 30 controllers can use a single server for database and application.

** For sites with more than 30 controllers must use a server to the database server and one for the application.

*** Disk capacity must be topic under analysis case by case.

Application Server - Central



Application Server - Server Transaction Service and Enterprise Vault Central

controllers	Simultaneous Hits on the web	Processors' (upper)	Memory RAM	Operating System Recommended	Storage***
Hasta 10*	2	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows 7 Professional (x64)	250GB
11 a 30*	2	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows Server 2008 R2 (x64)	250GB
31 a 90 **	5	Intel Xeon E3-1280 @ 3.50 Ghz Intel Xeon W3680 @ 3.33Ghz Intel Core I7-970 @ 3.20Ghz Intel Core I7-2700K @ 3.50Ghz Dual Xeon E5620 @ 2.40Ghz	8GB	Windows Server 2008 R2 (x64)	500GB
superior a 99 **	5	Intel Xeon E5-2670 @ 2.60 Ghz Dual Xeon E5-2670 @ 2.60Ghz Dual Xeon E5-2640 @ 2.50Ghz	16GB	Windows Server 2008 R2 (x64)	2 TB

- For sites with up to 30 controllers can use a single server for database and application.
- ** For sites with more than 30 controllers must use a server to the database server and one for the application.
- *** Disk capacity must be topic under analysis case by case.

Server Database - Central



Servidor de Banco de Datos para el software VAULT Enterprise Central

controllers	Simultaneous Hits on the web	Processors' (upper)	Memory RAM	Operating System Recommended	Database	Storage***	
						Sist.Op	Database
Hasta 10*	2	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows 7 Professional (x64)	Microsoft SQL Express (freeware)	250GB	250GB
11 a 30*	2	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows Server 2008 R2 (x64)	Microsoft SQL Server 2008 R2 Standard	250GB	250GB
31 a 90 **	5	Intel Xeon E3-1280 @ 3.50 Ghz Intel Xeon W3680 @ 3.33Ghz Intel Core I7-970 @ 3.20Ghz Intel Core I7-2700K @ 3.50Ghz Dual Xeon E5620 @ 2.40Ghz	8GB	Windows Server 2008 R2 (x64)	Microsoft SQL Server 2008 R2 Standard	250GB	500GB
superior a 99 **	5	Intel Xeon E5-2670 @ 2.60 Ghz Dual Xeon E5-2670 @ 2.60Ghz Dual Xeon E5-2640 @ 2.50Ghz	16GB	Windows Server 2008 R2 (x64)	Microsoft SQL Server 2008 R2 Standard	500GB	2 TB

For sites with up to 30 controllers can use a single server for database and application.

** For sites with more than 30 controllers must use a server to the database server and one for the application.

*** Disk capacity must be topic under analysis case by case.

Software Requirements



Software Requirements for the Enterprise Vault software Site / Central

Operational systems approved	Softwares and Tools Needed	Approved browsers
Microsoft Windows 7 Professional SP1 (x86/x64) Microsoft Windows Server 2008 R2 (x86/x64) Microsoft Windows 8 Professional (x86/x64) Microsoft Windows 8.1 Professional (x86/x64)	Microsoft Internet Information Service 5.1 o superior(IIS) Microsoft .Net Framework 4.5	Internet Explorer 11 (Con integración CCTV) Mozilla Firefox versión 31.0 (Sin Integración con CCTV) Google Chrome versión 36.0.1985.143M (Sin Integración con CCTV)

Application Server - Central



Cloud Hosting Provider



- ❖ Can be accessed anywhere remotely
- ❖ Eliminates IT infrastructure needs
- ❖ Redundancy availability (Easy Recovery)
- ❖ Data Storage (Backup & Restore)
- ❖ Reduces problem with virus / malware
- ❖ VM Cost / OS/ IP / Memory / CPU / GPU
- ❖ IoT Hub
- ❖ Load Balance
- ❖ N Tier Regional
- ❖ SQL / Azure SQL
- ❖ HDD/ SDD / BLOB DB

installation

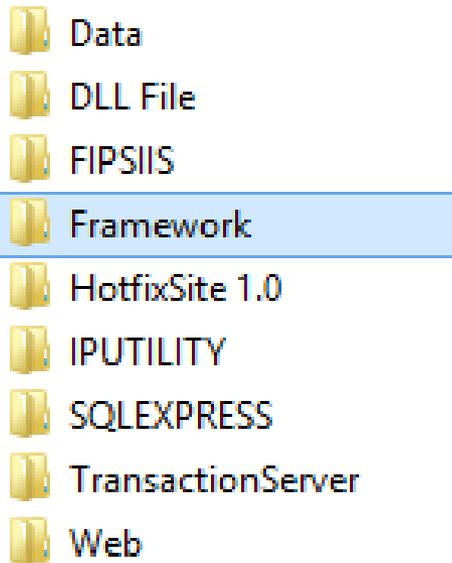


SOFTWARE INSTALLATION

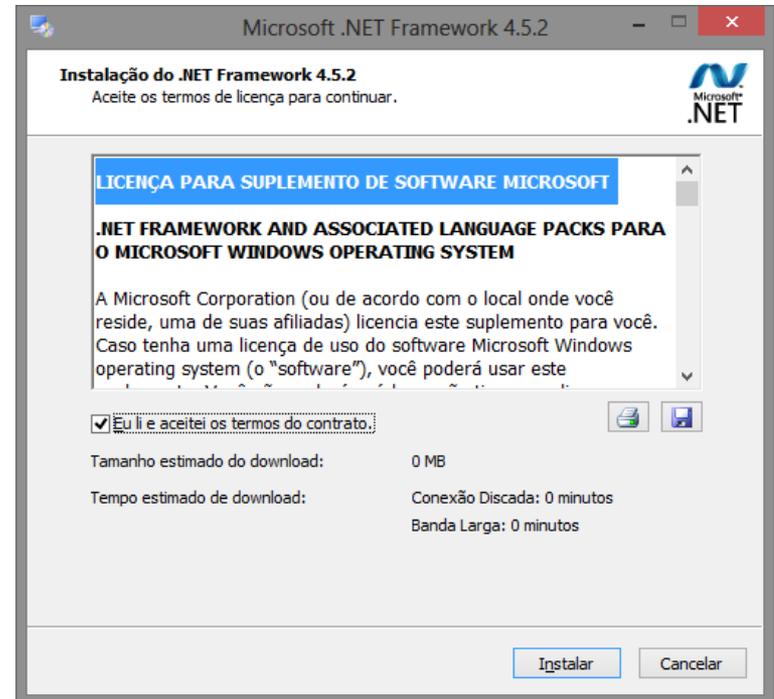
SOFTWARE INSTALLATION



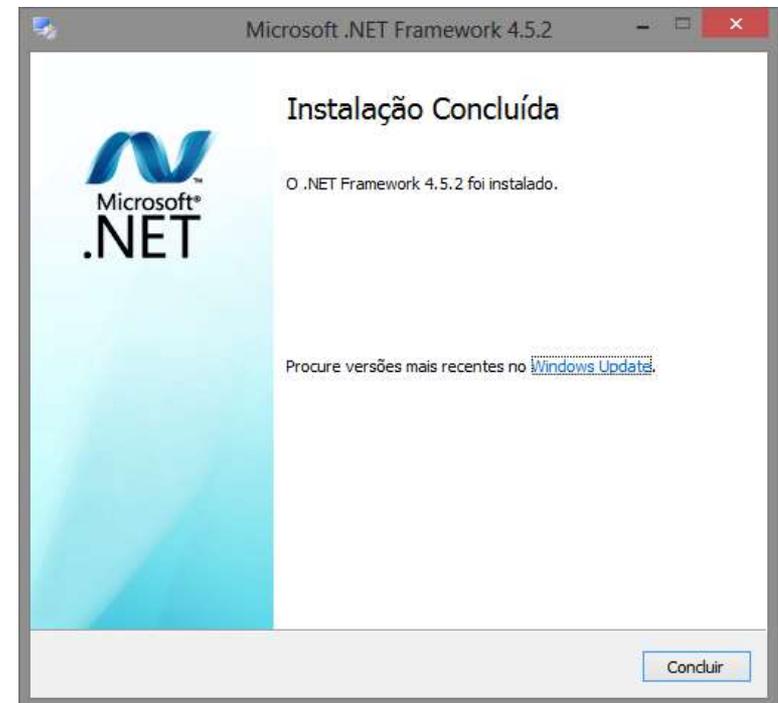
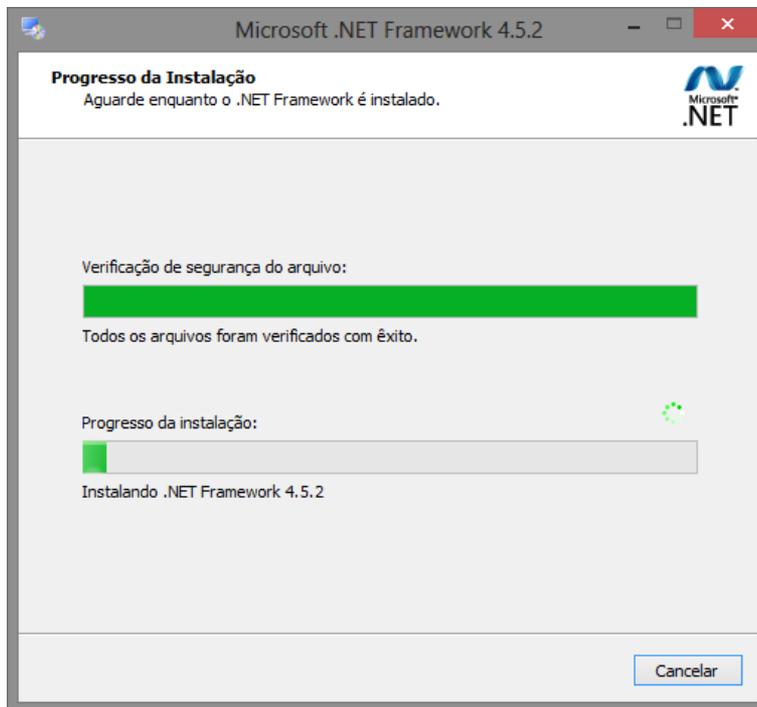
- 1) The user must first make the installation of Net Framework 4.5,
- 2) which can be searched on the Framework folder.



dotNetFx4.5.2-x86-x64-AllOS-ENU



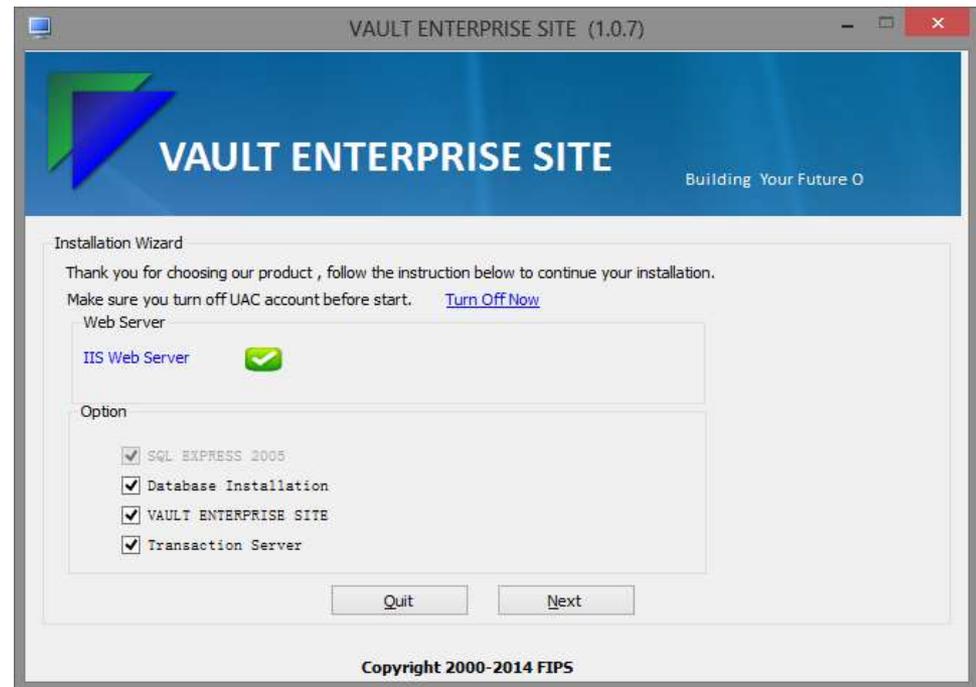
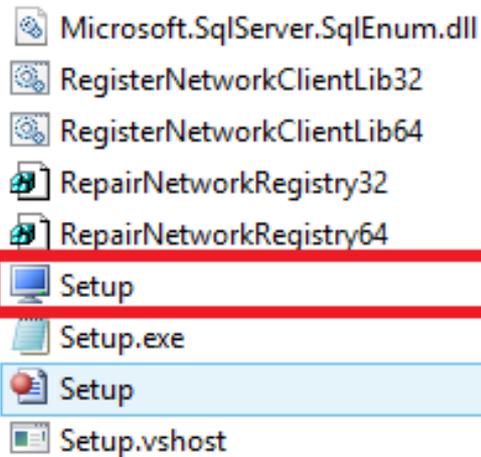
2) Wait until the entire installation without errors install.



SOFTWARE INSTALLATION



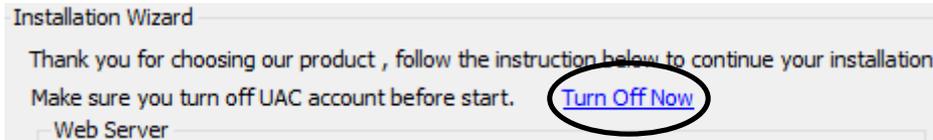
3) In the installation folder, click SETUP.EXE. Use the option to install as a system administrator.



SOFTWARE INSTALLATION



1) Click Turn off to disable the UAC now.



2) Install the software and select the Leave UAC Off.

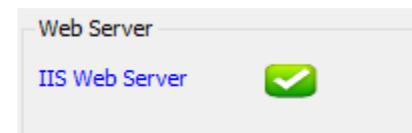
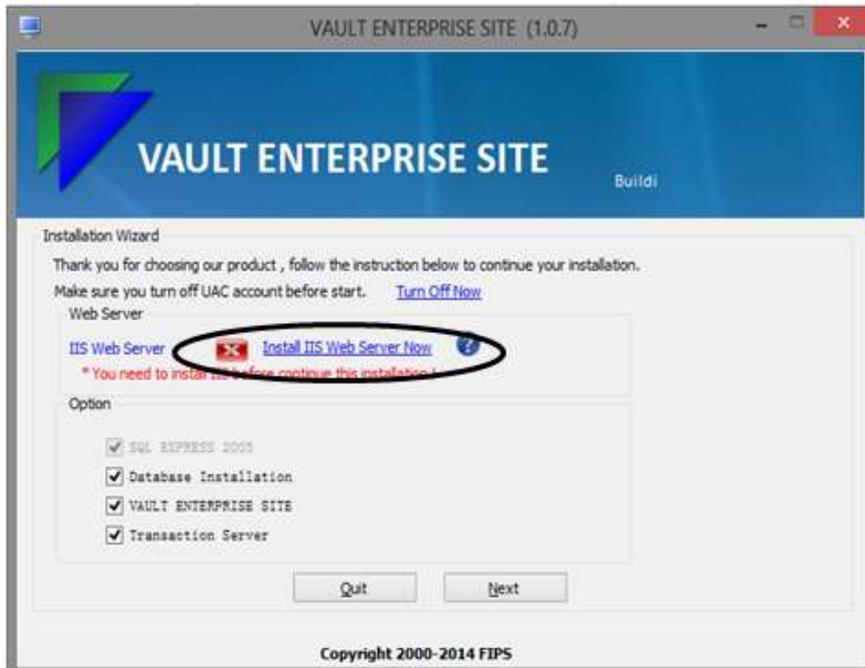


SOFTWARE INSTALLATION



- 1) For the Operation of Enterprise Vault, the Internet Information Service (IIS) must be installed. Click Install Now IIS Web Server to install.

- 2) Select your operating system and wait for the end of the installation.



SOFTWARE INSTALLATION



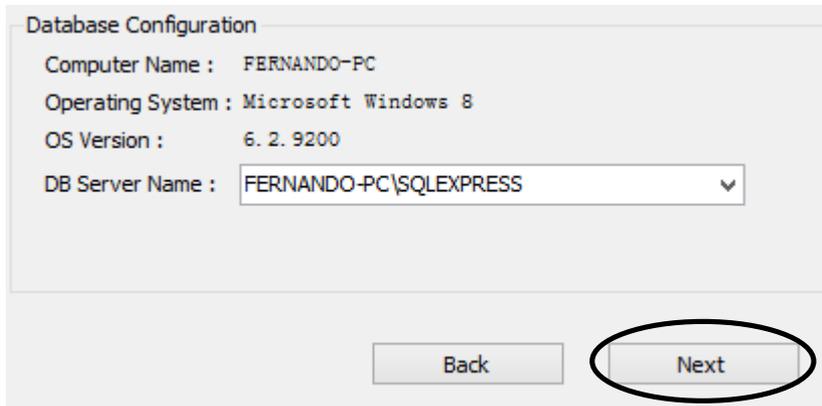
1) Select all options, and click Next.



Option

- SQL EXPRESS 2005
- Database Installation
- VAULT ENTERPRISE SITE
- Transaction Server

2) Select where you want to install the database and click Next.

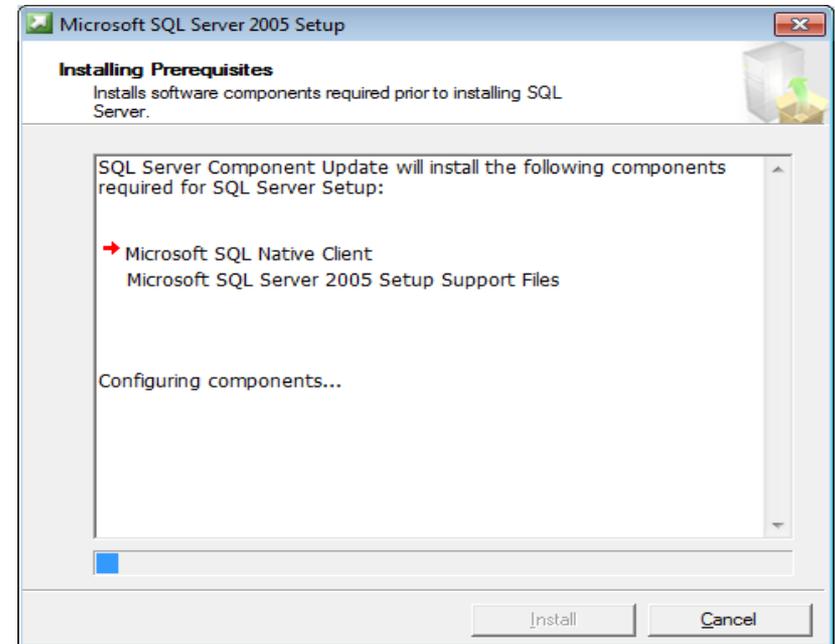


Database Configuration

Computer Name : FERNANDO-PC
Operating System : Microsoft Windows 8
OS Version : 6. 2. 9200
DB Server Name : FERNANDO-PC\SQLEXPRESS

Back Next

3) Installing SQL SERVER EXPRESS 2005.



Microsoft SQL Server 2005 Setup

Installing Prerequisites
Installs software components required prior to installing SQL Server.

SQL Server Component Update will install the following components required for SQL Server Setup:

- Microsoft SQL Native Client
- Microsoft SQL Server 2005 Setup Support Files

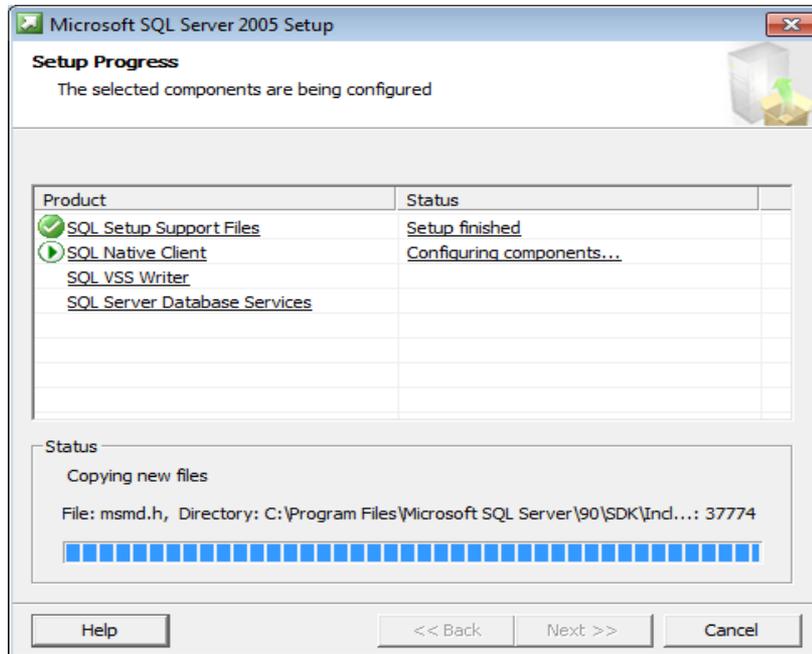
Configuring components...

Install Cancel

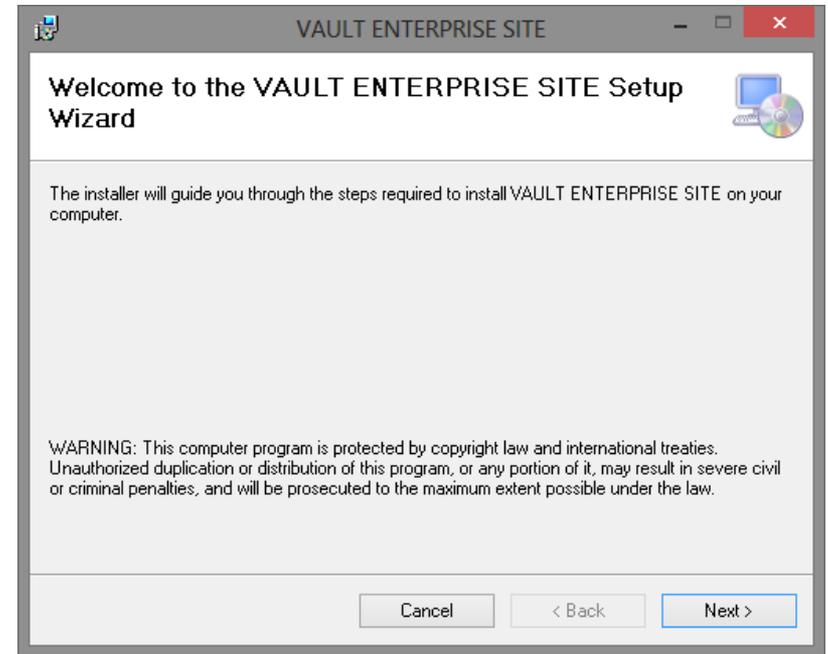
SOFTWARE INSTALLATION



4) At the end of the installation, verify that all items are installed correctly.



5) Installing the Enterprise Vault Site software. Click Next to install.



SOFTWARE INSTALLATION



6) Select the DefaultAppPool Application Pool option and click Next.

7) Click Close to enclose the facility.

VAULT ENTERPRISE SITE

Select Installation Address

The installer will install VAULT ENTERPRISE SITE to the following web location.
To install to this web location, click "Next". To install to a different web location, enter it below.

Site:
Default Web Site

Virtual directory:
VAULTSITE

Application Pool:
DefaultAppPool

Cancel < Back **Next >**

VAULT ENTERPRISE SITE

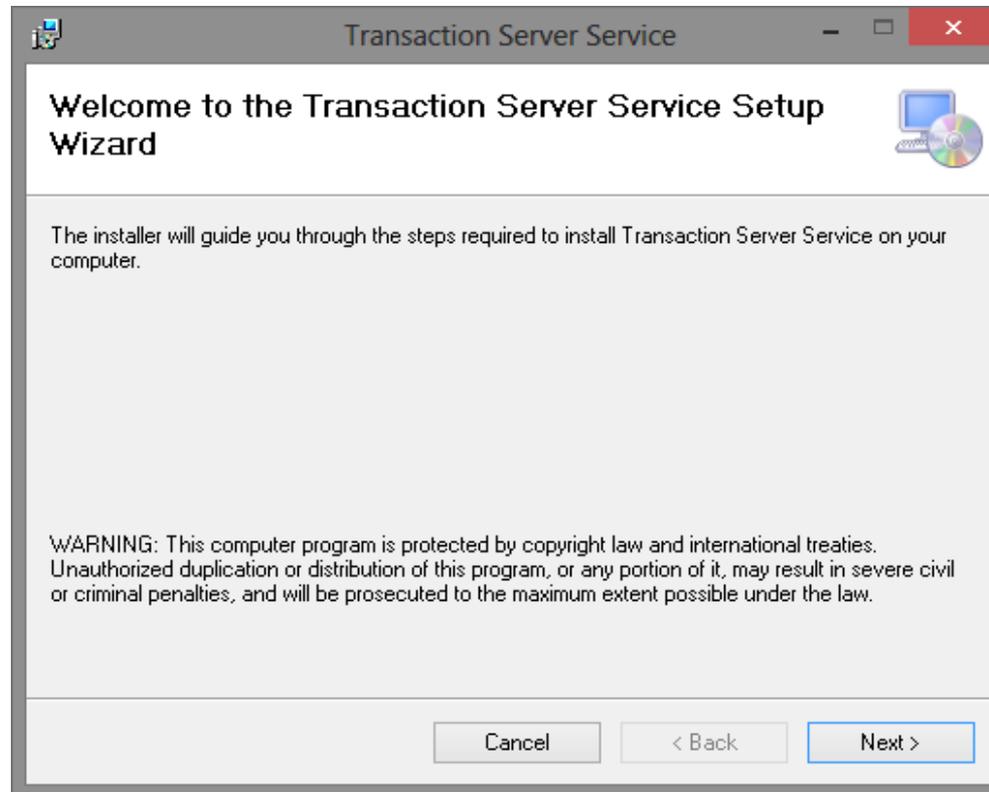
Installation Complete

VAULT ENTERPRISE SITE has been successfully installed.
Click "Close" to exit.

Cancel < Back **Close**



8) Installing the Service Transaction Server software. Click Next to install.

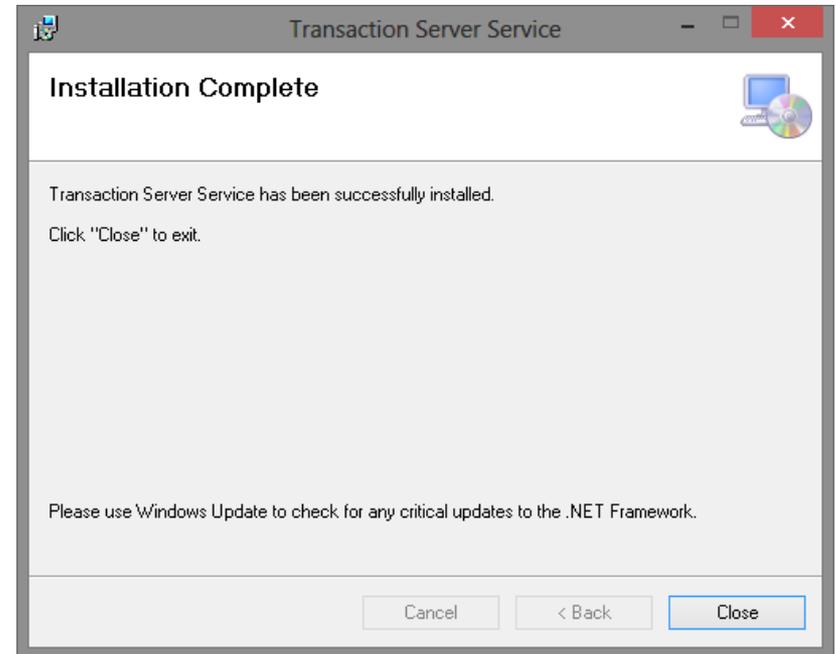
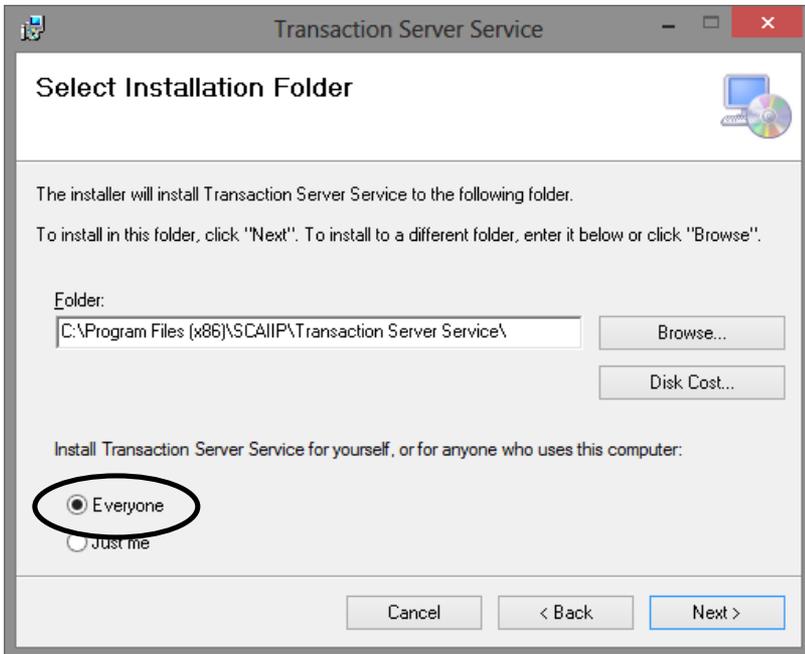


SOFTWARE INSTALLATION

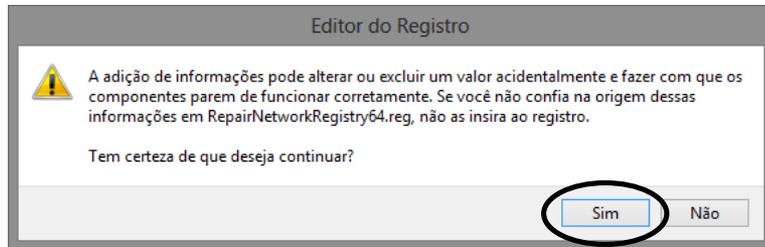


9) EVERYONE Select the option and click Next.

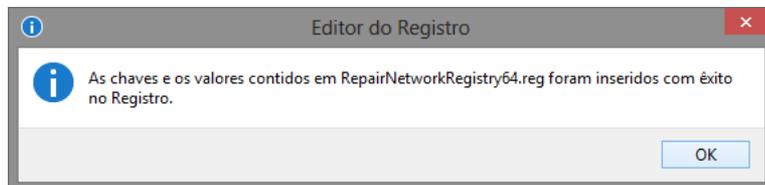
10) Click Close to enclose the facility.



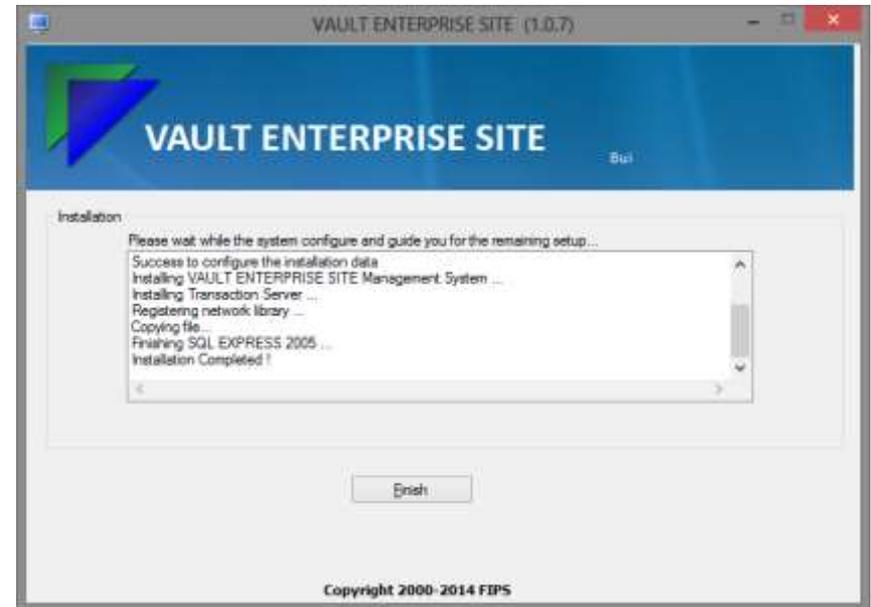
11) Click to register Dll Sim necessary to Vault software work with the controllers.



12) Check if the registry was made successfully.



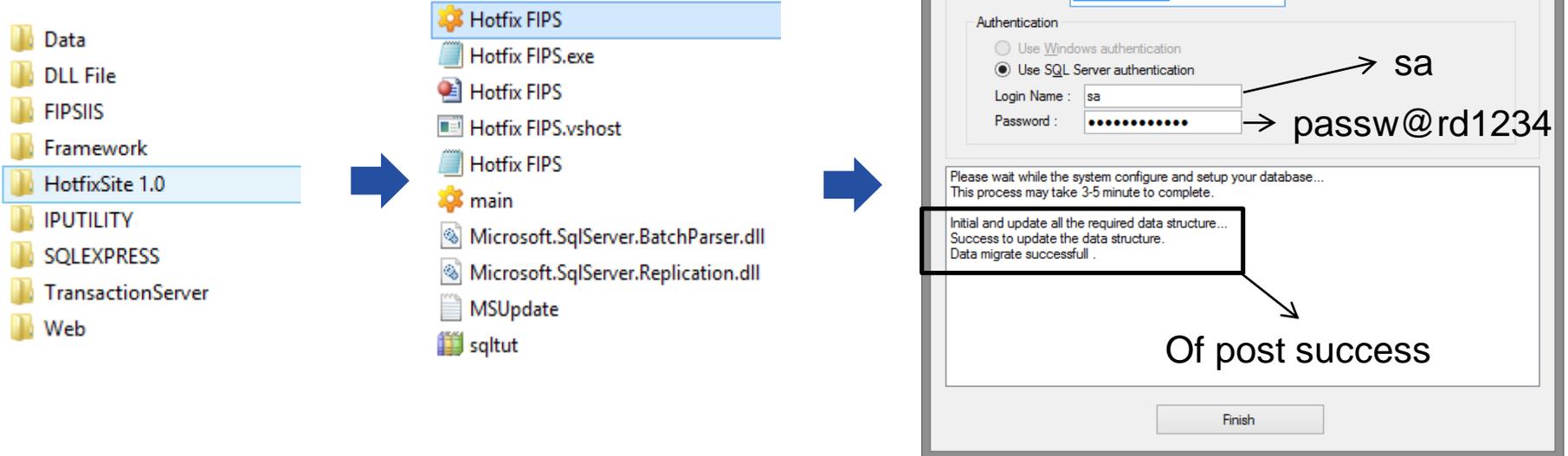
13) The facility is enclosed. Click Finish.



SOFTWARE INSTALLATION



11) Where is hacinedo a software update, we then updated the database structures. Open the installation folder and locate the folder HotfixSite 1.0. Click Hotfix FIPS.



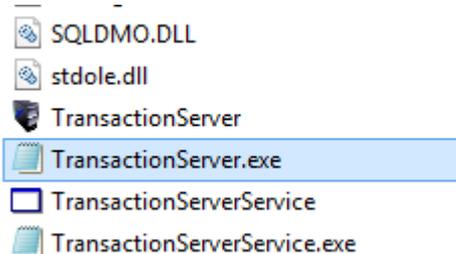
files

Configuration Files

If the installation is divided in two servers, an application and a database, we must change two files connection to the database, they are:

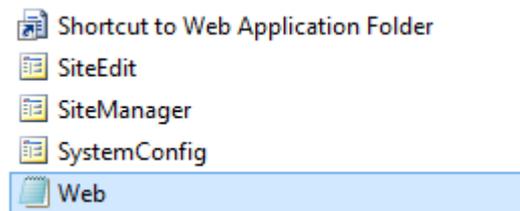
- TransactionServer.exe.config

C:\Program Files (x86)\VAULT\Transaction Server Service\



- Web.config

C:\inetpub\wwwroot\VAULTSITE\



TransactionServer.exe.config

C:\Program Files (x86)\VAULT\Transaction Server Service\

```
</setting>
<setting name="FVMSConnStr" serializeAs="String">
  <value>server=.\SQLEXPRESS;uid=sa;pwd=passwd1234;database=VisDB</value>
</setting>
<setting name="ConnStr" serializeAs="String">
  <value>server=.\SQLEXPRESS;uid=sa;pwd=passwd1234;database=DataDBEnt</value>
</setting>
```

Server = Database \ Instance

Uid= user database

Pwd= user's password database

Database= Name of the database

Web.config

C:\inetpub\wwwroot\VAULTSITE\

```
<add key="ReportMaxDays" value="60"/>  
<add key="connStr" value="server=. \SQLEXPRESS;uid=sa;pwd=passwd@rd1234;database=DataDBEnt"/>  
<add key="CamServer" value="N"/>  
<add key="GT" value="No"/>
```

Server = Database \ Instance

Uid= user database

Pwd= user's password database

Database= Name of the database

***CamServer**= Camera server

N = NUUO

M = Milestone

V = Verint

D = Digifort

**Check cam server version for integration*

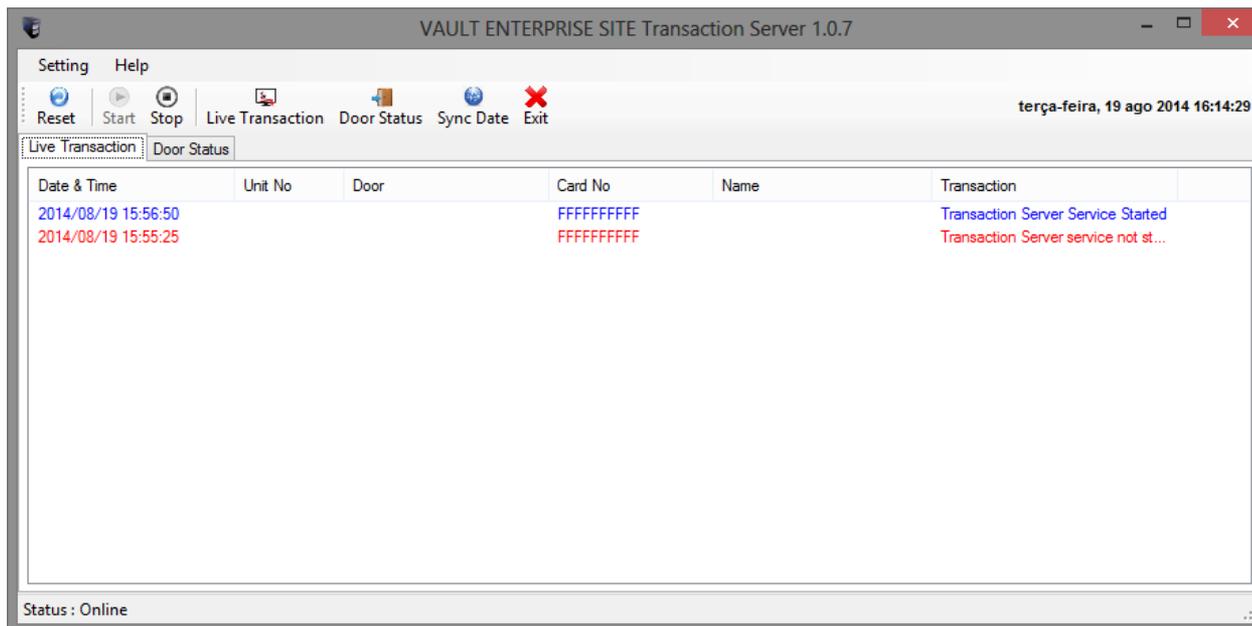
Software

Beginning with Enterprise Vault Site

1) Open the shortcut Service Transaction Server software.



2) Select the START button to start the service of communication with the database.

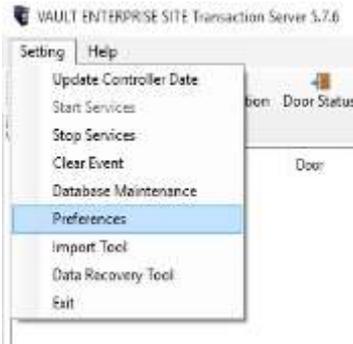


Site/Cloud Synchronize Data

Software



3) Go to setting > Preference



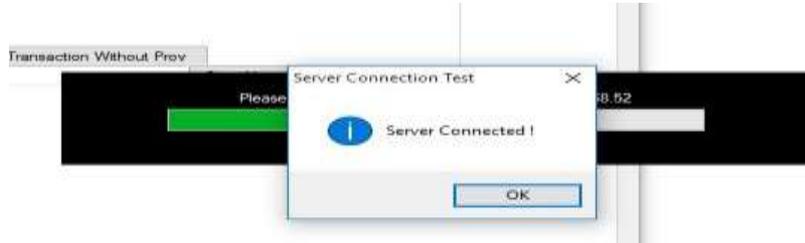
4) Under Enterprise Server tab

5) Enable server connection

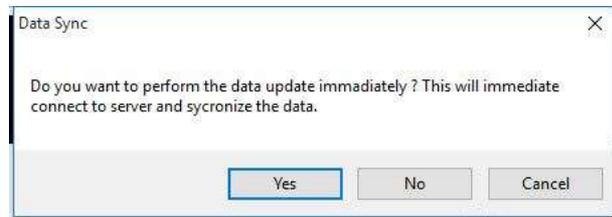
6) Enter Cloud IP and web port no



7) Click OK when the server connected



8) Click Yes to connect to server and sync data



9) Open (Cloud IP add)/vaultcentral

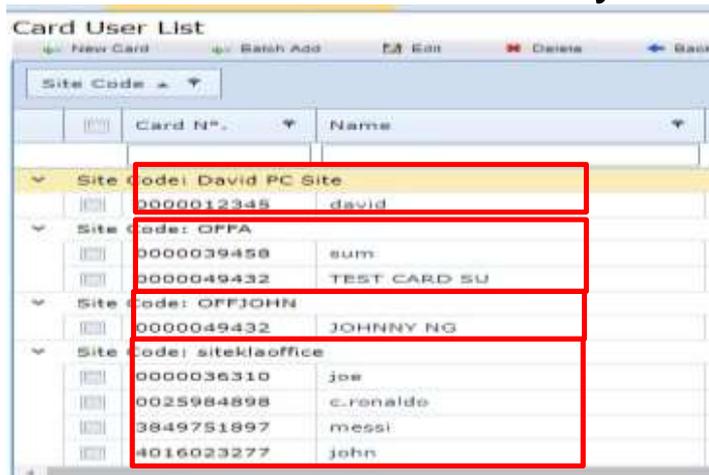
10) Default ID and Password is admin

11) Login to confirm data is sync

- 12) Open (Cloud IP add)/vaultcentral
- 13) Default ID and Password is admin
- 14) Login to confirm data is sync



- 15) All site are differentiate by site code



Site Code	Card N°	Name
Site Code: David PC Site	0000012345	david
Site Code: OFFA	0000039450	sum
	0000049432	TEST CARD SU
Site Code: OFFJOHN	0000049432	JOHNNY NG
Site Code: siteklaoffice	0000036310	joe
	0025984898	c.ronalde
	3849751897	messi
	4016023277	john

Login and Password



16) Open the Enterprise Vault Shortcut Site software.



17) Use the Login: and Password vault: vault (standard)

Login Screen - VAULT ENTERPRISE SITE



English

Login ID :*
Enter you Login ID

Password :*
Enter your password

Login

2014 © Copyright by VAULT

Software

**Sites
Management**

5) After login, the user has to add their site information.
Important: You must add the code of the site. Once recorded, you can not change the code of the site.

Gestión del Sitio

Configuración del Sitio	
Tipo de Usuario:*	<input type="text" value="SP"/>
Sitio Descripción:	<input type="text" value="SAO PAULO"/>
GMT del Sitio:*	<input type="text" value="(UTC-03:00) Brasília"/>
Sitio Puerta No:*	<input type="text" value="2003"/>
Modo de Lectura:*	<input type="text" value="3"/>
Tipo :	<input checked="" type="radio"/> Red <input type="radio"/> NDVR
URL:	<input type="text" value="Entre con la URL del NDVR"/>
ID del Login:	<input type="text" value="NDVR - ID de Login"/> Contraseña de Login: <input type="text"/>
Pais:*	<input type="text" value="Brazil"/>
Dirección:	<input type="text" value="Alameda Santos, 274"/>
Complemento:	<input type="text" value="Apto. 200"/>
Ciudad:	<input type="text" value="OSASCO"/> Provincia: <input type="text" value="SAO PAULO"/>
Código Postal:	<input type="text" value="08980-123"/> Correo: <input type="text" value="fernando@vaultbr.com"/>
Reserva:	<input type="text" value="011-38467087"/> Ramal: <input type="text" value="234"/>
Fax No:	<input type="text"/>
Persona de Contacto:	<input type="text" value="Fernando"/> Móvil: <input type="text" value="011-99999999"/>

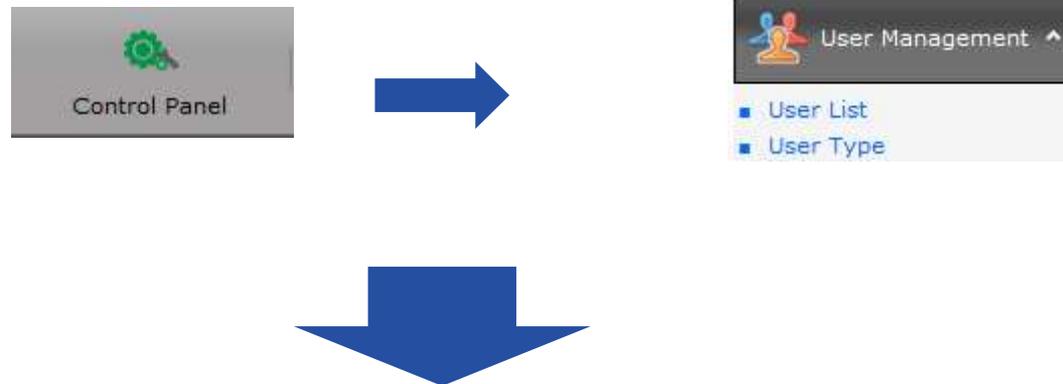
Software

**Add user
software**

Add user software



6) After login, the user has to add their site information.
Important: You must add the code of the site. Once recorded, you can not change the code of the site.



User Type

Drag a column header here to group by that column				
<input type="checkbox"/>	No	User Type	<input type="text"/>	Description
<input type="checkbox"/>	1	Enterprise System Admin		Enterprise System Admin

Here you can add new types of users with permissions distinct.

Add user software



User Type

User Type:

Description:

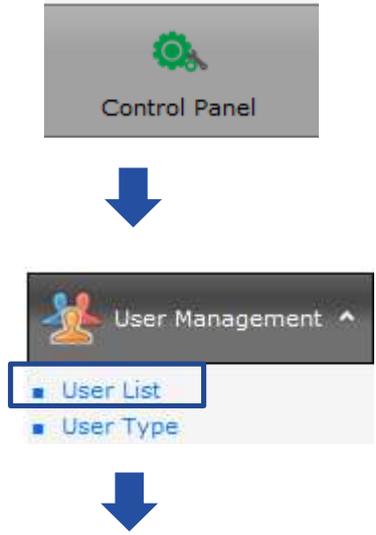
→ Type of user

<input type="checkbox"/> All	<input type="checkbox"/> View	<input type="checkbox"/> Add	<input type="checkbox"/> Edit	<input type="checkbox"/> Delete	<input type="checkbox"/> Export
Site Manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Card User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temporary Card	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temporary Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temporary Card Reserv List	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Controller	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Time Zone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Time Set	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lift Access Interval	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Holiday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm holiday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Floor Plan	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System User Type	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

→ permits



Add user software



System User

User Detail

User Login ID :

Login Password:

User Role:

Site Code:

- User must change password at next login
- User cannot change password
- Password never expires
- Account is disabled

User List

Drag a column header here to group by that column		
<input type="checkbox"/>	No	User ID

Software

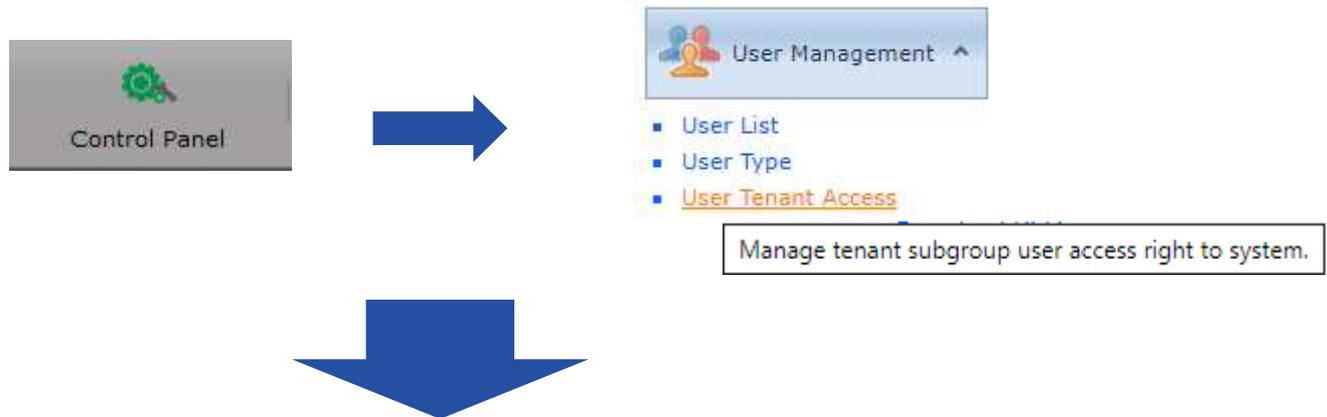
**Add Tenant
user software**

Add Tenant user software



6) After login, the user has to add their site information.

Important: You must add the code of the site. Once recorded, you can not change the code of the site.



Tenant User Access List

Drag a column header here to group by that column			
<input type="checkbox"/>	No	Login ID	Company Name
<input type="checkbox"/>	1	tenant	complicated

Here you can add new types of Tenant users with few controls only.

Add Tenant user software



Tenant User Access

User Detail

User Login ID:

Login Password:

Company Detail

Company Name:

Building: Floor / Unit No:

Address 1:

Address 2:

Office No: Ext:

Fax No: Contact Person:

Remark:

Door Access Controller Group

Door Controller:

User must change password at next login

User cannot change password

Password never expires

Account is disabled

Tenant ID and Password

Selected Controller only

Save and User is ready to Login to the software

INITIALIZE & LOGIN



- 1) Open any web browser such as, Internet Explorer, Firefox, Google Chrome, Safari.
- 2) serverIP/vaultsite/tenant/Login.aspx
- 3) Login with your Login ID and Password

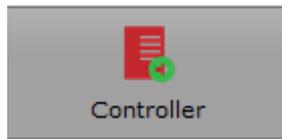
192.168.9.9/vaultsite/tenant/Login.aspx

The screenshot shows a web browser window titled "Login Screen". The page features the VAULT logo in the top left corner and a language dropdown menu set to "English" in the top right. Below the logo, there are two input fields: "Login ID :*" and "Password :*", each with a placeholder text "Enter your Login ID" and "Enter your password" respectively. A "Login" button is positioned below the password field. At the bottom of the page, the text "2019 © Powered by VAULT" is displayed.

Software

**Add
Controllers**

Adding a controller



Controller List

New Controller Add Ext Manual Edit Delete Pdf Xls

Drag column header to group that column

	Site Code	Unit No	Name	Description

- 1 Add ID 0 controller using the automatic search for the Broadcast command.
- 2 Add ID 1 controller using the automatic search for the Broadcast command.
- 3 Add ID 0 or 1 controller using UDP unicast.
- 4 Edit controllers.

Adding a controller



- 1
 - 2
- Adding one controller / expansion automatically.

Controller Searching

IP Address	Mac Address	Firmware	Type	Controller ID	Status
192.168.0.99	0.0.21.74.213.99	T5.99.6A9STFI	D	0	■
192.168.0.54	0.26.21.43.144.54	R5.91.6A9SFFI	D	0	■
192.168.0.50	0.26.21.53.212.50	R5.91.5ADSJFI	D	0	■
192.168.0.51	0.26.21.43.212.51	R5.91.6ABSeFI	D	0	■
192.168.0.200	0.52.21.113.124.200	R5.99.5A9DAFI	D	0	■
192.168.0.251	0.52.21.113.124.251	T4.99.62DSJFI	D	0	■
192.168.0.47	0.32.21.13.201.47	T4.99.62RS4PL	S	0	■
192.168.0.44	0.52.21.13.204.44	T4.99.62DSJFI	D	0	■

Refresh Add Cancel



Network

Controller Detected : 192.168.0.99 . Change the setting to your desired network configuration and press next to continue.

IP Address:*	192.168.0.99	Firmware:*	T5.99.6A9STFI
Mac Address:*	0.0.21.74.213.99	Subnet Mask:*	255.255.255.0
Gateway:*	192.168.0.1	Dest TCP Port:*	1008
Server IP Address:*	192.168.0.140	SRC UDP Port:*	2003
SRC IP:*	255.255.255.255	Info Desk Port:*	2003
Info Desk IP:*	255.255.255.255		

Next >>



Sistema

Cancelar

Notas : Por favor, espere enquanto los datos son procesados en el sistema. No oprima el botón Volver o cierre hasta que termine.

Adding a controller



3 → Adding one controller / manual expansion.

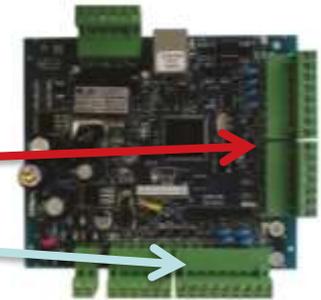
 **Controller Wizard**

Please enter the controller IP Address you want to register. Door Wizard w

Controller IP Address :

Controller Type :

-
-



Network

Controller Detected : 192.168.0.99 . Change the setting to your desired network configuration and press next to continue.

IP Address:*	<input type="text" value="192.168.0.99"/>	 *
Mac Address:*	<input type="text" value="0.0.21.74.213.99"/>	 *
Gateway:*	<input type="text" value="192.168.0.1"/>	 *
Server IP Address:*	<input type="text" value="192.168.0.140"/>	 *
SRC IP:*	<input type="text" value="255.255.255.255"/>	
Info Desk IP:*	<input type="text" value="255.255.255.255"/>	
Firmware:*	<input type="text" value="T5.99.6A9STFI"/>	 *
Subnet Mask:*	<input type="text" value="255.255.255.0"/>	
Dest TCP Port:*	<input type="text" value="1008"/>	
SRC UDP Port:*	<input type="text" value="2003"/>	
Info Desk Port:*	<input type="text" value="2003"/>	

Adding a controller



Adding a controller

1) Adding a controller / manual expansion.

General Module.

Controller Profile

192.168.0.99 :

Controller Details

Setting

Network Configuration

Camera Setting

Alarm Config

IO Config

Controller Name:* MAIN DOOR

Description:* MAIN DOOR

Site Control:* OFFA

Unit No:* 11

IP Address: 192.168.0.99

Mac Address: 0.0.21.74.213.99

Controller ID: 0

Firmware: T5.99.6A9STFI

Controller Status : Active

Controller Type

Alarm:

I/O:

Lift:

LCD:

Rack:

Adding a controller



2) The menu and other tools.

192.168.0.99 :

The screenshot shows the VAULT web interface with the following configuration options:

Controller Details	Setting	Network Configuration	Camera Setting	Alarm Config	IO Config
Controller Configuration					
Open Time (s) :	<input type="range"/>	Release Time (s) :	<input type="range"/>		
Open Time (s) :	<input type="text" value="5"/>	Release Time (s) :	<input type="text" value="2"/>		
Lock Release TZ:	<input type="text" value="00"/>	Push Button TZ:	<input type="text" value="01"/>		
Antipassback:	<input type="text" value="00"/>	Global Antipassback Group:	<input type="text" value="Disable"/>		
Rack Control:	<input type="text" value="1-16"/>				

Open Time : How long can the door be left open until an alarm is generated.

Release Time: time relay control lock.

Lock Release TZ : Can be programmed a TZ for the lock becomes unlocked for that time period. 00 -> Always shut / 01-> Always released.

Antipassback: Each parent has antipassback location that can be enabled by TZ. (anti dual input / dual output).

Push Button TZ: TZ to release the door by Button (00 -> Always disabled / 01-> Always enabled).

Global Antipassback Group: When we have more than one way to enter / exit a room and want to make the control antipassback, you must create a group with controllers belonging to this environment. Ex .: Group turnstiles reception.

Control of Rack: Only used for Rack controllers.

Adding a controller



3) The menu tools and other.

Mode

Fire Alarm: <input type="checkbox"/> Enable	Guard Tour: <input type="checkbox"/> Enable
Buzzer Door Release: <input type="checkbox"/> Enable	Card Lockout: <input type="checkbox"/> Enable
Auto Pin Access: <input type="checkbox"/> Enable	Report Mode: <input type="checkbox"/> Enable
Emergency Card Mode: <input type="checkbox"/> Enable	

Card & Pin

Card & Pin : Enable

Card & Pin Entry TZ: ▼

Card & Pin Exit TZ: ▼

Mode

- **Fire Alarm** : Enables parent to be part of a group of fire.
- **Open Door Buzzer**: Enables or disables buzzer during Lock Release TZ.
- **Acceso Auto Pin**: Enables password function to the parent. Passwords up to 10 pre-programmed by the parent.
- **Guard Tour** : Enables guard tour controller .
- **Card Lock** : Blocks user card after 3 attempts to circumvent the antipassback.
- **Report Mode** : Writes markings point in text format, separating them by day.
- **Emergency Card Mode** : special card, when touched onto a reader on a specific controller, will trigger the “security off”

Card & Pin

- **Card & Pin**: Enables dual authentication for card use and password. (* Keyboard should work in Rosslare format)
- **Card & Pin Entry TZ** : set the time to enable card and pin mode by TZ for the entry reader.
- **Card & Pin Exit TZ**: set the time to enable card and pin mode by TZ for the Exit reader.

Adding a controller



4) The menu and other tools.

Dual Card Mode

Dual Card: Enable

Entry Reader Dual Card TZ: Exit Reader Dual Card TZ:

Pin No

1.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	6.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>
2.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	7.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>
3.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	8.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>
4.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	9.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>
5.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	10.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>

Double Authentication Mode

Double Authentication : Enables dual authentication to the parent. This feature is specific to the firmware T5.96DAFI.

- Entry Reader Dual Card TZ**: Enables authentication for double entry into a particular TZ configured by the user.
- Exit Reader Dual Card TZ** : Enables authentication to double Exit in a given TZ configured by the user.

Pin No

Per controller, we can have up to 10 pre-programmed passwords for access in a particular time zone. To use this feature you need to use a keyboard and enable Acceso Auto Pin mode.

Adding a controller



5) Config Network Configuration

192.168.0.99 :

Controller Details	Setting	Network Configuration	Camera Setting	Alarm Config	IO
Retrive Network Setting		Set Network Setting			
IP Address:	192.168.0.99				
Mac Address:	0.0.21.74.213.99	Firmware:	T5.99.6A9STFI		
Gateway:	192.168.0.1	Subnet Mask:	255.255.255.0		
Server IP Address:	192.168.0.140	Dest TCP Port:	1008		
SRC IP:	255.255.255.255	SRC UDP Port:	2003		
Info Desk IP:	255.255.255.255	Info Desk Port:	2003		

IMPORTANT

After modifying the parameters of the parent network, the user must click the Set Network Configuration to the new parameters are sent to the controller.

To learn the current configuration of the network controller, the user must click on the Retrive Network Setting

Adding a controller



5) Camera Setting

192.168.0.99 :

Controller Details	Setting	Network Configuration	Camera Setting	Alarm Config	IO Config
--------------------	---------	-----------------------	----------------	--------------	-----------

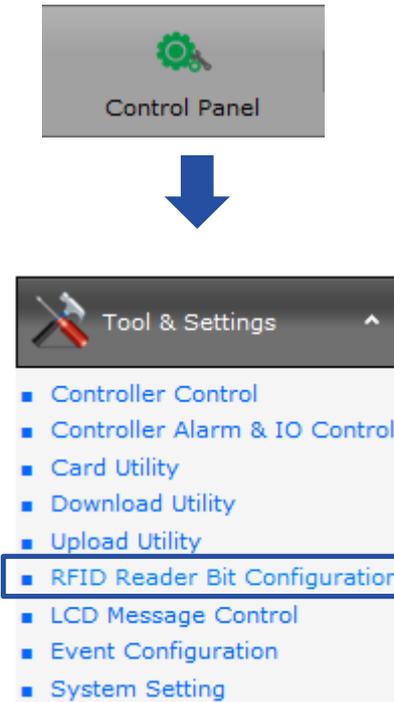
Entry Camera:	<input type="text" value="Null"/>	<input type="text" value="Null"/>	<input type="text" value="Null"/>
Exit Camera:	<input type="text" value="Null"/>	<input type="text" value="Null"/>	<input type="text" value="Null"/>

You can add a camera input and output for each parent, so that when the access is kept a log of the event with video. (Images are always stored in the CCTV server.)

Software

**RFID Read
Mode**

RFID Read Mode



Settings

* Reader Mode needs to be configured to work under different installer if you not sure how it works.

Reader Mode: 03 - Wiegand 34 bits (with facility code)

Network Mode: 03 - Wiegand 34 bits (with facility code)

Hardware Mode: 04 - Wiegand 34 bits (without facility code)

Parity bit (even): 05 - Wiegand 42 bits (without facility code)

Total bits - Parity: 06 - Wiegand 34 bits (with 5 Digit Card No)

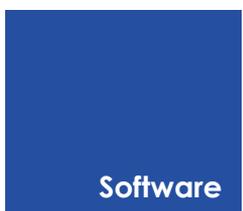
07 - Wiegand 32 bits (with 5 Digit Card No)

Protocols available to controllers:

- Wiegand 26, 32 , 34 or 42 bits

Software

Config. Time
Set



Config. Time Set



- Controller Management ^
 - Controller List
 - Time Set**
 - Time Zone
 - Lift Access Zone
 - Holiday
 - Alarm Holiday
 - IO Output Type
 - IO Output Trigger Group



Time Set No	Time Interval 01	Time Interval 02	Time Interval 03	Description
00	00:00 - 00:00	00:00 - 00:00	00:00 - 00:00	No Access Time Set
01	00:00 - 23:59	00:00 - 00:00	00:00 - 00:00	Free Access Time Set



Controller Time Set

Timer Setting

Time Set No:*

Description:

Interval 1	Interval 2	Interval 3
From Hour: <input type="text" value="00"/> Minute: <input type="text" value="00"/> To Hour: <input type="text" value="00"/> Minute: <input type="text" value="00"/>	From Hour: <input type="text" value="00"/> Minute: <input type="text" value="00"/> To Hour: <input type="text" value="00"/> Minute: <input type="text" value="00"/>	From Hour: <input type="text" value="00"/> Minute: <input type="text" value="00"/> To Hour: <input type="text" value="00"/> Minute: <input type="text" value="00"/>

You can store up to 99 Time Set on the controller settings, and each can have up to three valid intervals.

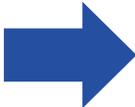


Configure. Time Zone



Controller Management ^

- Controller List
- Time Set
- Time Zone**
- Lift Access Zone
- Holiday
- Alarm Holiday
- IO Output Type
- IO Output Trigger Group



Controller Time Zone

Time Zone

Time Zone No:*

Description:

Week View

Monday: Friday:

Tuesday: Saturday:

Wednesday: Sunday:

Thursday:

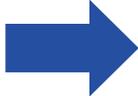
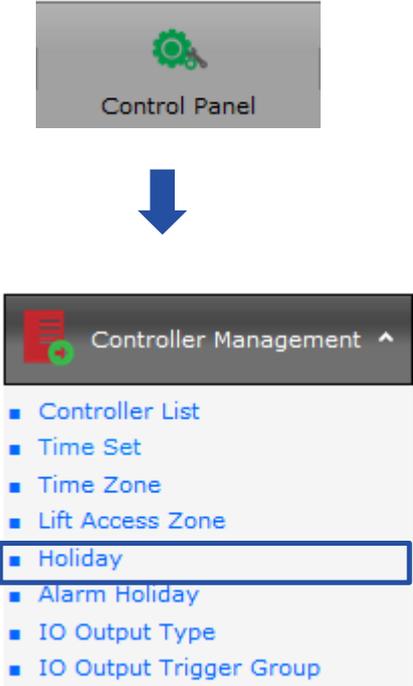


Time Zone Detail

Time Zone No : 02

Day	Time Set No:	Time Setting Value		
Monday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Tuesday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Wednesday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Thursday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Friday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Saturday	00	00:00 - 00:00	00:00 - 00:00	00:00 - 00:00
Sunday	00	00:00 - 00:00	00:00 - 00:00	00:00 - 00:00

In this example, the User TZ will be Monday to Friday working hours using previously created, and weekend and holidays will default to 00 (No Access) level.



Holiday

Holiday Detail

Holiday Name:

Site Code:

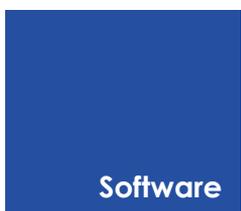
Date

From	Month: <input type="text" value="12"/>	Day: <input type="text" value="24"/>
To	Month: <input type="text" value="12"/>	Day: <input type="text" value="25"/>
Time Set :	<input type="text" value="00 - No Access Time Set"/>	

In this example, on 24/12 and 25/12 will be considered as a holiday. In this case, for visitors and contractors. Employees to be obeyed their respective TZ.

Software

Access Level



Access Level



Group Management ^

- Group Controller Access Level
- Group Lift Access Level**
- Group Global-Antipassback
- Group Fire Alarm
- Group Delete Card
- Group Emergency Card



Group Access Level

Controller Access Setting

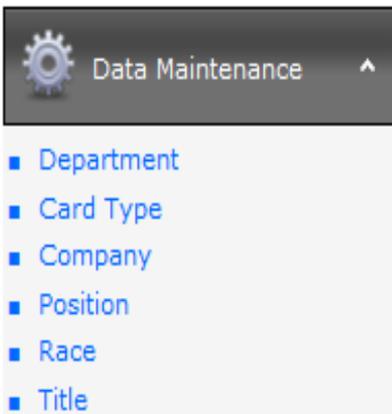
Group No: 01 (Total : 9 Controller)			Group Access No: * <input type="text" value="01"/>	
189 OFFA 01 ALARM CONTROLLER OFFA 01 BACK DOOR CONTROLLER OFFA 01 BARRIER CONTROLLER OFFA 01 EMER-2 OFFA 01 EMERGENCY DOOR CONTROLLER OFFA 01 LIFT CONTROLLER OFFA 01 MAIN DOOR OFFA 01			Description: <input type="text" value="FREE ACCESS"/> Site Code: <input type="text" value="OFFA"/>	
	Controller	Description	Site Code	Time Zone
<input checked="" type="checkbox"/>	189		OFFA	<input type="text" value="01"/>
<input checked="" type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA	<input type="text" value="01"/>
<input checked="" type="checkbox"/>	BACK DOOR CONTROLLER	BACK DOOR TESTING CONTROLLER	OFFA	<input type="text" value="01"/>
<input checked="" type="checkbox"/>	BARRIER CONTROLLER	BARRIER TESTING CONTROLLER	OFFA	<input type="text" value="01"/>
<input checked="" type="checkbox"/>	EMER-2		OFFA	<input type="text" value="01"/>
<input checked="" type="checkbox"/>	EMERGENCY		OFFA	<input type="text" value="01"/>
<input checked="" type="checkbox"/>	EMERGENCY DOOR CONTROLLER	EMERGENCY DOOR TESTING CONTROLLER	OFFA	<input type="text" value="01"/>
<input checked="" type="checkbox"/>	LIFT CONTROLLER	LIFT TESTING CONTROLLER	OFFA	<input type="text" value="01"/>
<input checked="" type="checkbox"/>	MAIN DOOR	TESTING DOOR CONTROLLER	OFFA	<input type="text" value="01"/>
> Group No: 02 (Total : 1 Controller)				
> Group No: 03 (Total : 1 Controller)				

Add the controllers for each pattern group you want to create, placing their desired time zone for each parent. Can add up to 999 standard groups.

IMPORTANT: To delete an access level, we must clear the controller, delete the description and click Save.

Software

Card User



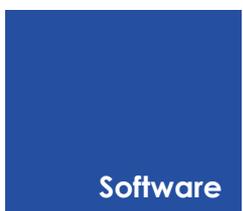
Data Maintenance ^

- Department
- Card Type
- Company
- Position
- Race
- Title

Department List

Drag a column header here to group by that column			
<input type="checkbox"/>	No	Department Code	Description
<input type="checkbox"/>	1	Department	Department
<input type="checkbox"/>	2	AD	ADMIN
<input type="checkbox"/>	3	ACC	ACCOUNT

First, we register all departments, types of word cards, company, office, Nacionalidad and title, and then do the registration cards



Card User



Grupo de doble autenticación



Card User List

Add new card

Add batch of cards (Ex. 1-1000)

Card Info | Employee Details | Access Level | Custom Fields



Name & Card number

Card No:*

Card Name:*

Site Control:*

Rack Access Level

Releasing Antipassback

Card Properties

Card Type:

Card Pin No:*

Fingerprint Mode:

Bypass Antipassback: Enable

Alarm Card: Enable

Guard Tour Card: Enable

Card Status: Enable

Dual Card Group:

Rack Access Level:

Card Expiry Status: Non Expired

Emergency Card Type: Enable

Expired Date (dd-MM-yyyy):

Dual Authentication Group

Expiration Date

Card Profile

Card Info	Employee Details	Access Level	Custom Fields
Employment			
Staff No:	<input type="text"/>		
Title:	<input type="text" value="Mr"/>	Position:	<input type="text" value="Manager"/>
NRIC No:	<input type="text"/>	Passport No:	<input type="text"/>
EPF No:	<input type="text"/>	Socco No:	<input type="text"/>
Department:	<input type="text" value="Department"/>	Company Name:	<input type="text" value="Company"/>
Gender:	<input type="text" value="Male"/>	Race:	<input type="text" value="Unknow"/>
Date Of Birth (dd-MM-yyyy):	<input type="text"/>	Marital Status:	<input type="text" value="Single"/>
Joining Date (dd-MM-yyyy):	<input type="text" value="10-10-2014"/>	Resign Date (dd-MM-yyyy):	<input type="text"/>
Contact			
Address :	<input type="text"/>		
Adjunct:	<input type="text"/>		
Postal Code:	<input type="text"/>	City:	<input type="text"/>
State:	<input type="text"/>	Country:	<input type="text"/>
Email:	<input type="text"/>		

General information of cardholders

Card User



Configuring the group for access

The Apply button searches for the standard information group 01, for example.

Card Profile

Card Info | Employee Details | Access Level | Custom Fields

Door Access | Lift Access

Group Access No: 01 [v] Apply Custom Mode
Site Code: OFFA [v] Reset

Ex. -> 01 = Access 24 hrs

#	Controller	Description	Site Code	Time Zone
<input type="checkbox"/>	189		OFFA	00 [v]
<input type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA	00 [v]
<input type="checkbox"/>	BACK DOOR CONTROLLER	BACK DOOR TESTING CONTROLLER	OFFA	00 [v]
<input type="checkbox"/>	BARRIER CONTROLLER	BARRIER TESTING CONTROLLER	OFFA	00 [v]

Select controller

Permits for Timezone

The settings of the user access level for each user are different.

Card User



We can have up to 5 custom fields for general use, to enable them, we should go

■ System Setting

System Preference and Configuration

General Setting | Email Notification | Card User Custom Field

Custom Field Setting

Enable: <input checked="" type="checkbox"/>	Field name: TEST	<input checked="" type="checkbox"/> Required field
Enable: <input type="checkbox"/>	Field name: Max 50 character	<input type="checkbox"/> Required field
Enable: <input type="checkbox"/>	Field name: Max 50 character	<input type="checkbox"/> Required field
Enable: <input type="checkbox"/>	Field name: Max 50 character	<input type="checkbox"/> Required field
Enable: <input type="checkbox"/>	Field name: Max 50 character	<input type="checkbox"/> Required field



Card Profile

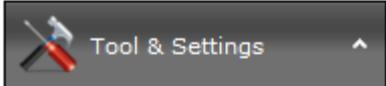
Card Info | Employee Details | Access Level | Custom Fields

TEST:

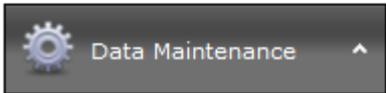
Software

**Installing /
handling
cards**

Install card



- Controller Control
- Controller Alarm & IO Control
- **Card Utility**
- Download Utility
- Upload Utility
- RFID Reader Bit Configuration
- LCD Message Control
- Event Configuration
- System Setting



Card Utility

Card Details

Card No:

Site Code:

Download Option

- Clear all existing card before download.
- Follow card user access right
- Delete card user access right
- Free Access

Controller List

<input type="checkbox"/>	Controller	Description	Site Code	IP Address	Controller ID
<input type="checkbox"/>					
<input type="checkbox"/>	189		OFFA	192.168.0.189	0
<input type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA	192.168.0.51	0
<input type="checkbox"/>	BACK DOOR CONTROLLER	BACK DOOR TESTING CONTROLLER	OFFA	192.168.0.44	1

Controllers available to Download.

Manage the access level of the card



- Card Management
 - Card User
 - Temporary Card
 - Temporary Access
 - Reserv Temporary card
 - Card Access Batch Update**
 - Card Location Search



Filter to change the access level of a particular department / company

Card Search

* Select the card range you want . Use the quick filter to speed up your search and select the records you want.

Card No	Name	Department	NRIC	Staff No	Position
0000039158	SELVI	TECH	791202085254	001	Normal Sta



New access level to be used for the group

Batch update of Cards

Card Details

Card No : 0000039158

Site Code: OFFA

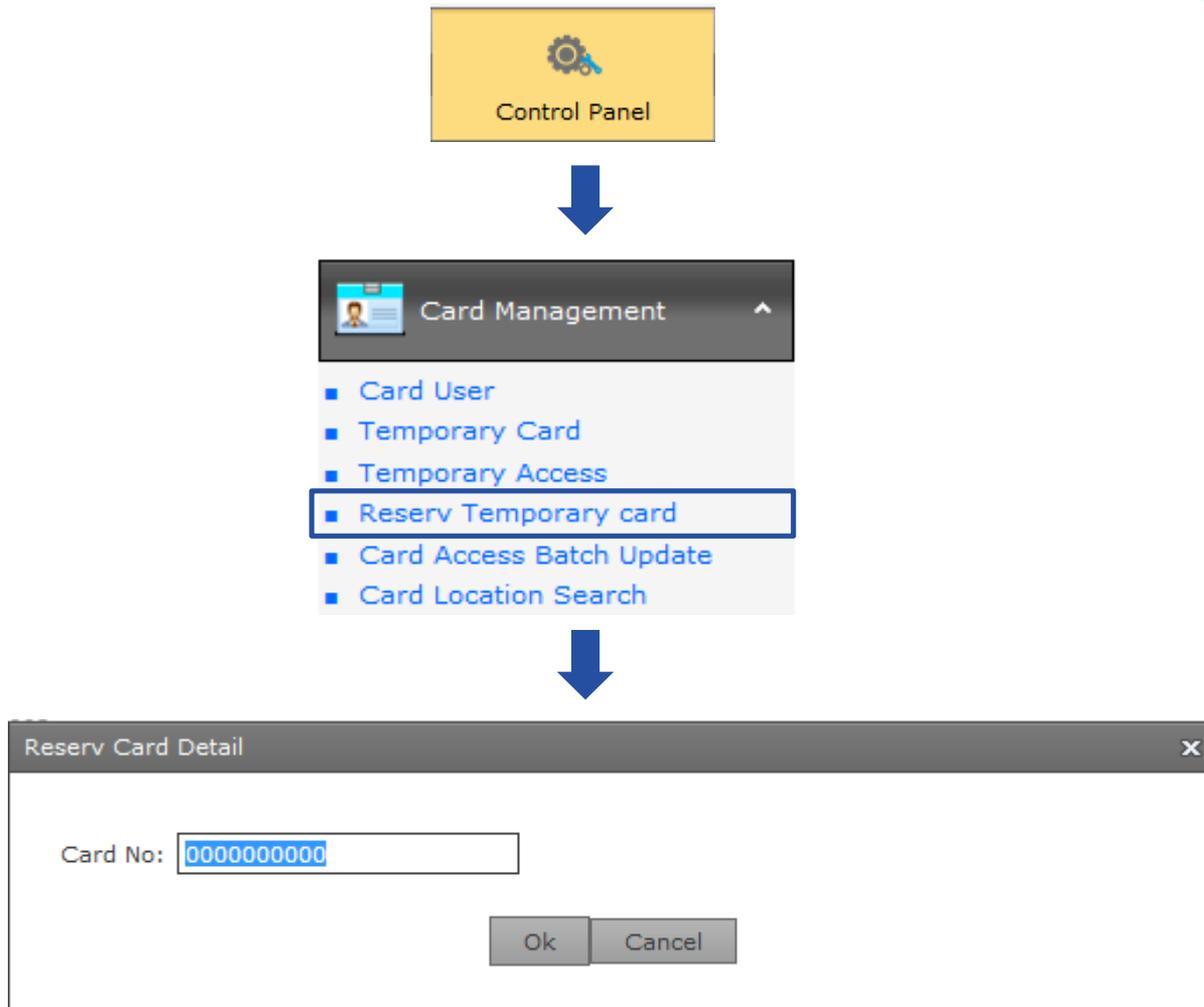
Door Access: Lift

Group Access No: 01

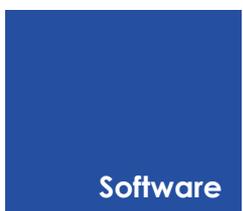
Site Code: OFFA

#	Controller	Description	Site Code	Time Zone
189			OFFA	00
	ALARM CONTROLLER	TEST ALARM & I/O	OFFA	00

Temporary Reserve Card



The reservation of temporary cards makes the operator can not use this card for other purposes (eg. Visitor, employee, etc.)



Temporary Card



Card Management

- Card User
- Temporary Card**
- Temporary Access
- Reserv Temporary card
- Card Access Batch Update
- Card Location Search

Manejo de tarjetas

- Usuario de tarjetas
- Tarjeta temporaria
- Acceso Temporario
- Tarjeta Temporaria de reserva
- Actualización de tarjetas de Acceso en Lote

Temporary Card

User information

Card Detail

Site Code: OFFA

Existing Card No: 0000039158

Staff Name : SELVI

NRIC: 791202085254

Department: TECH

Temporary Card Info

Temporary Card No: 45987

Expiry Date: 13/10/2014

Remark:

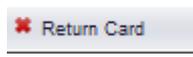
The date to be expired for the Temp card

Temporary Card

New Edit Return Card Pdf Xls

Drag a column header here to group by that column

	Staff Name	NRIC	Department
	SELVI	791202085254	TECH



Used to return the card use the employee

Temporary Access Level



- Card Management
- Card User
- Temporary Card
- Temporary Access**
- Reserv Temporary card
- Card Access Batch Update
- Card Location Search



Card Search

* Select the card you want . Use the quick filter

Card No	Name	Department
0000039158	SELVI	TECH

User information

Card Detail

Site Code: OFFA

Existing Card No: 0000039158

Staff Name : SELVI

NRIC: 791202085254

Department: TECH

Duration Time

Date From: 13-10-2014 Time: 12 00 AM

Date To: 23-10-2014 Time: 11 59 AM

Remark: VACATION

Temporary Access Access period

Door Access Lift Access

#	Controller	Description	Site Code	Time Zone
189			OFFA	00
	ALARM CONTROLLER	TEST ALARM & I/O	OFFA	00

Temporary permission

Software

**Utiliti to
Download
and Upload**

Utility Download



Download Utility

Antipassback, time to unlock, etc..

- Tool & Settings
- Controller Control
- Controller Alarm & IO Control
- Card Utility
- Download Utility**
- Upload Utility
- RFID Reader Bit Configuration
- LCD Message Control
- Event Configuration
- System Setting

Date Time	Controller Parameter	Time Zone	Time Set
Lift Access Zone	Holiday	Alarm Holiday	Rack Access Level
IO Output Trigger Grp	IO Output Type	Clear Command	

Next >>

Within the command - Smudge there are other parameter, such as Delete all cards, memory clean, unlock card, etc.

Clear Command

- Clear Alarm
- Clear Card
- Clear Visitor Card
- Clear Antipassback
- Clear Global-Antipassback
- Clear Lift Zone
- Clear LCD
- Clear Hardware Parameter
- Clear All Card Lockout
- Clear Specific Card Lockout
- Clear Controller Memory
- Clear Rack Access Group

Command used to send data from the database to the Controller.

Upload Utility



Control Panel

↓

Tool & Settings

- Controller Control
- Controller Alarm & IO Control
- Card Utility
- Download Utility
- Upload Utility**
- RFID Reader Bit Configuration
- LCD Message Control
- Event Configuration
- System Setting

Select the option below to upload the setting from controller.

Date Time	Time Zone	Time Set	Lift Access Zone
Holiday	Card User	Controller Firmware	Alarm Parameter
Controller Parameter	Global Antipassback Group	FIRE ALARM Group	Rack Access Level

Next >>

Command used to check the data recorded in the controller.



Control of Barriers



Select the option below to control your devices



Next >>

Used to lock the doors / barriers after a fire alarm.

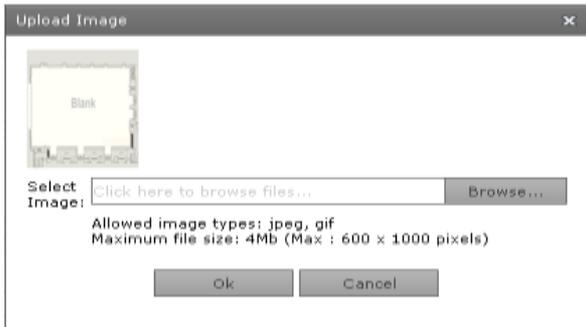
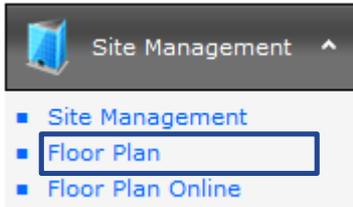
Software

Floor Plan

Add / Edit a Floor Plan

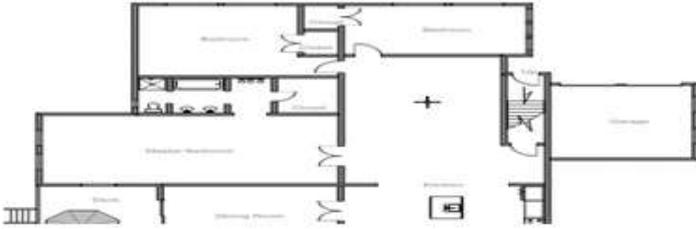


Floor Plan



Detail

142 Main Street



Upload

Floor Plan Name:* OFFICE

Description: OFFICE

Site Control:* OFFA



Important: You must give full permission (read, modify, delete, write) in the VAULT Enterprise folder so that the user can add a floor plan.

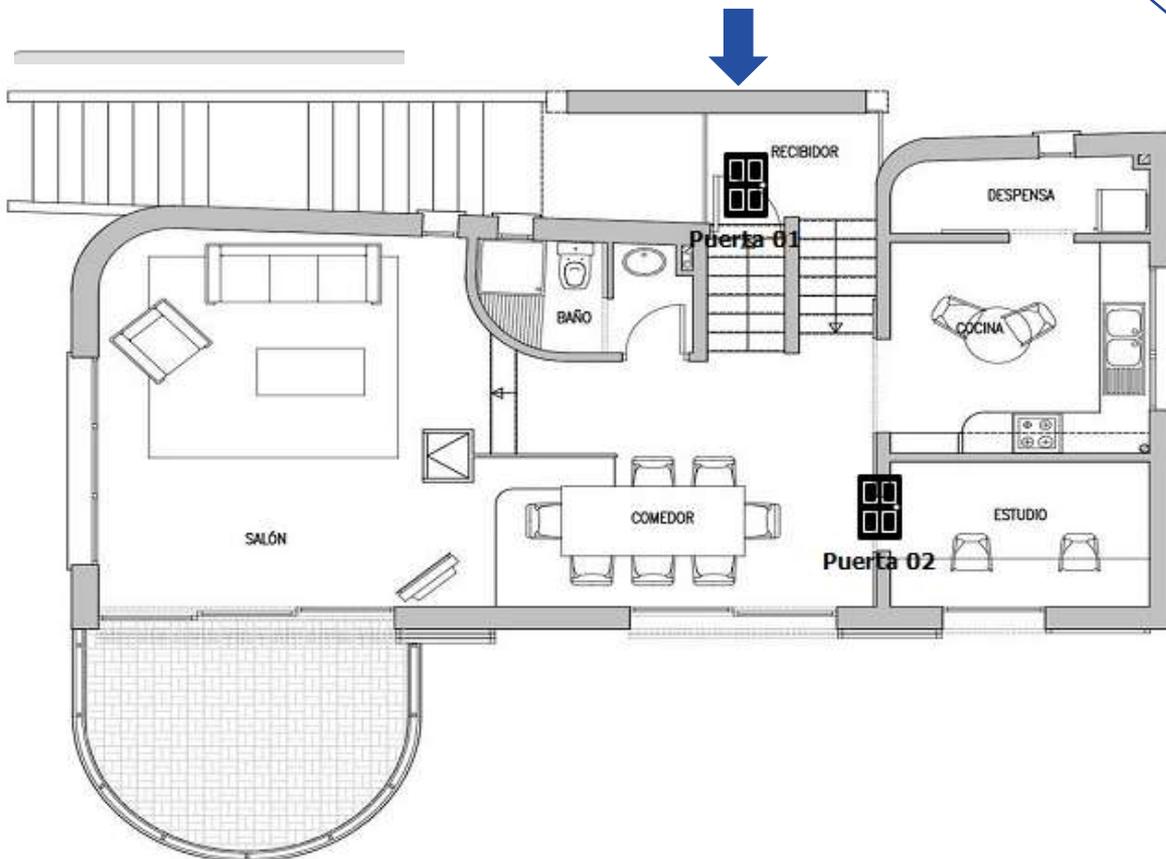
Add / Edit a plant controller



Floor Plan

Door :

Ok Cancel



Tool Bar

Save Close

OFFICE
OFFA

Door	<input type="button" value="+"/>	<input type="button" value="X"/>
Alarm	<input type="button" value="+"/>	<input type="button" value="X"/>
Camera	<input type="button" value="+"/>	<input type="button" value="X"/>
IO Input	<input type="button" value="+"/>	<input type="button" value="X"/>
IO Output	<input type="button" value="+"/>	<input type="button" value="X"/>

Max : 600 x 1000 pixels

Software

Floor Plan - Online



Floor Plan



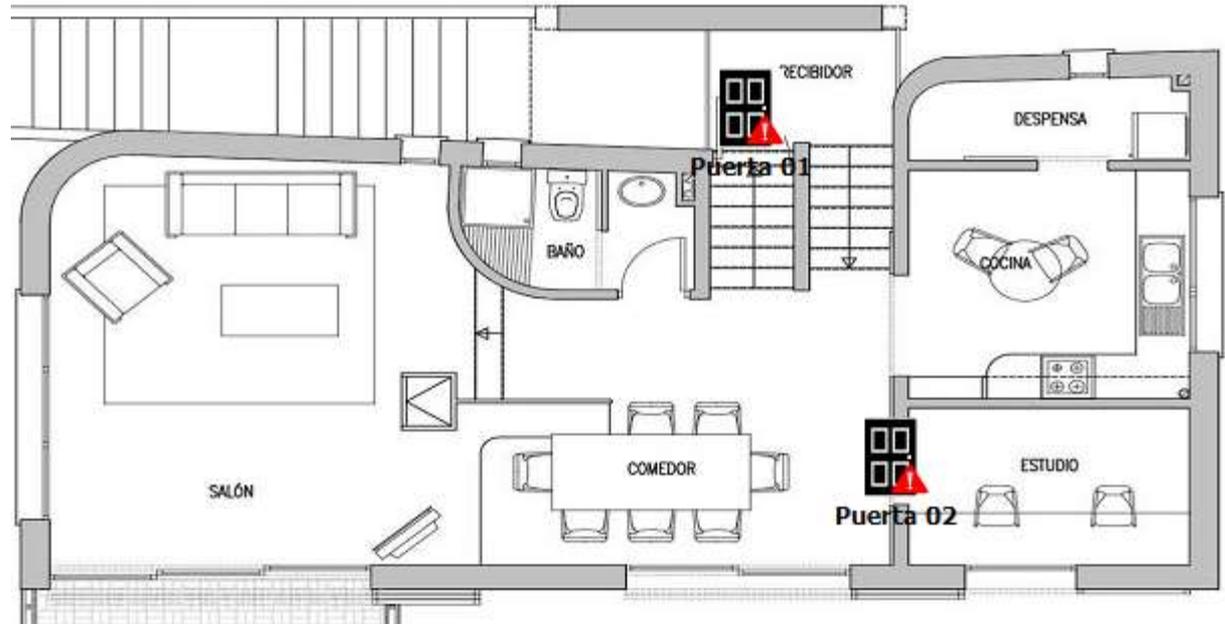
Tool Bar

Floor Plan Name :
OFFICE

Site Code :
OFFA

ALARM MONITOR

Start Stop



Transaction View

Pulse Door Security On Security Off Acknowledge Alarm Live Cam Playback

2014/10/13 08:30:17
MAIN DOOR

Transaction : **Controller Down**

Name :

Card No : FFFFFFFFFF

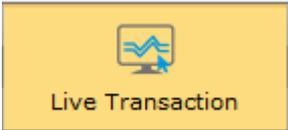
Site : OFFA

Close

Software

**Monitor
Online**

Monitor Online



Navigation menu with tabs: **2** Live Transaction, **3** Alarm List, **4** Card User Monitoring, **5** Controller Status

Buttons: Filter, Start, Stop, Acknowledge All Alarm Event, Alarm Manual Entry

#	Date & Time	Site	Controller	Card No	Name	Facility Code	Transaction
1	2014/10/13 16:59:20	OFFA	EMERGENCY	FFFFFFFF			Controller Down
	2014/10/13 16:59:19	OFFA	EMERGENCY DOOR CONTROLLER	FFFFFFFF			Controller Down



1 Transaction View

Buttons: Quick Register, Reset Antispassback, Acknowledge Alarm, Live Cam, Playback, Video Comparison

2014/10/13 17:09:34
189

Transaction: **Controller Down**

Name:

Card No: FFFFFFFFFF

Site: OFFA

[View Floor Plan](#)



2 Live Transaction Filter

Time Refresh: 1 Seconds

Site Code: OFFA

Controller:

Show Alarm Only:

Popup:

Sound:

Buttons: Apply, Close

3

#	Date & Time	Site	Controller	Card No	Name	Facility Code	Transaction
⚙	2014/10/13 17:19:55	OFFA	EMERGENCY DOOR CONTROLLER	FFFFFFFFF			Controller Down
⚙	2014/10/13 17:19:52	OFFA	189	FFFFFFFFF			Controller Down
⚙	2014/10/13 17:14:46	OFFA	EMERGENCY DOOR CONTROLLER	FFFFFFFFF			Controller Down

4

Location	BARRIER CONTROLLER	Date Time	2014/10/07 15:48:35
Valid Entry Access			
Name	SELVI	Department	TECH
Card No	0000039158	Position	Normal Staff
Staff No	001	Company	KLA TECH
<hr/>			
Location	BARRIER CONTROLLER	Date Time	2014/10/07 15:48:33
Valid Exit Access			
Name	SELVI	Department	TECH
Card No	0000039158	Position	Normal Staff
Staff No	001	Company	KLA TECH

Monitor Online



5

Live Transaction Alarm List Card Monitoring Controller Status

Site: OFFA Controller: Refresh

#	Controller	Site	IP Address	Controller ID	Status
189		OFFA	192.168.0.189	0	Offline -
	ALARM CONTROLLER	OFFA	192.168.0.51	0	Online -
	BACK DOOR CONTROLLER	OFFA	192.168.0.44	1	Online -

Shows whether the controller is online or offline the system

Config. Events



- Tool & Settings
- Controller Control
- Controller Alarm & IO Control
- Card Utility
- Download Utility
- Upload Utility
- RFID Reader Bit Configuration
- LCD Message Control
- Event Configuration**
- System Setting



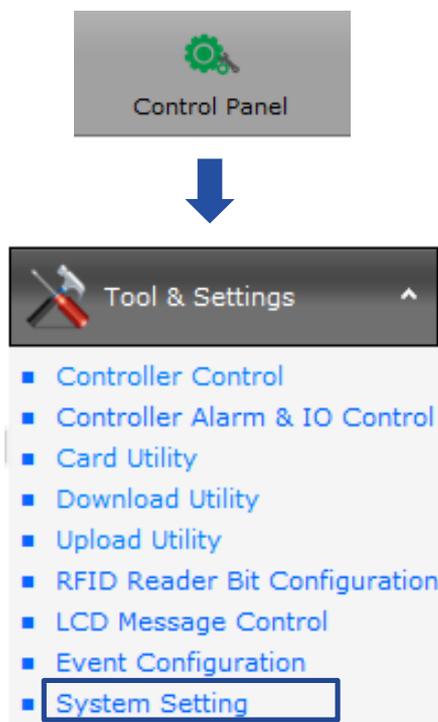
Settings

* Event setting and notification.

Event	Event Color	Pop-up	Email	SMS
Acknowledge alarm	#FF0000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Activated	#FF0000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Disable	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Enable	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Normal	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ALARM TYPE OUTPUT OFF	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ALARM TYPE OUTPUT ON	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Zone Activated	#FF0000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Zone Deactivated	#00FF00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AntiPassback Entry	#FF0000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

To facilitate monitoring, we can set so that when an alarm occurs, a pop-up is displayed on the screen along the local sound. Besides the possibility to send an email and SMS to preconfigured people.

Config. System



General Setting | Email Notification | Card User Custom Field

Facility Code

Enable Facility Code:

Facility Code 1:

Facility Code 2:

Facility Code 3:

Facility Code 4:

Facility Code 5:

Facility Code 6:

Facility Code 7:

Facility Code 8:

CCTV & Video Integration Mode

Video Server Type:

Biometric Device

Biometric Model:

User Login

Number of day to change password:

Number of time to retry login :

Each site can have up to 8 facility code.

Config. System



- Tool & Settings ^
- Controller Control
 - Controller Alarm & IO Control
 - Card Utility
 - Download Utility
 - Upload Utility
 - RFID Reader Bit Configuration
 - LCD Message Control
 - Event Configuration
 - **System Setting**



System Preference and Configuration

General Setting | Email Notification | Card User Custom Field

SMTP Mail Server

SMTP Server:

Outgoing Port:

Authentication Required: Required SSL:

Username: Password:

Email Account

Send email to below recipient(s) when alarm event detected.

Email 1:

Email 2:

Email 3:

Email 4:

Email 5:

Software

reports

Informes



Categoría :

Historico de Transacciones **Ubicación Informes**

Categoría :

Informe de Empleados **Informe de Tarjeta Temporal** **Informe de Niveles de Acceso**

Categoría :

Informe de Auditoria **Informe de Alarmas reconocidos**

Categoría :

Informe de Zonas Horaria **Informe de Config. Horario**

Categoría :

Informe de Control de Asistencia

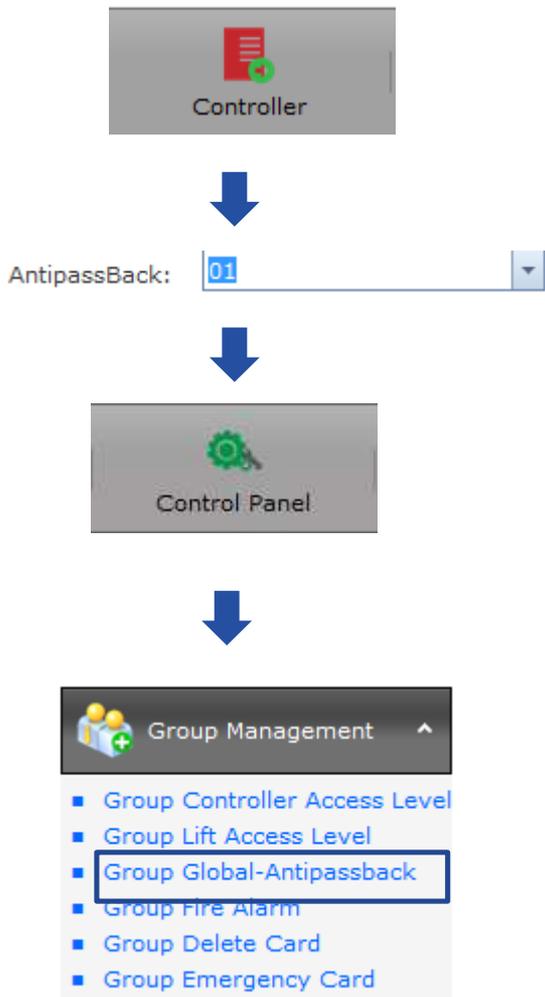
Categoría :

Informe de Entradas Manuales **Informe de Resumen de Entradas Manuales**

Software

**Additional
modules**

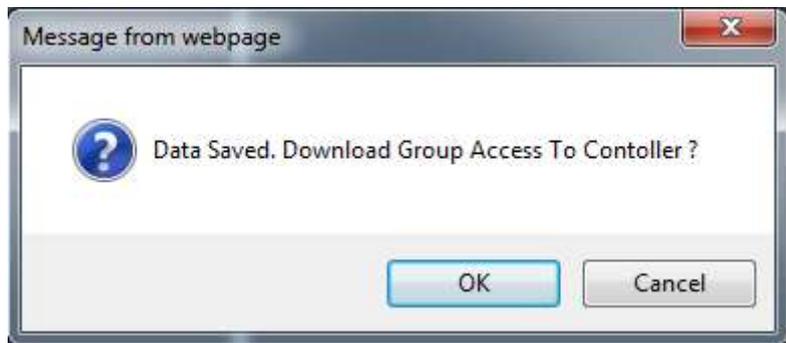
Global Antipassback



Group Access No: *

Site Code:

<input type="checkbox"/>	Controller	Description	Site Code
<input checked="" type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA
<input checked="" type="checkbox"/>	EMER-2		OFFA
<input checked="" type="checkbox"/>	MAIN DOOR	TESTING DOOR CONTROLLER	OFFA

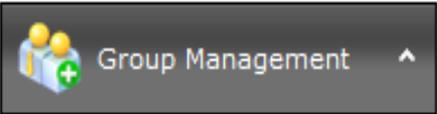


Global Antipassback Group:

Fire Alarm



Fire Alarm: Enable

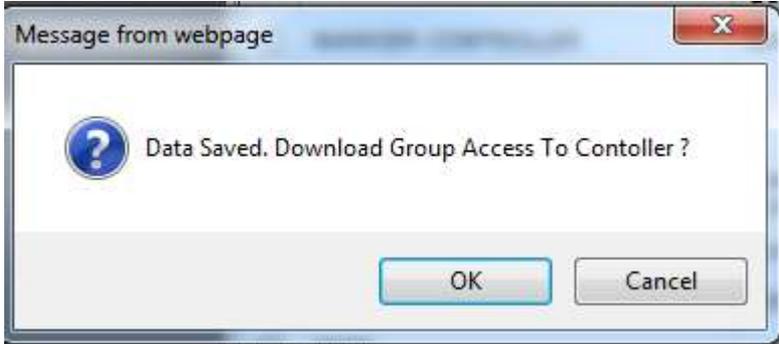


- Group Controller Access Level
- Group Lift Access Level
- Group Global-Antipassback
- **Group Fire Alarm**
- Group Delete Card
- Group Emergency Card

Group Access No:

Site Code:

<input type="checkbox"/>	Controller	Description	Site Code
<input checked="" type="checkbox"/>	189		OFFA
<input type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA
<input type="checkbox"/>	BACK DOOR CONTROLLER	BACK DOOR TESTING CONTROLLER	OFFA



Group Delete Card



Group Management

- Group Controller Access Level
- Group Lift Access Level
- Group Global-Antipassback
- Group Fire Alarm
- Group Delete Card
- Group Emergency Card



Controller List

Site Code: OFFA

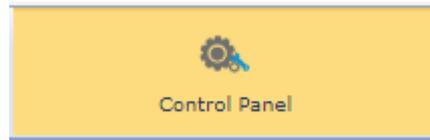
<input checked="" type="checkbox"/>	Controller	Description	Site C
<input checked="" type="checkbox"/>	189		OFFA
<input checked="" type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA
<input checked="" type="checkbox"/>	BACK DOOR CONTROLLER	BACK DOOR TESTING CONTROLLER	OFFA
<input checked="" type="checkbox"/>	BARRIER CONTROLLER	BARRIER TESTING CONTROLLER	OFFA
<input checked="" type="checkbox"/>	EMER-2		OFFA

Feature only applies to controllers enable at Auto delete group. When the visitor card to deposit in the ballot box, it will be automatically deleted from the system.

Software

Integration with Face Recognition

Integration with Face Recognition



Add new face device and fill the information like below.
The default password is:
12345678



Details Network Configuration

Device Name:*

Description:*

Site Control:* Unit No:*

IP Address: Password:

Server URL:

Device Status : Active

Time Zone

Device Time Zone:



Integration with Face Recognition



Controller Configuration

Release Time (ms) :	<input type="text" value="500"/>	Multi-Face Detection:	<input type="text" value="Recognize Multiple Faces"/>
Recognition Distance:	<input type="text" value="No limits"/>	Recognition Score:	<input type="text" value="80"/>
Recognition Interval:	<input type="text" value="0"/>	Stranger Voice Mode:	<input type="text" value="Customize"/>
Stranger Detection:	<input checked="" type="checkbox"/>	Stranger Voice Customization:	<input type="text" value="Stranger"/>
Stranger Threshold:	<input type="text" value="3"/>	Voice Customization:	<input type="text"/>
Voice Mode:	<input type="text" value="Broadcast Name"/>	Display Customization:	<input type="text"/>
Display Mode:	<input type="text" value="Display Name"/>	Wiegand Output:	<input type="text" value="WG26 User ID"/>
Liveness:	<input checked="" type="checkbox"/>		



Fill the face recognition setting like you needed

192.168.0.150 :

Details Network Configuration

Set Network Setting

LAN Network	WIFI Network
IP Address: <input type="text" value="192.168.0.150"/>	SSID: <input type="text"/>
Subnet Mask: <input type="text" value="255.255.255.0"/>	Password: <input type="text"/>
Gateway: <input type="text"/>	IP Address: <input type="text" value="192.168.0.150"/>
DNS: <input type="text" value="255.255.255.255"/>	Gateway: <input type="text"/>
DHCP: <input type="checkbox"/>	DNS: <input type="text"/>
	DHCP: <input type="checkbox"/>



Need to connect the network cable first before setting up WIFI

Integration with Face Recognition



Group Face Access Level

Create new Face Access Level

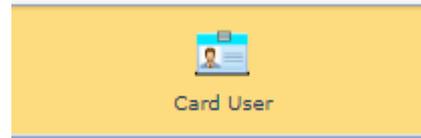
Access Level Setting

Group Access No:* 01

Description: Free Access

#	Face Device	Time Set
<input checked="" type="checkbox"/>	test face	01

Integration with Face Recognition



Card User List

New Card Batch Add Edit Delete Back

Site Code ▾

<input type="checkbox"/>	Card N° ▾	Name ▾
Site Code: BASS Philippines		
<input type="checkbox"/>	0000012121	sa
<input checked="" type="checkbox"/>	0000012345	joe
<input type="checkbox"/>	0000123432	da
<input type="checkbox"/>	0123456789	jojo
<input type="checkbox"/>	0168028730	test user 1

Edit existing user to register face

Integration with Face Recognition



Card No:* 0000012345
Name:* joe
Site Code:* BASS Philippines

Card Properties

Card Type: Normal Card
Card Pin No:* 0
Bypass Antipassback: Enable
Guard Tour Card: Enable
Face Access Level: None
Card Expiry Status: No
Bypass Holiday: Enable
Expired Date (dd-MM-yyyy): 24-03-2020
Car Park Max Spot Group: None

Biometric Authentication: FP
 Enable
 Enable

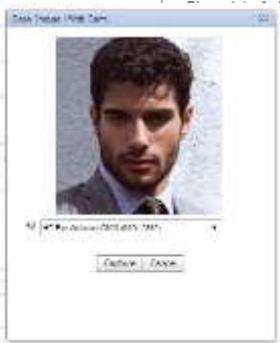
Access Level: 00 - No Access Rack Zone
Card Type: Enable
Group: Master Card
HMS: 12:29 PM
Card Type: 00

Attendance Control

System

Other

Floor No:
Plate: B1570PQB
Parking Lot No:



Scan the Face Image via webcam or upload from PC

Card Profile

Card Info Employee Details Access Level Custom Fields



Card No:* 0000012345
Name:* joe
Site Code:* BASS Philippines

Card Properties

Card Type: Normal Card
Card Pin No:* 0
Bypass Antipassback: Enable
Guard Tour Card: Enable
Face Access Level: None
Card Expiry Status: Non Expired
Bypass Holiday: Enable
Expired Date (dd-MM-yyyy): 24-03-2020
Car Park Max Spot Group: None

Biometric Authentication: FP
Alarm Card: Enable
Card Status: Enable
Rack Access Level: 00 - No Access Rack Zone
Emergency Card Type: Enable
Dual Card Group: Master Card
Expiry Time (HMS): 12:29 PM
Canteen TZ: 00

Attendance Control

System

Other

Floor No:
Plate: B1570PQB
Unit No:
Parking Lot No:

Save and the information will simultaneously download to controller and Face reader

Software

Integration with License Plate Recognition

Integration with License Plate Recognition



Car Plate Binding

Access Controller:*

Description:*

Camera Brand: Direction:

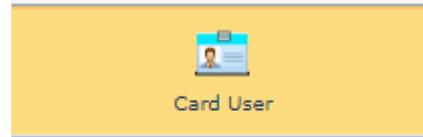
Site Control:*

Camera Network Setting

IP Address:* Port No:*

Login ID:* Password:*

Integration with License Plate Recognition



Card User List

New Card Batch Add Edit Delete Back

Site Code ▾

<input type="checkbox"/>	Card N ^o . ▾	Name ▾
Site Code: BASS Philippines		
<input type="checkbox"/>	0000012121	sa
<input checked="" type="checkbox"/>	0000012345	joe
<input type="checkbox"/>	0000123432	da
<input type="checkbox"/>	0123456789	jojo
<input type="checkbox"/>	0168028730	test user 1

Edit existing user to register License
Plate Number

Integration with License Plate Recognition



Card Profile

Card Info Employee Details Access Level Custom Fields



Card No:*

Name:*

Site Code:*

Card Properties

Card Type:	<input type="text" value="Normal Card"/>	Biometric Authentication:	<input type="text" value="FP"/>
Card Pin No:*	<input type="text" value="0"/>	Alarm Card:	<input type="checkbox"/> Enable
Bypass Antipassback:	<input type="checkbox"/> Enable	Card Status:	<input checked="" type="checkbox"/> Enable
Guard Tour Card:	<input type="checkbox"/> Enable	Rack Access Level:	<input type="text" value="00 - No Access Rack Zone"/>
Face Access Level:	<input type="text" value="None"/>	Emergency Card Type:	<input type="checkbox"/> Enable
Card Expiry Status:	<input checked="" type="checkbox"/> Non Expired	Dual Card Group:	<input type="text" value="Master Card"/>
Bypass Holiday:	<input type="checkbox"/> Enable	Expiry Time (HMS):	<input type="text" value="12:29 PM"/>
Expired Date (dd-MM-yyyy):	<input type="text" value="24-03-2020"/>	Canteen TZ:	<input type="text" value="00"/>
Car Park Max Spot Group:	<input type="text" value="None"/>		

Attendance Control

System

Other

Floor No:	<input type="text"/>	Unit No:	<input type="text"/>
Plate:	<input type="text" value="B1570PQB"/>	Parking Lot No:	<input type="text"/>

Save and download to controller

Software

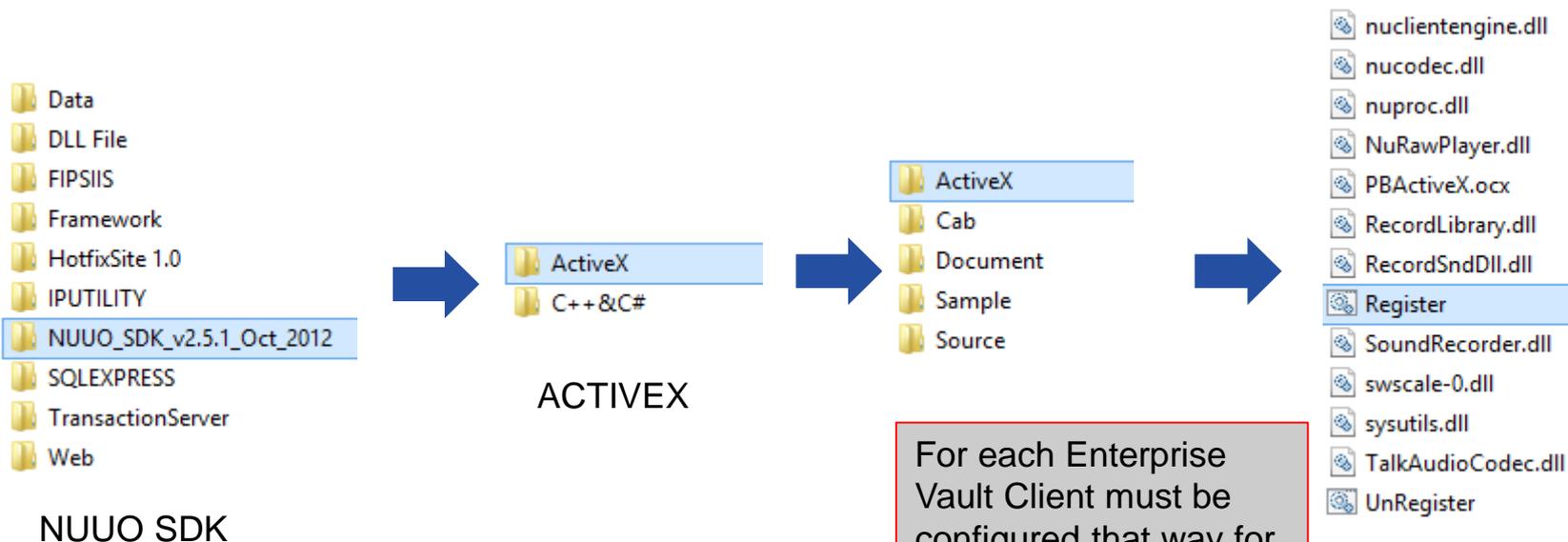
**Integration
with CCTV
NUUO**

Integration with camera



CCTV integration module is not available in the free versions of Enterprise Vault. For integration, check if your license is already activated and follow these steps:

Copy the folder SDK NUUO found within the Enterprise Vault installer to the root C: \

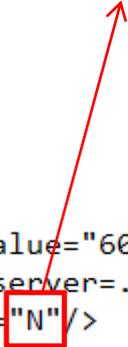


For each Enterprise Vault Client must be configured that way for integration with CCTV.

run the **REGISTER.BAT**

Make sure the Web.config file is configured correctly.

```
<appSettings>  
  <add key="ReportMaxDays" value="60"/>  
  <add key="connStr" value="server=.\SQLEXPRESS;uid=sa;pwd=passwd1234;database=DataDBEnt"/>  
  <add key="CamServer" value="N"/>
```

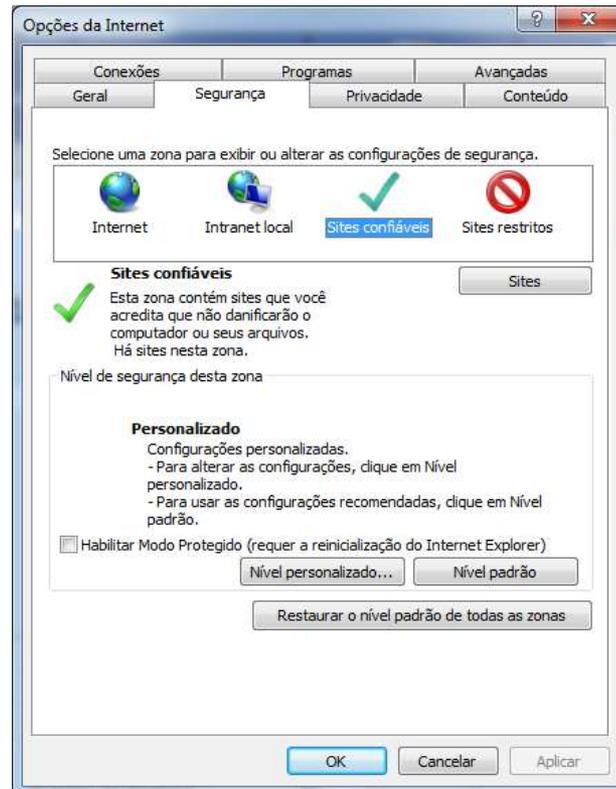


Integration with camera

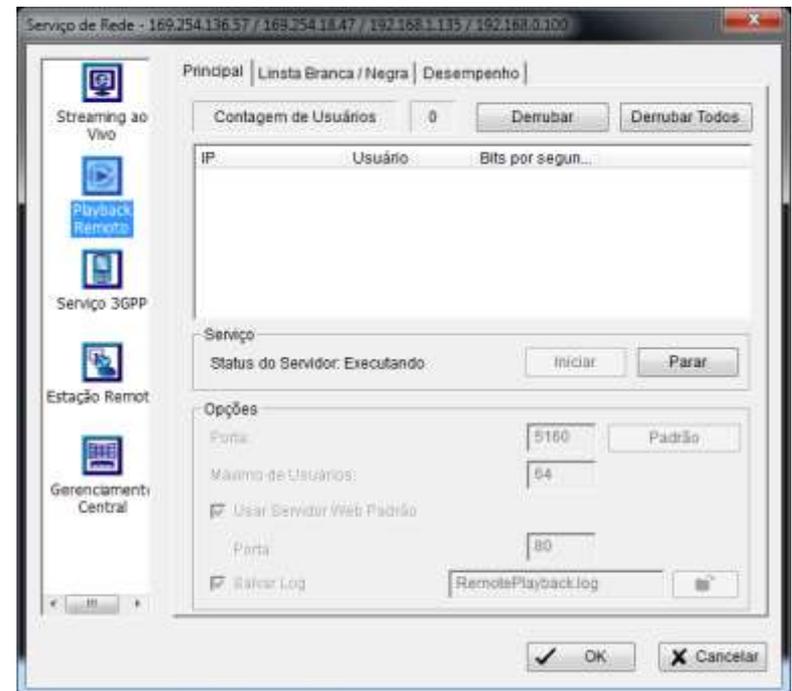
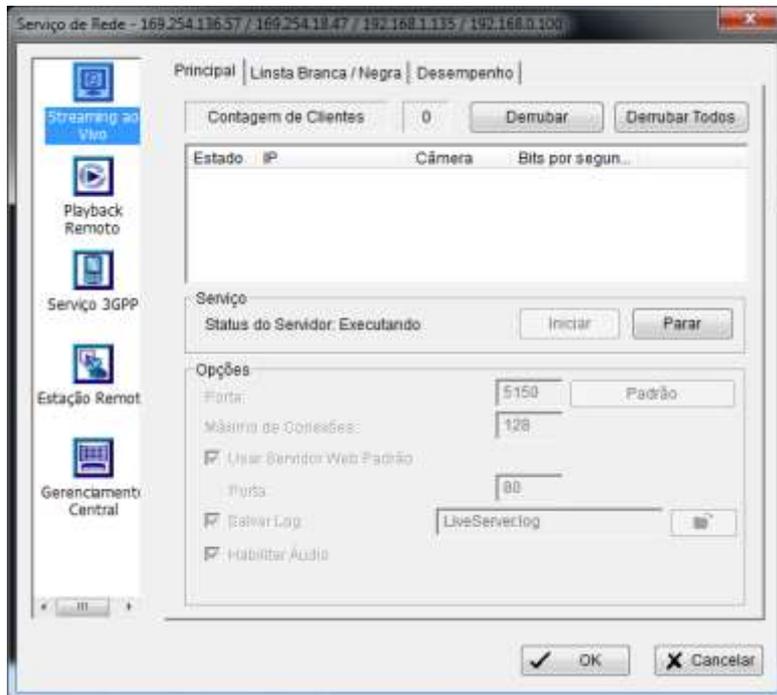


Integrating video only works in Internet Explorer, so we must enable all ActiveX, disable popups (pop-up) and include enterprise Vault in the list of trusted sites.

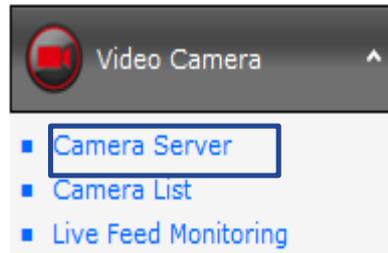
To set up that way, open the Tools tab of Internet Explorer and click Internet Options.



In the MAIN CONSOLE software, check if the network services and have begun recording:



Integration with camera



Video Server

Detail

Cam Server Name: NUUO SERVER

IP Address: 192.168.0.145

Site Code: OFFA

Live View Port: 5150

Playback Port: 5160

Authentication

Login ID: admin

Password: [REDACTED]

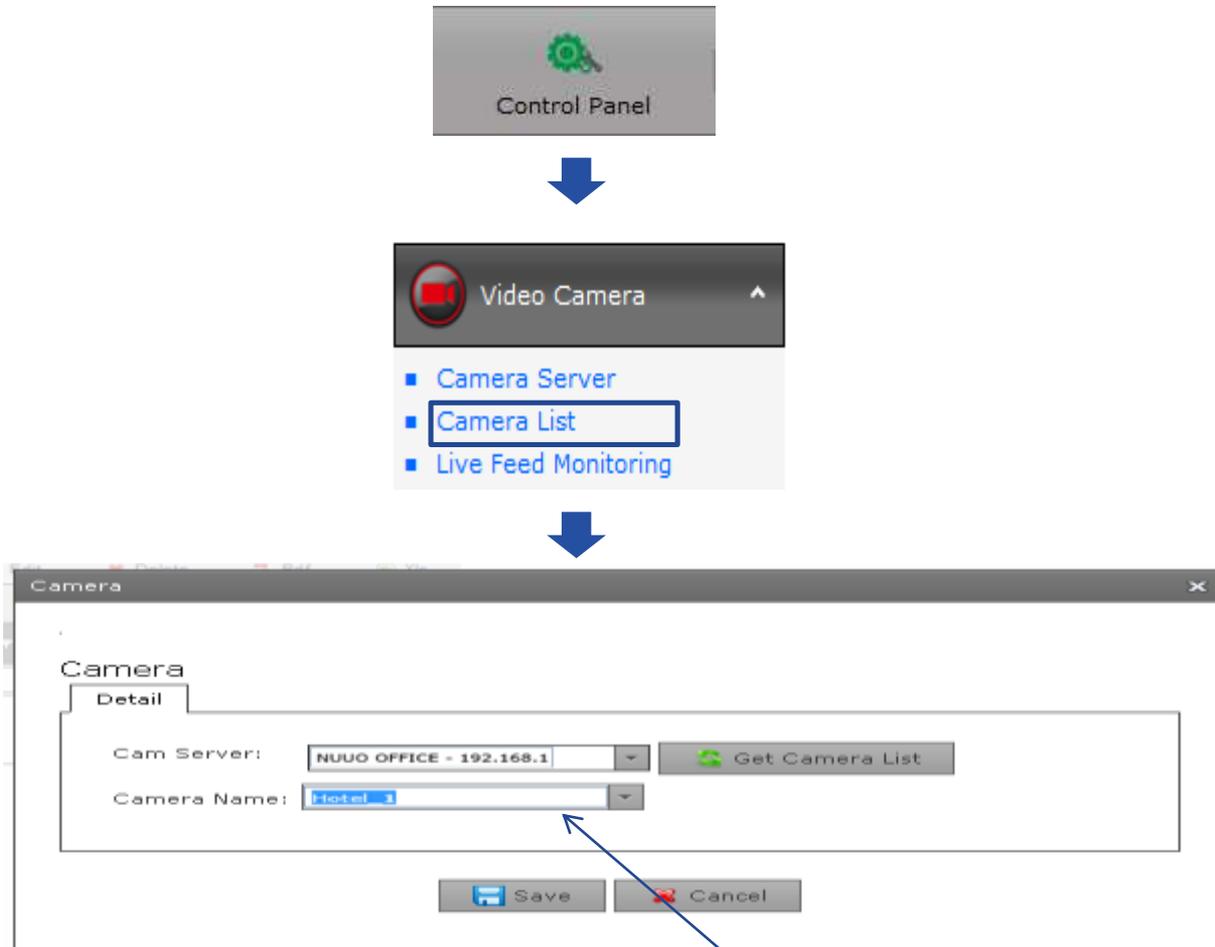
Standard Port



Integration with camera



Important: Camera names can not be changed!



Cameras video server

Important: We can have up to 3 cameras Associated input and for output.

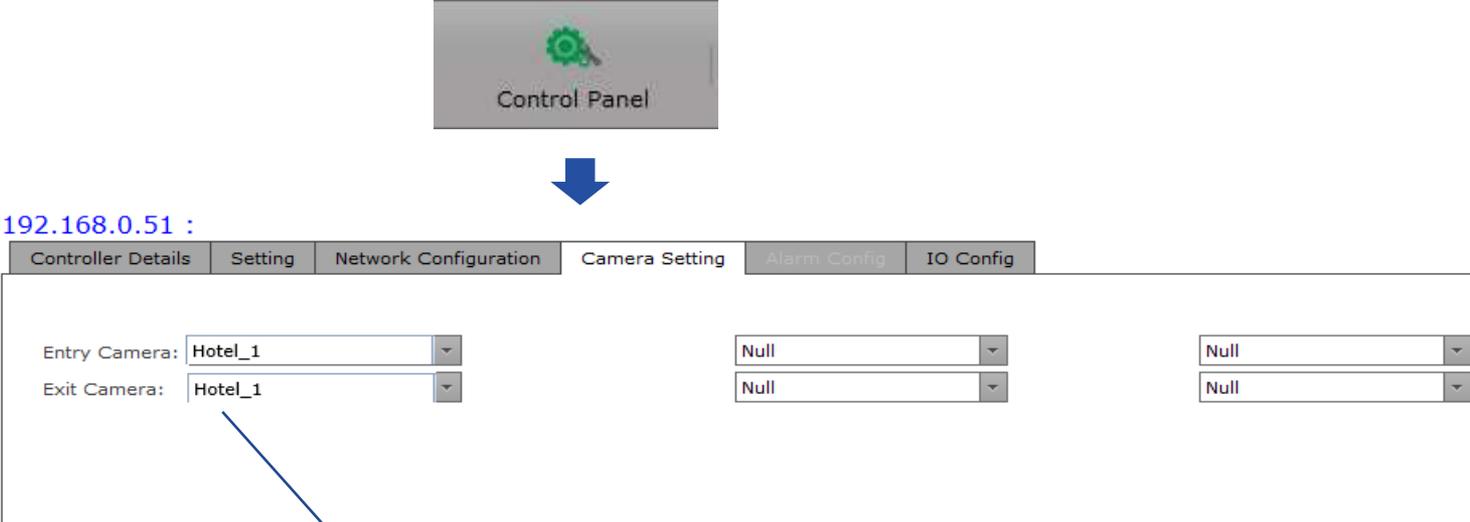
Control Panel

192.168.0.51 :

Controller Details Setting Network Configuration Camera Setting Alarm Config IO Config

Entry Camera: Hotel_1 Null Null

Exit Camera: Hotel_1 Null Null



Video cameras server for input and output.

Integration with camera



To check the operation, click on the online transaction access in / out of the door and set the Video option select Live or Recorded Video.

Visualización de Transacciones

Registro Rápido Limpiair AntipassBack Reconocer Alarma Video en Vivo Video Grabado Comparación de Video

2014/08/24 20:19:06
Puerta 01

Transacciones: **Wrong Time Zone**

Nombre: Fernando
No. Tarjeta 0007300798
Sitio : SP Visualizar el Plan de Piso

Staff No : NRIC :
Department : Engenharia Mobile No :
Joining Date :24-ago.-2014 Age : 25



ONLINE



PLAYBACK

Also Integrated transaction history!

NOTE: For best playback performance camera must be set to always record.

Software

**Integration
with ISS**

Doubts

Questions?

Thank you

Thank you!

Setting Work Time For Attendance



General Working Hour Lunch & Breaktime

Work Time Name: * Normal

Description: Normal

Site Code: MORUMBI

Grace Period

Time In: 15 Time Out: 15

Minimum Lapse Hour: 0

Over Time Setting

Auto None

Minimum Overtime: 0

At **General tab**, you can find the normal setting like **Work Time Name** and **Description**.

Grace Period, here is the option where you could allow discretion period in late-IN or early-OUT. When an employee who supposed to check in at **8:30am** checks in at **8:45am**, or checks out **at 5:15pm** when the time of check out is **5:30pm**, the short in time is not considered as lateness in the overall report, if you put its **Grace period at 15 minutes**. If the grace period is 15 minute, the check in time at 8:46am will be considered as 1 minute late. preview in the report.

Time In will set the lateness time and **Time Out** will set the early out time.

Minimum Overtime (in min) will determine when it is consider as overtime limit.

**** Make sure Server 24/7 turn on for attendance time accuracy**

Setting Work Time For Attendance



Work Time

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Time In	08:30	08:30	08:30	08:30	08:30	00:00	00:00
Time Out	17:30	17:30	17:30	17:30	17:30	00:00	00:00
Work Day	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
Next Day	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
OT Type	01 ▾	01 ▾	01 ▾	01 ▾	01 ▾	01 ▾	01 ▾

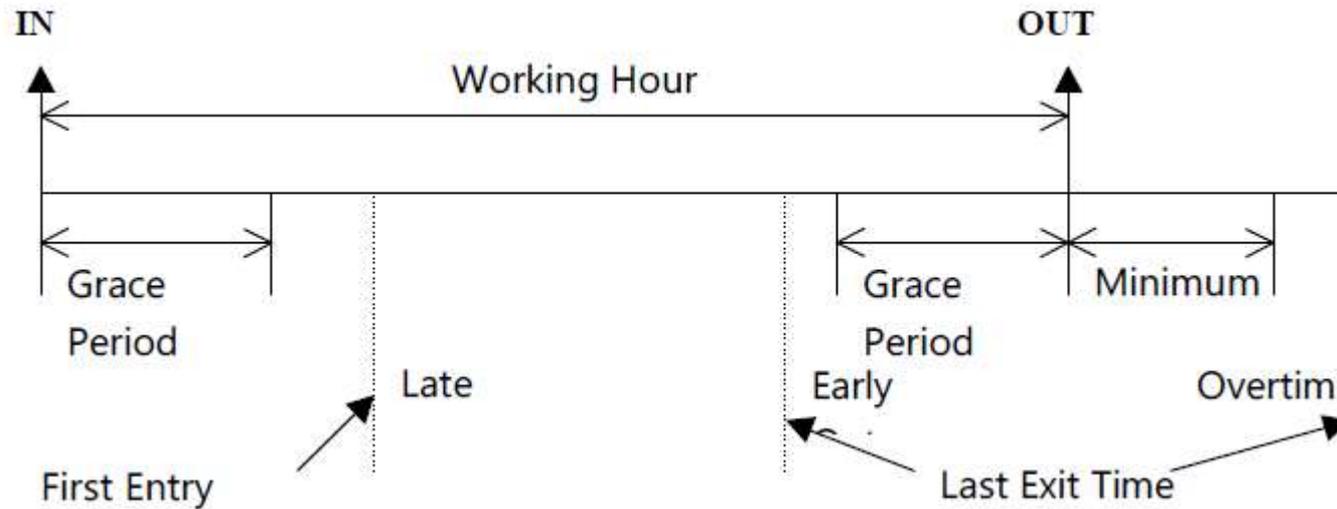
Under **Working Hour tab**, you will see the Time In ,Time Out, Work Day, Next Day, OT Type this is the area where you can configure the working time in the weekly basis.

Field	Description
Time In	Time start to work.
Time Out	Time end to work.
Work Day	Check it for working days or uncheck it for non working days.
Next Day	Use this option for those working time start at late / night shift / over night where the attendance the part involve for the second day calculation. Eg : Work from 10:00pm – 06:00am
OT Type	By default , system predefined with OT Type = 1, OT Type can be category from 1 – 4. Company who intend to use or category out the OT type for different user type can make use of this OT Type to differentiate out . It will appear as OT 1, OT 2 ,OT3 or OT4 when using generate the OT report.

Setting Work Time For Attendance



The diagram below shows the further details in setting the Grace Period, Working Hour and Minimum Overtime.



Setting Work Time For Attendance



2) Manual Entry

Go to **Control Panel > Time Attendance > Manual Entry**

Here is where the **operator / system admin** can register or add in the transaction manually in case the system need extra manual transaction or staff forget to swipe the card for attendance purpose. Under **Manual Entry Form**, select **New** to add in the new record. Record added (Valid Entry / Valid Exit) will be take place in calculation under attendance report.

Manual Entry Form

Detail

Site Code:	MORUMBI	Date:	17-03-2015	Date To:	17-03-2015
Time:	00:00:00	Time To:	23:59:59	Card No:	...
Staff Name :					
NRIC:					
Department:					
Transaction:	Valid Entry Access				
Reason:	Normal Transaction				
Remark:	Forget to swipe card.				

Save

Cancel

Setting Work Time For Attendance



3) Attendance Reason

Go to **Control Panel > Time Attendance > Attendance Reason**



- Work Time
- **Attendance Reason**
- Manual Entry

The Attendance Reason will display or appear in Manual Entry Section only. Operator / System Admin can manage all the Reason profile under this section.

Eg : Forget to bring card , Oversea Training and etc.

Late Reason List

New Edit Delete Pdf Xls			
Drag a column header here to group by that column			
<input type="checkbox"/>	No	Code	Description
<input type="checkbox"/>			
<input type="checkbox"/>	1	Normal	Normal Transaction
<input type="checkbox"/>	2	MC	Medical CheckUp
<input type="checkbox"/>	3	AL	Annual Leave
<input type="checkbox"/>	4	NPL	No Pay Leave
<input type="checkbox"/>	5	NPH	No Pay Hour

Setting Work Time For Attendance



4) Attendance Report

To view the attendance report , go to Report > Time Attendance Report



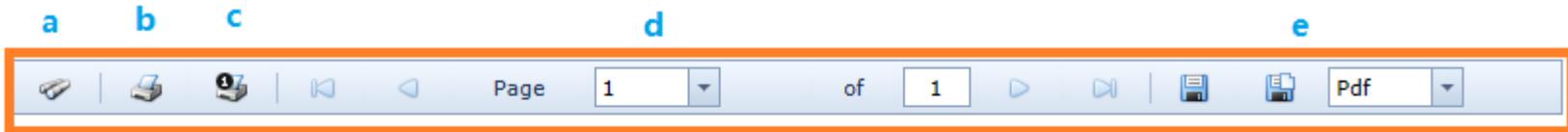
Select the report you want to view and input the criteria for report you want to filter. See screen capture below for the report type available.

The screenshot shows the 'Attendance Report' configuration form. The form has a title 'Attendance Report' and a 'Report' section. The 'Report Type' is set to 'Daily Report'. The 'Report Name' is set to 'Daily Complete'. The 'Report By' dropdown menu is open, showing options: 'Daily Complete', 'Daily Incomplete', 'Daily Lateness', 'Daily Early Out', 'Daily Absentee', 'Daily Overtime', and 'Daily In Out Summary'. The 'Filter' section includes 'Date From' (7-03-2015), 'Site Code', 'Card No.' (All Card), 'Door Controller' (All Door), 'Company Name' (All), and 'Department' (All). There are 'Select' and 'Reset' buttons for 'Card No.' and 'Door Controller'. At the bottom, there are 'View' and 'Back' buttons.

Setting Work Time For Attendance



Report Window Tool Bar



Tuesday, March 17, 2015

Daily Complete Report

Site Code : MORUMBI
Date : 17/03/2015 **To** 17/03/2015 **Company :** All
Card : All Card **Department :** All

Date	Department	Card No	Name	Staff No	Time In	Time Out

Section	Description
a	Search the content in the report
b	Print the report.
c	Print the current page
d	Page Navigation. Navigate and select the page you want to view.
e	Export the current report to the document type you want. (PDF,Excel,CSV,HTML,RTF)

Setting Work Time For Attendance



Daily Report – Report type

Report Name	Description
Daily Complete	Daily staff attendance with In and Out record. Transaction for both valid entry and valid exit.
Daily Incomplete	Daily staff attendance incomplete with In or Out record. Eg : Entry record found but without Exit record.
Daily Lateness	Daily staff attendance with lateness
Daily Early Out	Daily staff attendance where the staff left early or back before the end work time.
Daily Absentee	Daily staff report for those who are absent
Daily Overtime	Daily staff Over time report.
Daily In Out Summary	Daily staff In & Out records summary report.

Monthly Report – Report type

Report Name	Description
Attendance Checklist	
Attendance Summary	
Staff In Out Report	

PC REQUIREMENT



Application Server - Server Transaction Service and Enterprise Vault Pro

controllers	Processors' (upper)	Memory RAM	Operating System Recommended	Storage***
< 10*	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows 7 Professional (x64)	250GB
11 - 30*	Intel Core I5-3570K @ 3.40Ghz Intel Core I5-3550 @ 3.30Ghz Intel Core I7-3615QM @ 2.30Ghz	4GB	Windows Server 2008 R2 (x64)	250GB
31 - 90 **	Intel Xeon E3-1280 @ 3.50 Ghz Intel Xeon W3680 @ 3.33Ghz Intel Core I7-970 @ 3.20Ghz Intel Core I7-2700K @ 3.50Ghz Dual Xeon E5620 @ 2.40Ghz	8GB	Windows Server 2008 R2 (x64)	500GB
> 99 **	Intel Xeon E5-2670 @ 2.60 Ghz Dual Xeon E5-2670 @ 2.60Ghz Dual Xeon E5-2640 @ 2.50Ghz	16GB	Windows Server 2008 R2 (x64)	1 TB

•For sites with up to 30 controllers can use a single server for database and application.

•** For sites with more than 30 controllers must use a server to the database server and one for the application.

•*** Disk capacity must be topic under analysis case by case.