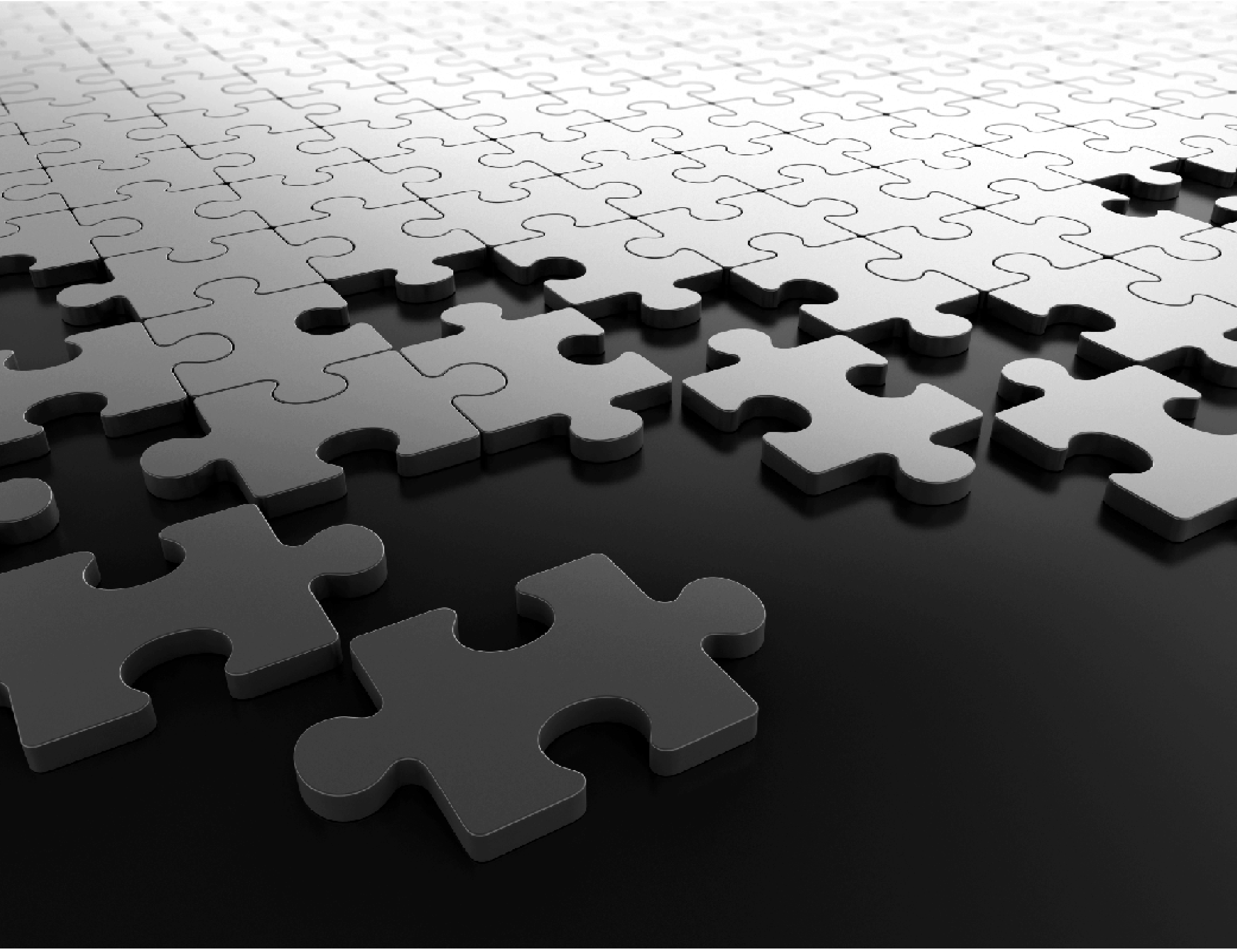
COSEC VMS

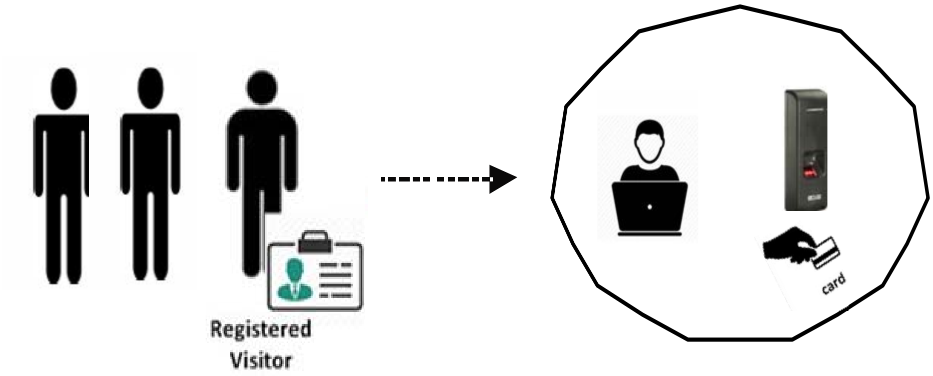
User Manual



MATRIX

SECURITY SOLUTIONS

COSEC VMS
User Manual



Documentation Disclaimer

Matrix Comsec reserves the right to make changes in the design or components of the product as engineering and manufacturing may warrant. Specifications are subject to change without notice.

This is a general documentation for all variants of the product. The product may not support all the features and facilities described in the documentation.

Information in this documentation may change from time to time. Matrix Comsec reserves the right to revise information in this publication for any reason without prior notice. Matrix Comsec makes no warranties with respect to this documentation and disclaims any implied warranties. While every precaution has been taken in the preparation of this system manual, Matrix Comsec assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Neither Matrix Comsec nor its affiliates shall be liable to the buyer of this product or third parties for damages, losses, costs or expenses incurred by the buyer or third parties as a result of: accident, misuse or abuse of this product or unauthorized modifications, repairs or alterations to this product or failure to strictly comply with Matrix Comsec operating and maintenance instructions.

Warranty

For product registration and warranty related details visit us at:
http://www.matrixaccesscontrol.com/product-registration-form.html

Copyright

Version 23
Release date: December 15, 2022

Contents

CHAPTER 1

Introduction

Welcome

Thank you for choosing the Matrix COSEC Visitor Management System (VMS). The COSEC VMS is a desktop based application which integrates with the COSEC WEB application as well as the COSEC database. It is a part of the COSEC suite of applications that helps in tracking and monitoring visitors to a premises in an efficient and comprehensive manner.

This integration with the COSEC application platform provides key advantages like accessing the existing Employee, Company and Department Information. It assists in capturing all relevant information about the visitor which is automatically stored in a database.

About this System Manual

This is common document providing detailed information and instructions for installing and using the COSEC Visitor Management System for Visitor Monitoring and Control purposes.

The COSEC VMS application connects to a database at the backend which contains all the information required by different COSEC modules.

If you are accessing the COSEC Server GUI, Device Module> Device Configuration > Click Add Button, there are three options related to Panel, namely Panel, Panel Lite and Panel200.

The term Panel refers to COSEC Panel200/Panel Lite. The feature access may differ as per the Panel variant.

Panel Lite V2 has been renamed as Panel200, hence the screens for Panel Lite V2/Panel200 represent the same.

Intended Audience

This System Manual is aimed at:

- **System Engineers**, who will install, maintain and support the COSEC System. System Engineers are persons who are responsible for configuring the COSEC system to meet the requirements of the organization/users. It is assumed that they are experienced in installing a Visitor Management System and are familiar with the operation of such systems. They are expected to be aware of how it works, and the various technical terms and functions associated with it. The SE must have undergone training in the installation and configuration of the COSEC system. No one, other than the System Engineer is permitted to make any alterations to the configuration of the COSEC system.

- **System Administrators**, who are persons who will monitor and control the COSEC system after installation. Generally, an employee of the IT/HR department in an organization or establishment is selected as the System Administrator. It is assumed that the System Administrator has some previous experience in configuring and deploying a Visitor Management system.

- **Operators**, persons/organizations who will be involved in the day to day operation of the COSEC VMS application. They may be include security personnel of small and medium businesses, large enterprises, front desk and service staff of commercial and public organizations/institutions.

Organization of this Document

This system manual contains the following topics:

- **Introduction** - gives an overview of this document, its purpose, intended audience, organization, terms and conventions used to present information and instructions.

- **Know Your COSEC VMS** - describes the system and its design, different network topologies, the interfaces, and the hardware.

- **Installing COSEC VMS application** - gives step-by-step instructions for installing the COSEC VMS application.

- **Starting the COSEC VMS application** - provides instructions for starting up the COSEC VMS application as also a description of all the functionalities.

How to Read this System Manual

This document is organized in a manner to help you get familiar with the COSEC VMS application, learn how to install it, and use its functionalities to monitor and control the visitors. The manual also covers the installation and configuration of the COSEC VMS application.

This System Manual is presented in a manner that will help you find the information you need easily and quickly.

You may use the table of contents and the Index to navigate through this document to the relevant topic or information you want to look up.

- **Instructions**

  The instructions in this document are written in a step-by-step format. Each step, its outcome and indication/notification, wherever applicable, have been described. Pictorial representations of the relevant screens have been provided wherever applicable.

- **Notices**

  The following symbols have been used for notices to draw your attention to important items.

  Important: *to indicate something that requires your special attention or to remind you of something you might need to do when you are using the system.*

Caution: *to indicate an action or condition that is likely to result in malfunction or damage to the system or your property.*

Warning: *to indicate a hazard or an action that will cause damage to the system and or cause bodily harm to the user.*

Tip: *to indicate a helpful hint giving you an alternative way to operate the system or carry out a procedure, or use a feature more efficiently.*

Technical Support

If you cannot find the answer to your question in this manual or in the Help files, we recommend you contact your system installer. Your installer is familiar with your system configuration and should be able to answer any of your questions.

Should you need additional information or technical assistance with the COSEC system and other Matrix products, contact our Technical Support Help desk, Monday to Saturday 9:00 AM to 6:00 PM (GMT +5:30) except company holidays.

Phone	(+91)18002587747
Internet	www.MatrixComSec.com
E-mail	Tech.Support@MatrixComSec.com

CHAPTER 2

Know Your COSEC VMS

The COSEC VMS is a desktop based visitor management tool that helps in tracking and monitoring visitors to the premises in an efficient and comprehensive manner. The COSEC VMS enables security conscious facilities to enhance the ways of tracking visitors. It can be installed on any computer on the network located near the lobby or the main entrance of the premises.

COSEC VMS Utility supports language translation using the Multi Language Utility. To know more, refer to the Multi Language Utility User Guide.

The COSEC VMS application is an advanced visitor management and tracking system that provides the following features:

- Determine the authorized visitors to your facility.
- Identify unwanted visitors.
- Improve lobby and security desk productivity.
- Create Visitor record with Photo and Fingerprint.
- Generate customized visitor passes.
- Maintains a watchlist or blacklist to filter unwanted visitors.
- Single screen visitor check in.
- Automatically notifies the host about a visitor’s arrival.
- Easily and quickly generates detailed reports of visitor traffic from the COSEC Web application.

CHAPTER 3

Installing COSEC VMS Software

Before commencing the installation, make sure that the computer on which the COSEC VMS software will be installed meets the necessary requirements.

System Requirements

- **Operating Systems:** Windows7 Professional and above
- **Processor:** Recommended is dual core processor and above
- **RAM:** Minimum available is 512 MB RAM
- **Hard disk:** Minimum available is 40 GB
- **Screen resolution:** Minimum Recommended is 1366 x 768
- DVD/CD-ROM drive
- **Network Interface card:** 10/100 Base-T network adapter
- Microsoft .Net Framework ver 4.0

Pre-Requisites for Face Enrollment

Computer Hardware Platform

For Windows with CPU:

- 6th and above generation Intel Core processors and Intel Xeon processors.
- Intel Xeon processor E family (formerly code named Sandy Bridge, Ivy Bridge, Haswell and Broadwell)
- 3rd generation Intel Xeon Scalable processor (formerly code named Cooper Lake)
- Intel Xeon Scalable processor (formerly Skylake and Cascade Lake).

Processor graphics are not included in all processors.

A chipset that supports processor graphics is required if you’re using an Intel Xeon processor.

For Windows with GPU:

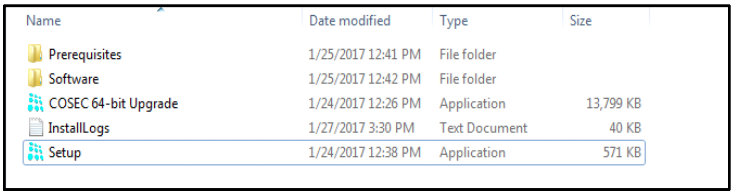
- Nvidia GeForce FTX 1050 Ti-4GB onwards

Operating System

Microsoft Windows 10 64-bit

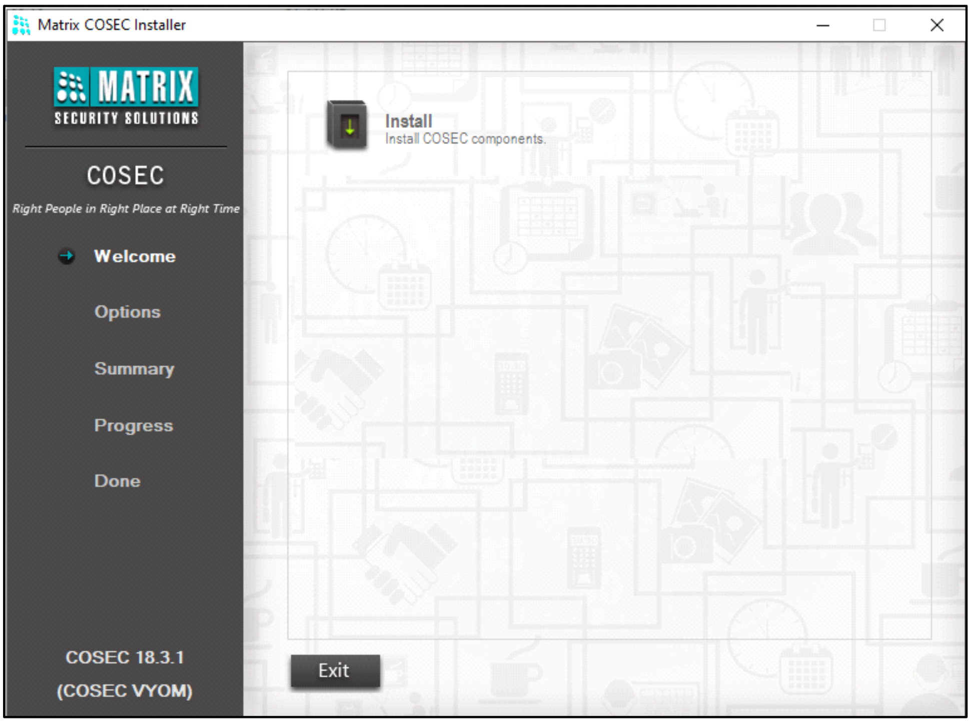
Installing COSEC VMS Utility

To install COSEC VMS Utility Application, first run the COSEC Installer setup.



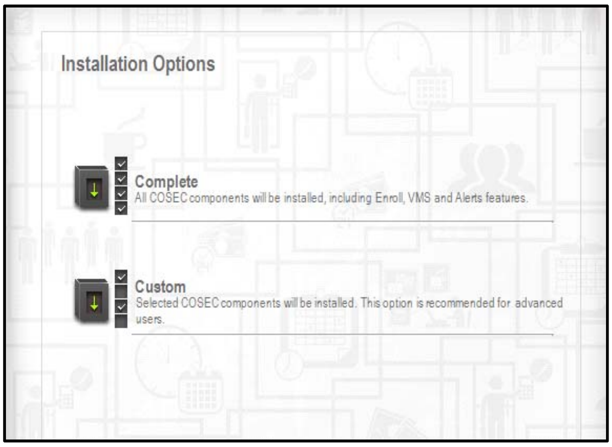
Name	Date modified	Type	Size
Prerequisites	1/25/2017 12:41 PM	File folder	
Software	1/25/2017 12:42 PM	File folder	
COSEC 64-bit Upgrade	1/24/2017 12:26 PM	Application	13,799 KB
InstallLogs	1/27/2017 3:30 PM	Text Document	40 KB
Setup	1/24/2017 12:38 PM	Application	571 KB

Click **Install**.



Install COSEC components.

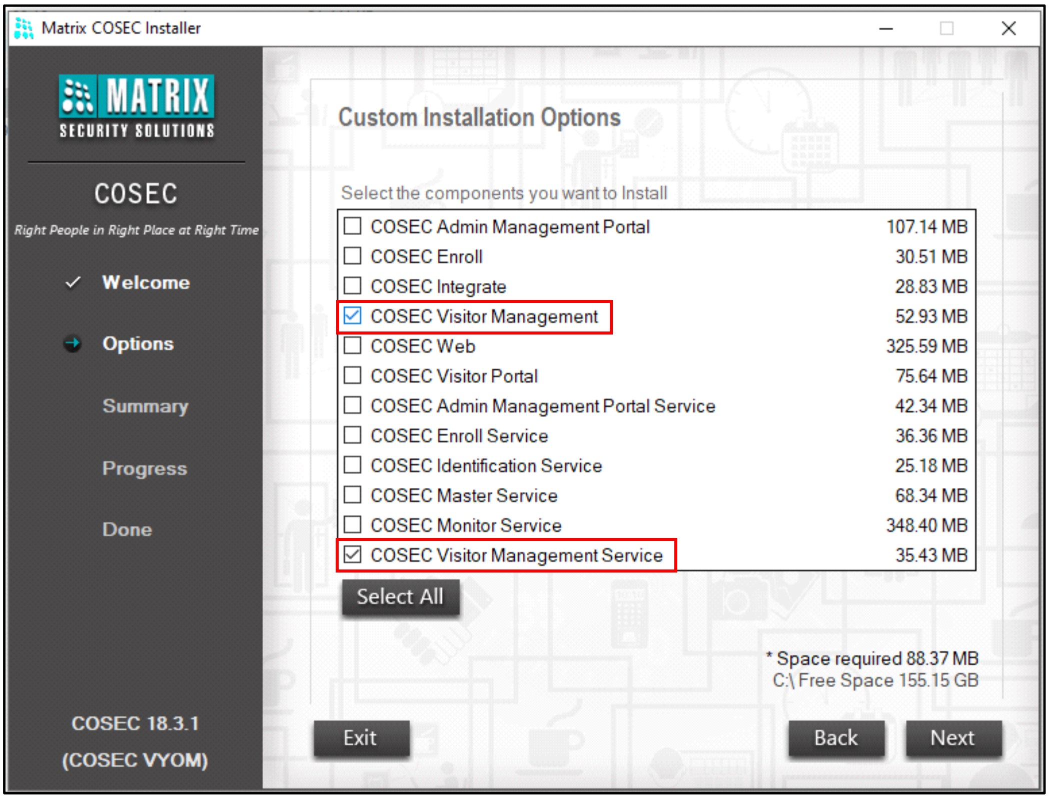
You can select **Complete** or **Custom** Installation. We will proceed further with **Custom** option.



All COSEC components will be installed, including Enroll, VMS and Alerts features.

Selected COSEC components will be installed. This option is recommended for advanced users.

Select **COSEC Visitor Management** and **COSEC Visitor Management Service** to install COSEC VMS Utility and Visitor Service respectively.



Matrix COSEC Installer

Custom Installation Options

Select the components you want to Install

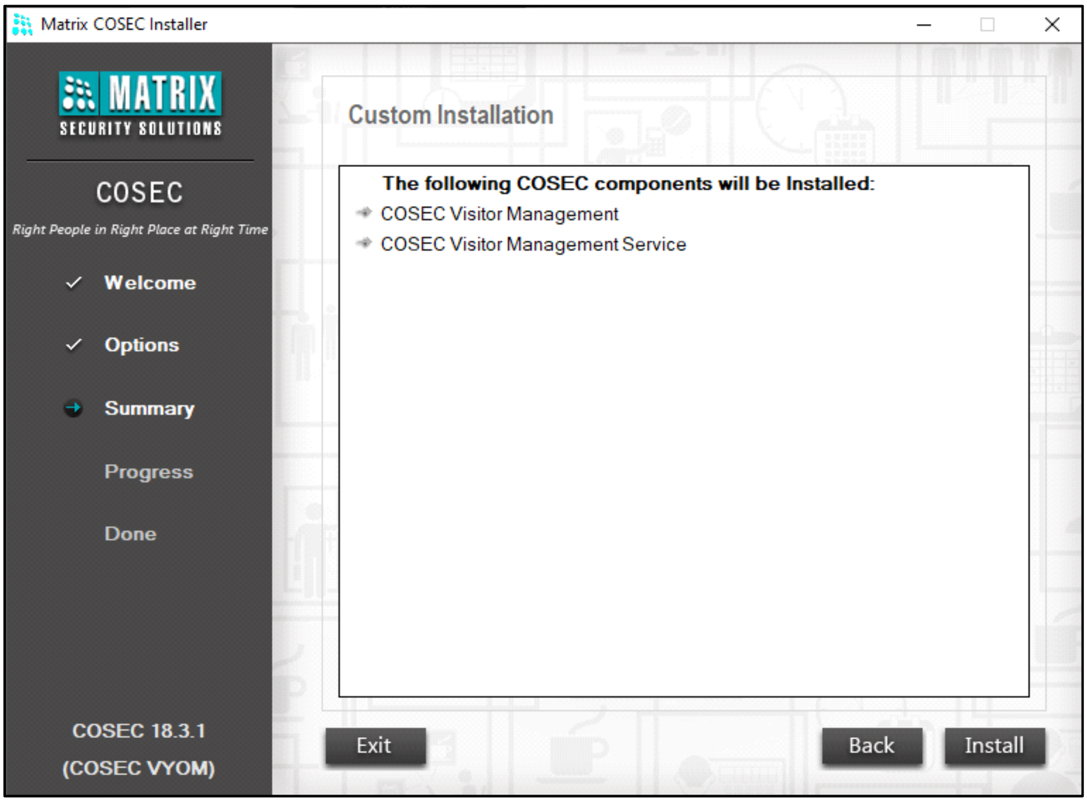
□	COSEC Admin Management Portal	107.14 MB
□	COSEC Enroll	30.51 MB
□	COSEC Integrate	28.83 MB
☑	COSEC Visitor Management	52.93 MB
□	COSEC Web	325.59 MB
□	COSEC Visitor Portal	75.64 MB
□	COSEC Admin Management Portal Service	42.34 MB
□	COSEC Enroll Service	36.36 MB
□	COSEC Identification Service	25.18 MB
□	COSEC Master Service	68.34 MB
□	COSEC Monitor Service	348.40 MB
☑	COSEC Visitor Management Service	35.43 MB

* Space required 88.37 MB
C:\ Free Space 155.15 GB

To install COSEC Visitor Management Service, the FIPS Algorithm Policy must be disabled. To know more, refer “Installing Visitor Service”.

Click **Next** to install the setup.

The confirmation window appears. Click **Install** to proceed with the installation.

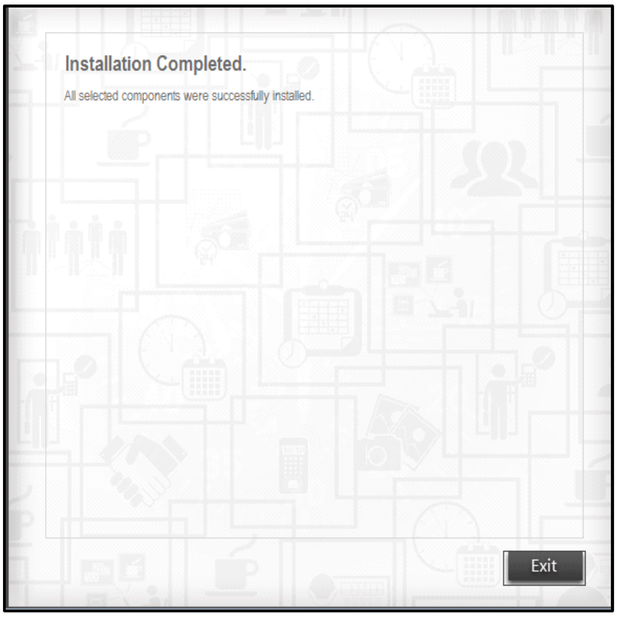


Custom Installation

The following COSEC components will be Installed:

- COSEC Visitor Management
- COSEC Visitor Management Service

After the successful installation of COSEC Visitor Management and COSEC Visitor Service, **Installation Complete** window appears as shown below.



Installation Completed.

All selected components were successfully installed.

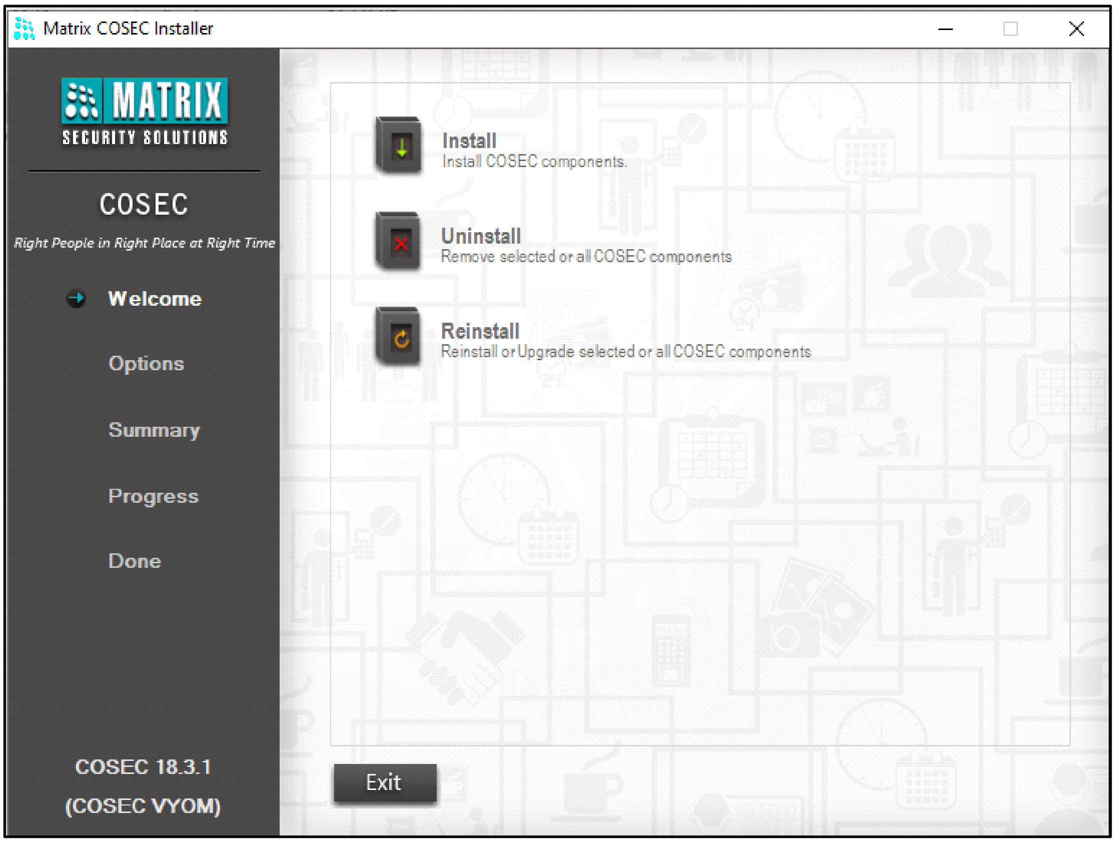
Click **Exit.**

After the successful Installation, a shortcut icon for VMS Utility COSEC VMS will be created on your desktop.

1. VMS Utility will work only if VMS Service is running.
2. VMS Service will be active and running only if Master service is running.

Uninstalling/Reinstalling COSEC VMS Utility and COSEC Visitor Service

To uninstall COSEC Visitor Management and COSEC Visitor Service, click **Uninstall.**
To reinstall COSEC Visitor Management and COSEC Visitor Service, click **Reinstall.**



Matrix COSEC Installer
MATRIX
SECURITY SOLUTIONS
COSEC
Right People in Right Place at Right Time
Welcome
Options
Summary
Progress
Done
COSEC 18.3.1
(COSEC VYOM)
Install
Install COSEC components.
Uninstall
Remove selected or all COSEC components
Reinstall
Reinstall or Upgrade selected or all COSEC components
Exit

Installing Visitor Service

To install the Visitor Management Service make sure you complete the steps mentioned in the pre-requisites and then install the same.

Visitor Service will be active and run only if Master Service is running.

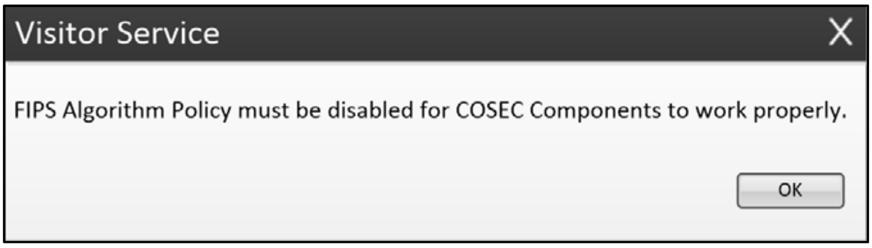
Pre-requisite for Installation

You must disable the FIPS Algorithm Flag. To do so, follow the steps mentioned below.

FIPS Algorithm Policy Check

To install COSEC Visitor Management Service, the FIPS Algorithm Flag must be disabled.

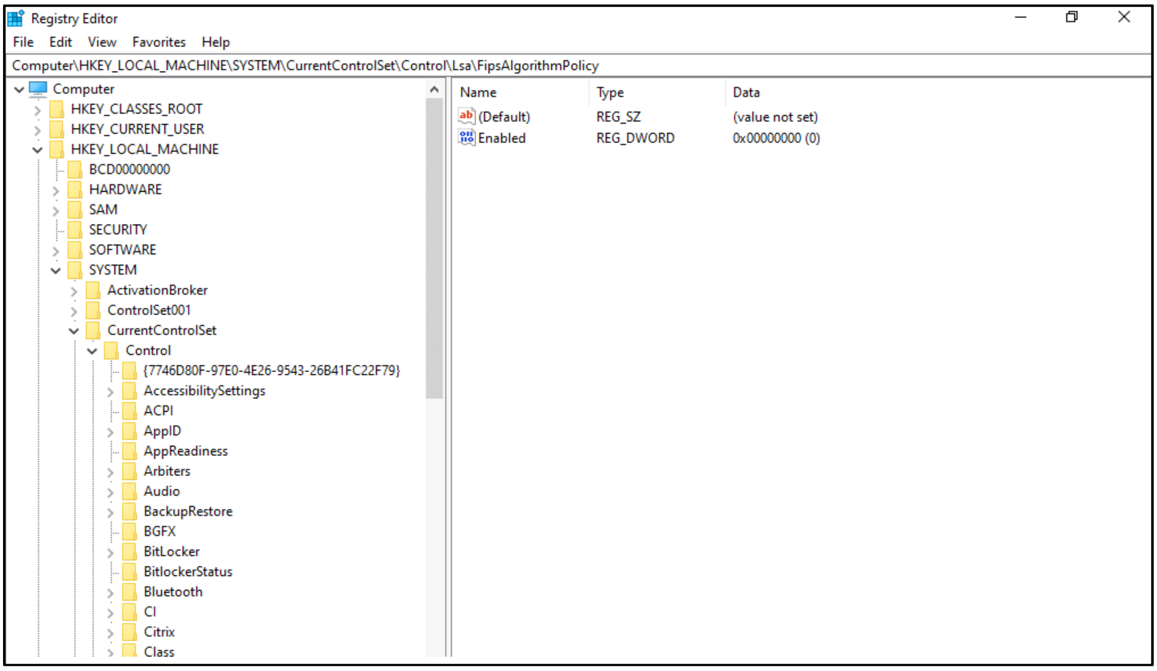
If you have started installing the Visitor Management Service and if the FIPS Algorithm flag is enabled then following pop up will appear.



Visitor Service

FIPS Algorithm Policy must be disabled for COSEC Components to work properly.

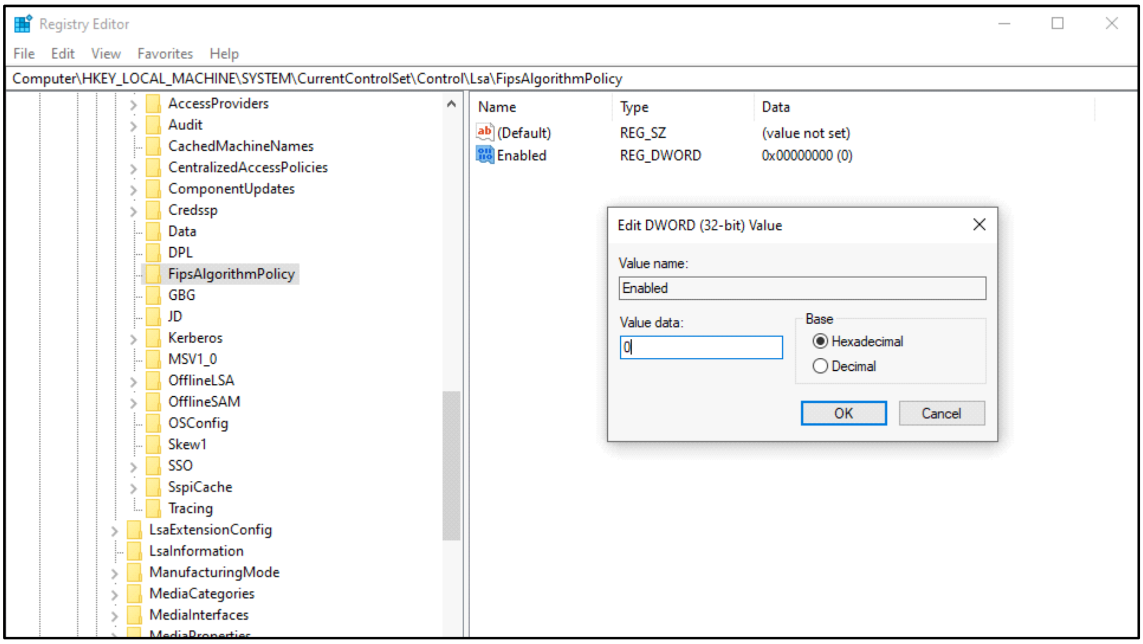
To disable FIPS Algorithm Policy, select **Registry Editor** (or search regedit) from the start menu of your computer. Then in the **Registry Editor** follow this path: ***Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy*.**



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy

Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000000 (0)

Double click on **Enabled** and the **Edit DWORD (32-bit) Value** dialog box appears as shown below:



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy

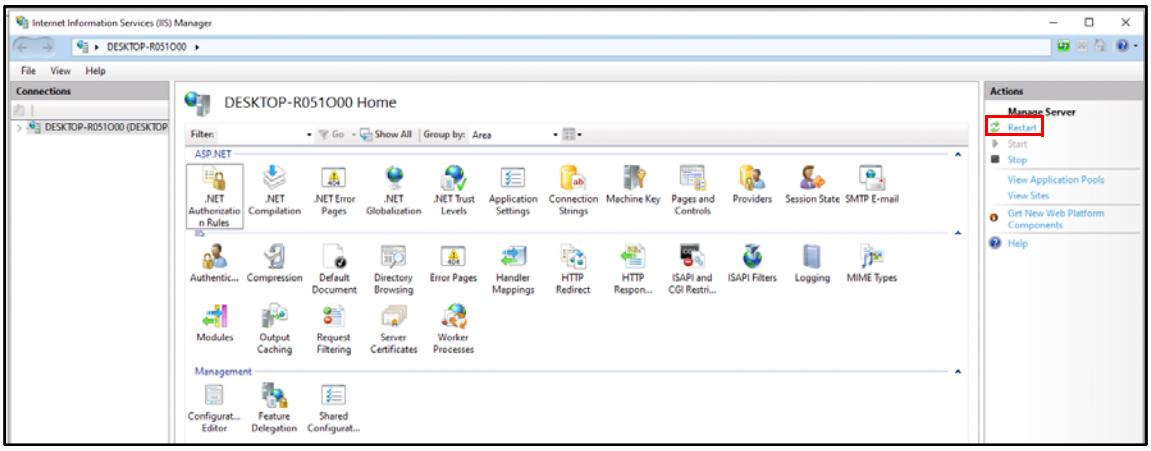
Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000000 (0)

Value name: Enabled

Value data: 0

Base: ● Hexadecimal ○ Decimal

- Enter 0 as the **Value data** to disable the FIPS Algorithm Policy.
- Now you need to reset the **Internet Information Services (IIS) Server**. To do so, search **Internet Information Services (IIS) Manager** from the start menu of your computer.



- To reset the IIS Server, click **Reset** under Actions > Manager Server.

Now you can proceed with the installation of the Visitor Service.

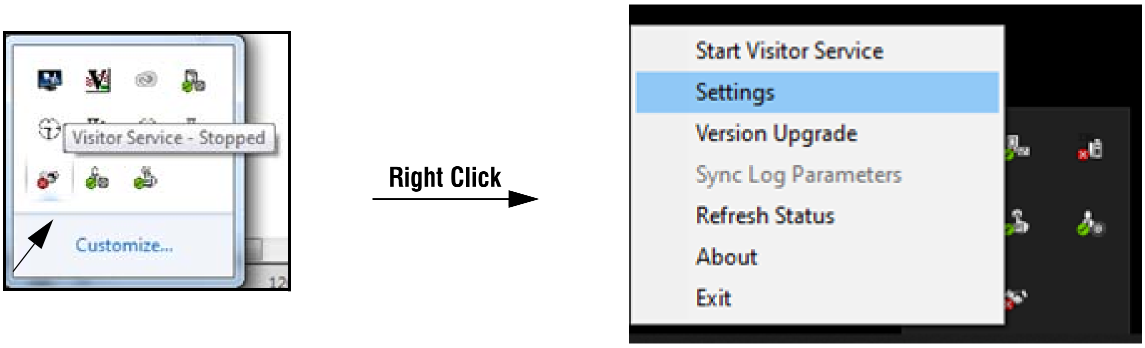
Accessing the Visitor Management Service from the Tray

To know about the installation of Visitor Management Service, refer *"Installing COSEC VMS Utility".*

After the installation, you can start the COSEC Visitor Service Application by browsing the folder from ***C:\Program Files (x86)\Matrix\COSEC Visitor Service***

When Visitor Service starts, Visitor Service's icon will be displayed in the System Tray (Notification area) on the right side of the taskbar. When Visitor Service stops, Visitor Service's icon will be displayed.

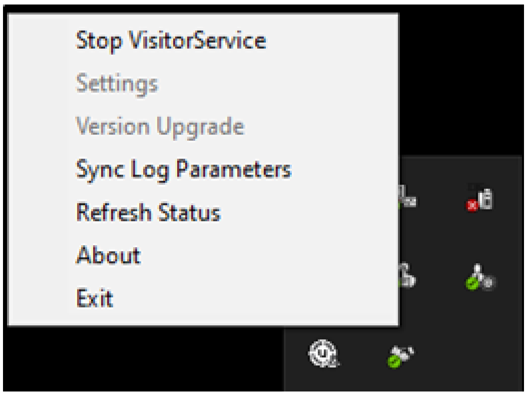
Right click on this icon.



The options displayed are — Start/Stop Visitor Service, Settings, Version Upgrade, Sync Log Parameters, Refresh Status, About and Exit.

- To start this service through the Service Manager Tray, click on **Start Visitor Service**.

- To configure the settings of Visitor Service, first stop this service by clicking **Stop Visitor Service**, and then click **Settings**. To know more, refer "Settings".



- To upgrade the version of Visitor Service, click **Version Upgrade**.
- To enable the debug logs of the Visitor Service, click **Sync Log Parameters**. This is used for trouble-shooting by the Technical Support Team.
- To refresh the status of this service, click **Refresh Status**.
- To view the service details, click **About**.
- To close the Service Manager Tray window, click **Exit**.

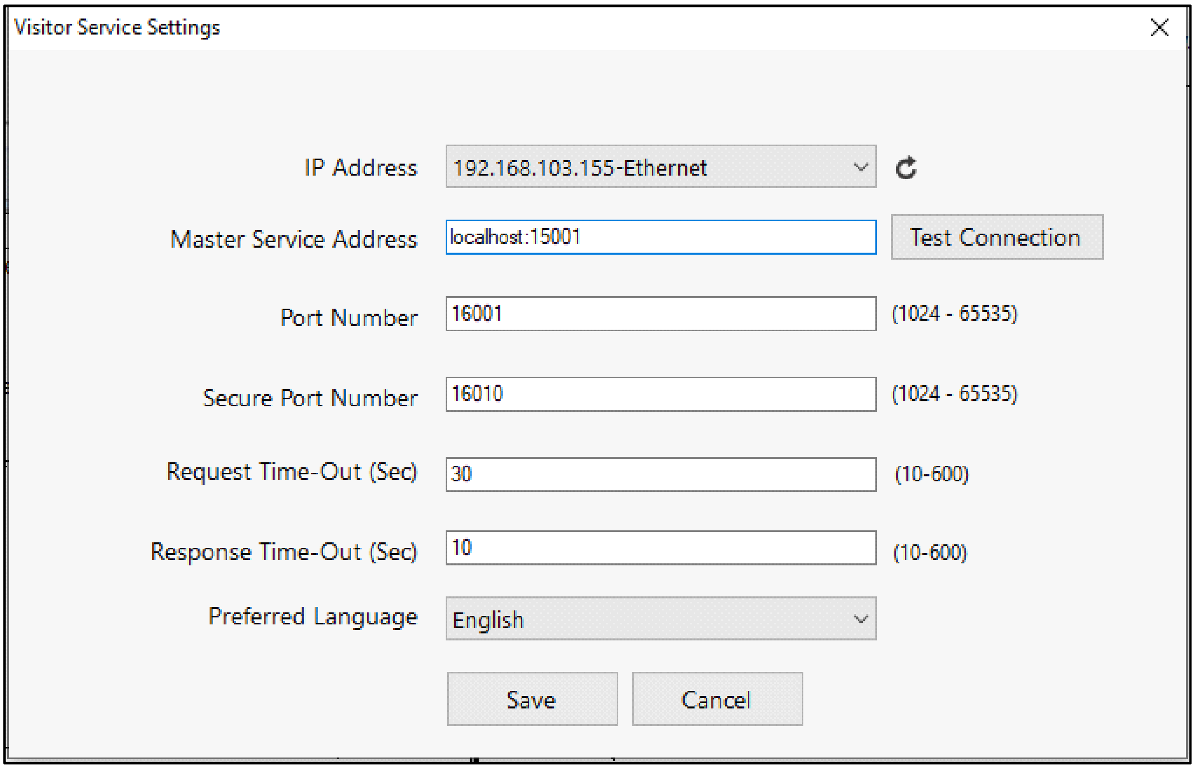
When service is running and Admin database loses connectivity or is unavailable then the service will keep running for 24 hours by default after which it will stop.

The maximum hours allowed for service is given as the configurable tag in Settings.xml file from ***C:\Program Files (x86)\Matrix\COSEC Visitor Service****.*

Settings

To configure the settings of Visitor Service, first stop this service, then click on **Settings** from the Service Manager Tray option.

Visitor Service Settings window appears as shown below.



Visitor Service Settings

IP Address: 192.168.103.155-Ethernet

Master Service Address: localhost:15001

Port Number: 16001 (1024 - 65535)

Secure Port Number: 16010 (1024 - 65535)

Request Time-Out (Sec): 30 (10-600)

Response Time-Out (Sec): 10 (10-600)

Preferred Language: English

Configure the following parameters:

- **IP Address**: If your PC is having multiple network connections, the IP Addresses of these networks will be displayed in the drop down list. Select the desired IP Address.

  The IP Address of the first enabled network will be set as the default IP Address for this service.

If none of the network connections are enabled, then IP Address of the running service will get updated to 127.0.0.1 - Localhost and the services will continue running.

To restore the IP Address to the desired one, you must first enable the connection from network connections and then select its IP Address from the drop down list manually.

As the Windows10 PC boots up fast, so services will check and retry for the availability of assigned IP address before finally moving to 127.0.0.1

If more than one network connections are enabled then the first enabled network connections IP Address will be assigned to all the services on service startup after installation.

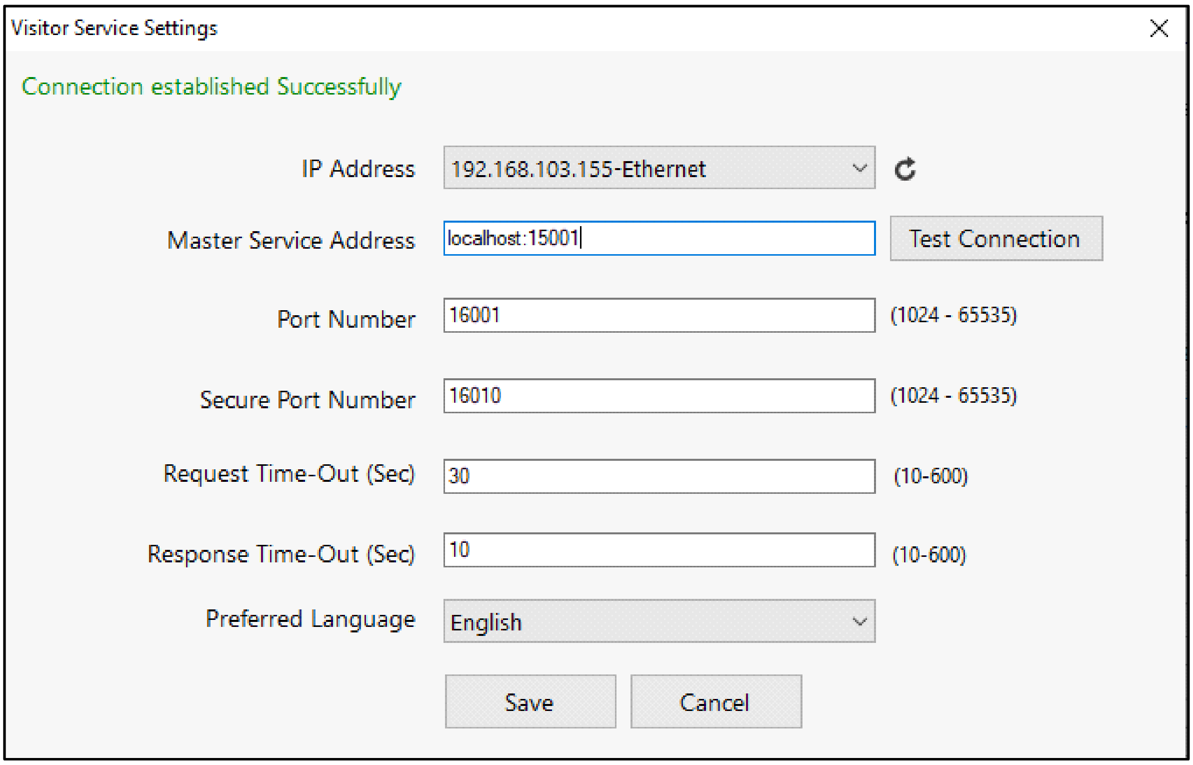
If the PC is assigned a DHCP Addressing scheme, then whenever the IP Address changes, the same will be updated against every service.

Click **Refresh IP List** ⟳ to update the list of all network adapters (network connections).

- **Master Service Address:** Enter the IP Address or URL of the Master Service.

  On changing or updating the Master Service Address, connection with the Master Service must be tested.

  Click **Test Connection** to test the connection of Visitor Service with Master service.



Visitor Service Settings

Connection established Successfully

IP Address: 192.168.103.155-Ethernet

Master Service Address: localhost:15001

Port Number: 16001 (1024 - 65535)

Secure Port Number: 16010 (1024 - 65535)

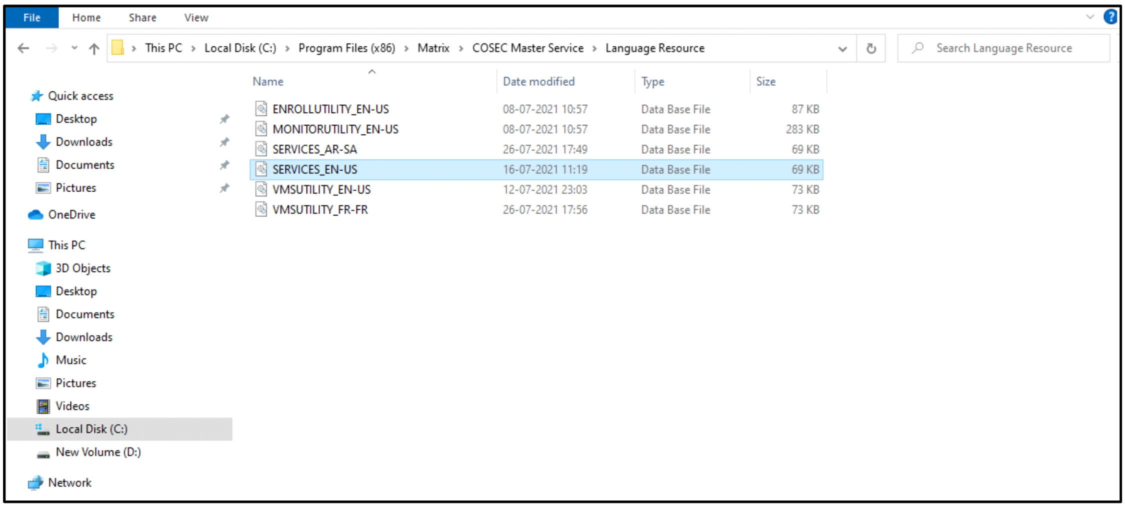
Request Time-Out (Sec): 30 (10-600)

Response Time-Out (Sec): 10 (10-600)

Preferred Language: English

- **Port Number:** This shows the port number at which the Visitor Service is accessible.
- **Secured Port Number:** This shows the port number at which the Visitor Service is accessible on SSL mode.
- **Request Time-Out (Sec)**: Enter the request time-out duration in seconds for the Visitor Service approaching Master Service for connection.
- **Response Time-Out (Sec)**: Enter the response time-out duration in seconds for the Visitor Service approaching Master Service for connection.
- **Preferred Language:** Select the desired language from the provided dropdown list.

  The languages listed here will be as per the language files present in the *C:\Program Files (x86)\Matrix\COSEC Master Service\Language Resource*.



Name	Date modified	Type	Size
ENROLLUTILITY_EN-US	08-07-2021 10:57	Data Base File	87 KB
MONITORUTILITY_EN-US	08-07-2021 10:57	Data Base File	283 KB
SERVICES_AR-SA	26-07-2021 17:49	Data Base File	69 KB
SERVICES_EN-US	16-07-2021 11:19	Data Base File	69 KB
VMSUTILITY_EN-US	12-07-2021 23:03	Data Base File	73 KB
VMSUTILITY_FR-FR	26-07-2021 17:56	Data Base File	73 KB

The default language file provided will be of English language.

Name of the English language file for services will be: SERVICES_EN-US.

Name of the language file differs as per the language. For example, name of the Arabic (Saudi Arabia) language file for services will be SERVICES_AR-SA.

If you prefer a different language other than the default language file (i.e. English), you can translate this default language into the desired language with the help of COSEC Multi-Language Utility. To know more, refer to the Multi-Language Utility User Guide.

Click **Save** to save the settings.

Service Tray in Multiple User login

When you log into your computer with different user other than Administrator who has installed COSEC; then service tray will be launched in the new user login as well but tray tool-tip messages and balloon messages will not be displayed to the new user.

This new user will have the rights to start/stop the service and make changes to the settings of service.

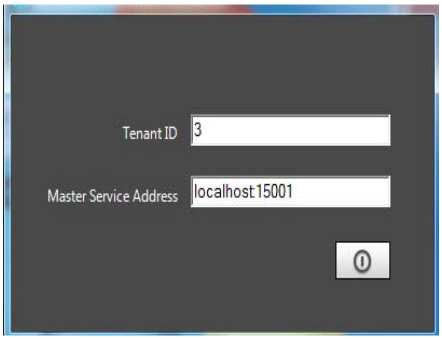
When you exit from the Visitor Service Tray Application manually then this service will not be visible in the tray for that particular windows login session. When you log in to windows session again, the service tray will be launched again.

CHAPTER 4

Starting the COSEC VMS Desktop Application

To start the COSEC VMS desktop application (VMS Utility), click on the COSEC VMS icon from your desktop.

For COSEC VYOM, Enter the Tenant ID and Master Service Address as shown below. Both the parameters are available in Tenant activation Email sent to the Tenant by the Tenant administrator.



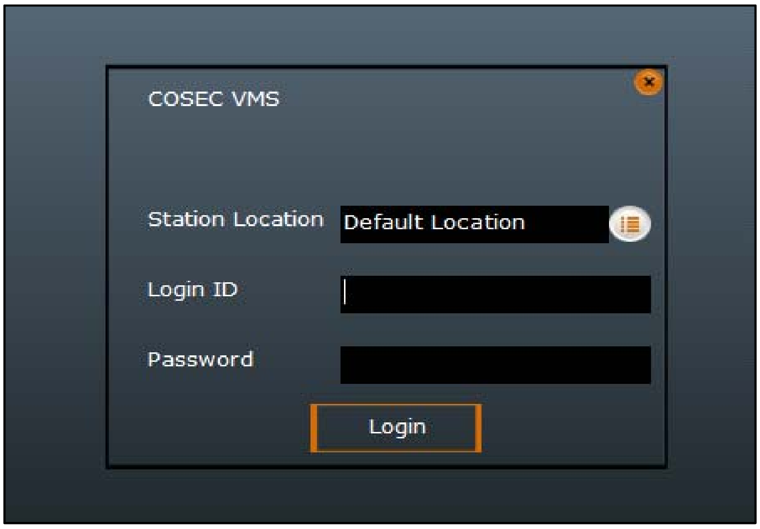
Tenant ID: 3

Master Service Address: localhost:15001

Tenant ID: Enter the tenant ID.

Master Service URL: The Master service URL is **net.tcp://192.168.104.11:15001/MasterService/**
The master service is running on PC: with IP address 192.168.104.11 at port 15001.

Click OK. The VMS login page appears as shown below.



COSEC VMS

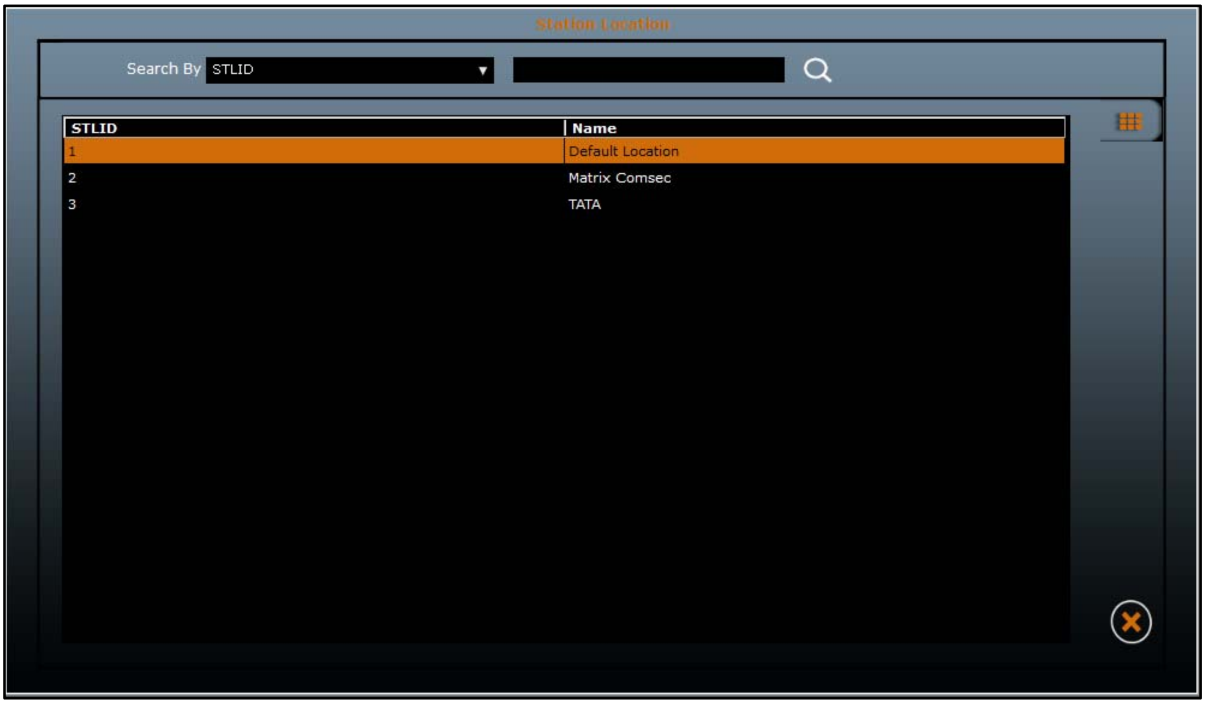
Station Location: Default Location

Login ID

Password

Before starting the COSEC VMS Utility, the Administrator needs to set the admin password from the COSEC Web application as described in the COSEC System manual.

Select the desired Station Location from the picklist.



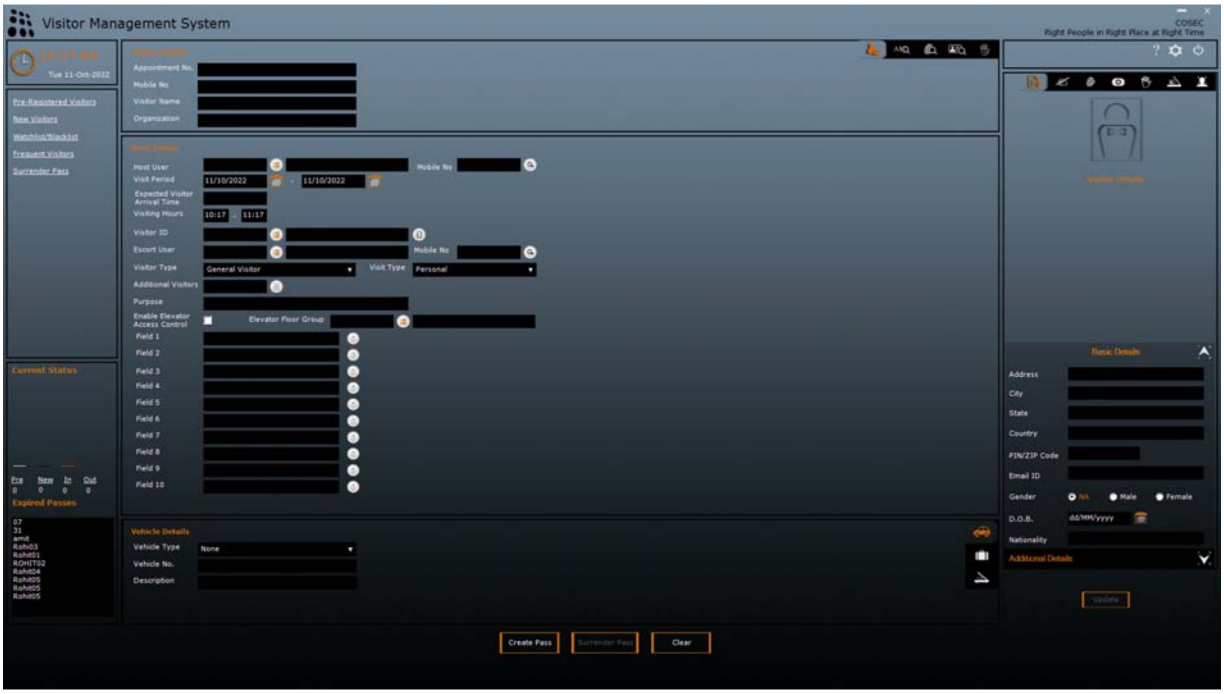
Station Location

Search By: STLID

STLID	Name
1	Default Location
2	Matrix Comsec
3	TATA

Enter the Administrator Login ID and the Password as set in the web application module.

The COSEC Visitor Management System window appears as shown.



Visitor Management System

COSEC
Right People in Right Place at Right Time

Tue 11-Oct-2022

Pre-Registered Visitors
New Visitors
Watchlist/Blacklist
Frequent Visitors
Surrender Pass

Current Status

Pre	New	In	Out
0	0	0	0

Expired Passes

07
31
amit
Rohit03
Rohit01
ROHIT02
Rohit04
Rohit05
Rohit05
Rohit05

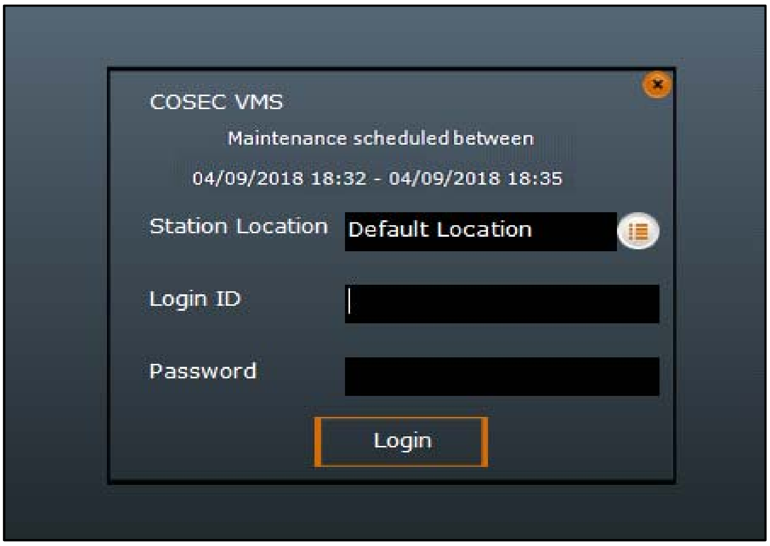
Appointment No.:
Mobile No:
Visitor Name:
Organization:

Host User: Mobile No:
Visit Period: 11/10/2022 - 11/10/2022
Expected Visitor Arrival Time:
Visiting Hours: 10:17 - 11:17
Visitor ID:
Escort User: Mobile No:
Visitor Type: General Visitor Visit Type: Personal
Additional Visitors:
Purpose:
Enable Elevator Access Control: □ Elevator Floor Group:
Field 1:
Field 2:
Field 3:
Field 4:
Field 5:
Field 6:
Field 7:
Field 8:
Field 9:
Field 10:

Vehicle Details
Vehicle Type: None
Vehicle No.:
Description:

Basic Details
Address:
City:
State:
Country:
PIN/ZIP Code:
Email ID:
Gender: ◉ NA ○ Male ○ Female
D.O.B.: dd/MM/yyyy
Nationality:
Additional Details

If the COSEC application is under maintenance; then user will not be allowed to access VMS Utility till the end of maintenance duration unless the scheduling is reset by the Admin in Admin Portal.



COSEC VMS

Maintenance scheduled between

04/09/2018 18:32 - 04/09/2018 18:35

Station Location: Default Location

Login ID:

Password:

The COSEC VMS user interface can be divided into eight parts.

1. Visitor Record options
2. Current Status
3. Expired passes

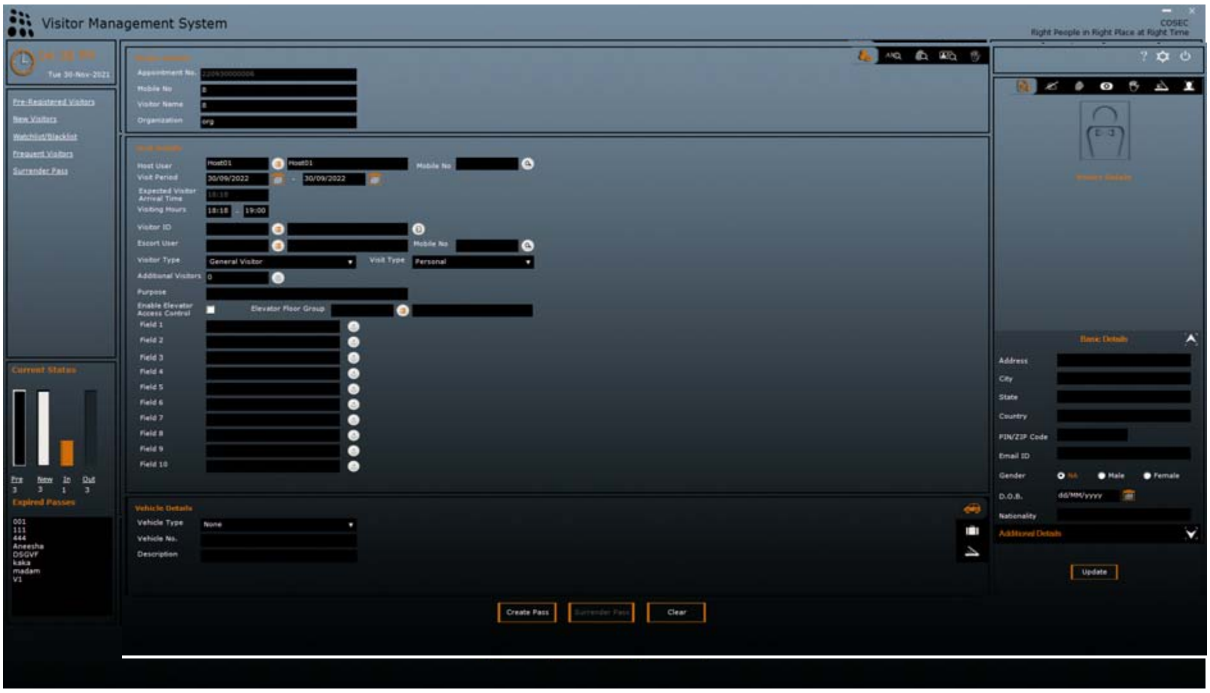
For Visitor Records, Current status and Expired Passes; refer *“Surrender Pass”*

4. COSEC VMS toolbar
5. Visitor details
6. Visit details
7. Vehicle details
8. Visitor Additional details

CHAPTER 5

Visitor Records

This section enables the user to view various visitor records like Pre-registered Visitors, Watchlisted or Blacklisted visitors, Frequent Visitors, Visitors whose passes are yet to be surrendered as well as entering the details of a new visitor.



Tue 30-Nov-2021

Mobile No: 8
Visitor Name: 8
Organization: org

Host User: Host01 Host01
Visit Period: 30/09/2022 - 30/09/2022
Visiting Hours: 18:18 - 19:00
Visitor Type: General Visitor
Visit Type: Personal
Additional Visitors: 0
Enable Elevator Access Control: □

Pre 3, New 3, In 1, Out 3

Expired Passes: 001, 111, 444, Aneesha, DSGVF, kaka, madam, V1

Vehicle Type: None

Gender: ● NA ○ Male ○ Female
D.O.B.: dd/MM/yyyy

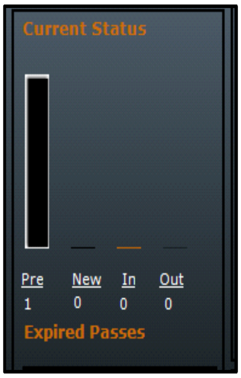
For more details see topics:

“Pre-Registered Visitors”
“New Visitors”
“Watchlist/Blacklist”
“Frequent Visitors”
“Surrender Pass”

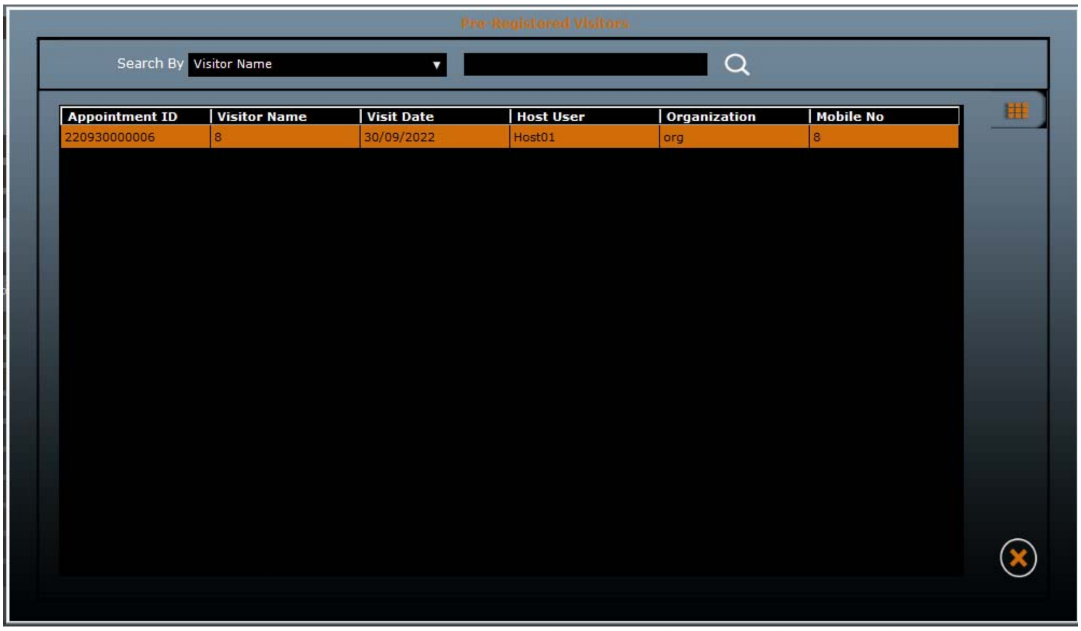
Pre-Registered Visitors

If there are any Pre-registered visitors, then Current Status of **Pre** will display the number of pre-registered visitors who are expected to come today. For the visitors who require security clearance will appear in **Pre** list only after getting security clearance.

Click on **Pre** to view the list of Pre-registered visitors.



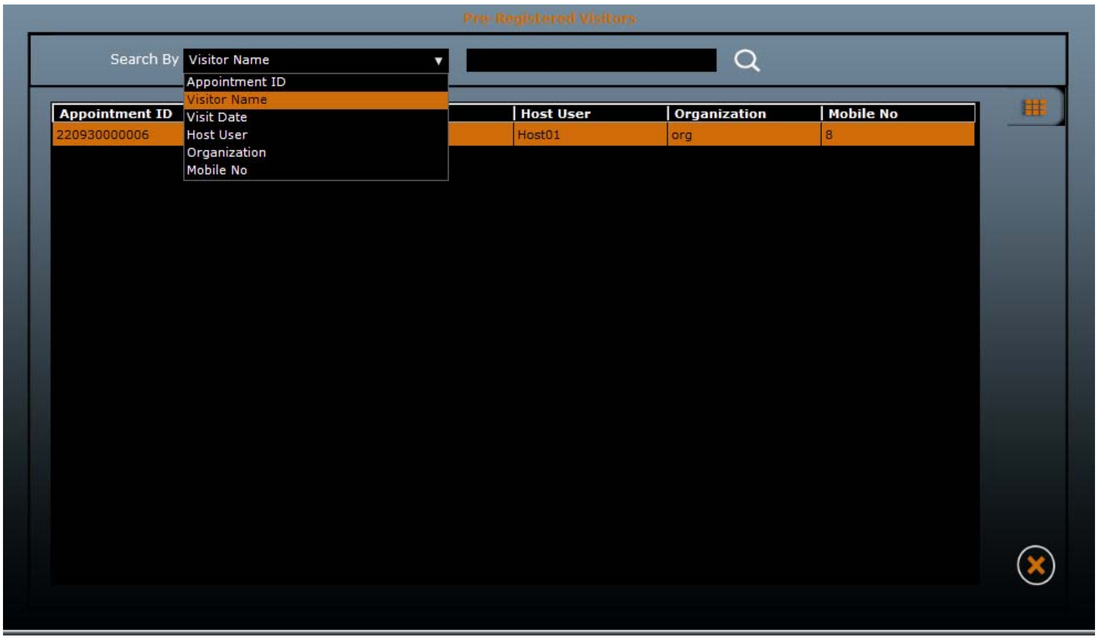
Also on clicking the Pre-Registered Visitors option, the following window appears.



Appointment ID	Visitor Name	Visit Date	Host User	Organization	Mobile No
220930000006	8	30/09/2022	Host01	org	8

The cross button appearing at the lower right corner of the windows are provided to close the window and return to the home page of the VMS application.

You can search the visitor by selecting the **Search By** option from the drop down list.



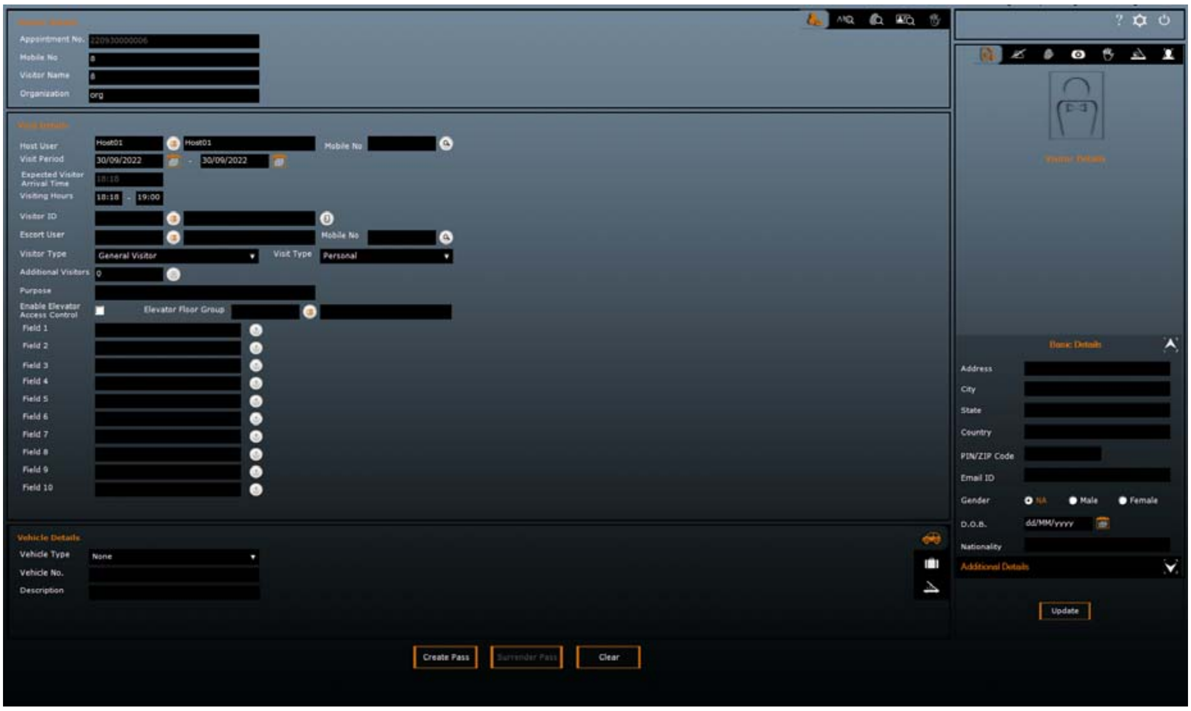
Pre-Registered Visitors

Search By: Visitor Name

Appointment ID	Host User	Organization	Mobile No
220930000006	Host01	org	8

The list of pre-registered or expected visitors will be displayed in the list.

Select the Visitor to be checked in from the list or to view the details of visitor. The details of the visitor as specified from the Visitor Management module of COSEC Web will appear here.



Appointment No. 220930000006
Mobile No 8
Visitor Name 8
Organization org

Host User Host01 Host01 Mobile No
Visit Period 30/09/2022 - 30/09/2022
Expected Visitor Arrival Time 18:18
Visiting Hours 18:18 - 19:00
Visitor ID
Escort User Mobile No
Visitor Type General Visitor Visit Type Personal
Additional Visitors 0
Purpose
Enable Elevator Access Control □ Elevator Floor Group
Field 1
Field 2
Field 3
Field 4
Field 5
Field 6
Field 7
Field 8
Field 9
Field 10

Vehicle Details
Vehicle Type None
Vehicle No.
Description

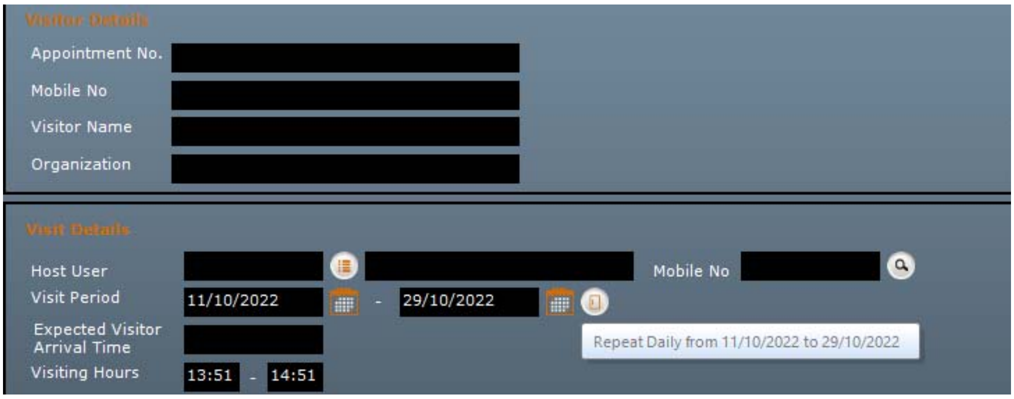
Basic Details
Address
City
State
Country
PIN/ZIP Code
Email ID
Gender ● NA ○ Male ○ Female
D.O.B. dd/MM/yyyy
Nationality

Host User: Select the desired Host User from the provided picklist.

Visit Period: The Visit Period can be selected from the Start Date and End Date calender buttons. When End Date is greater than Start date, then **Repeat** button gets enabled.

- Click **Repeat.** The Repeat Visit window appears. You can select repeat mode as — Daily, Weekly or Monthly — based on which visit will repeat.

- Eg: If Weekly mode is selected, and Days are selected as Monday and Thursday so the visit will be repeated on every Monday and Thursday in the range of Visit period.



Visitor Details

Appointment No.

Mobile No

Visitor Name

Organization

Visit Details

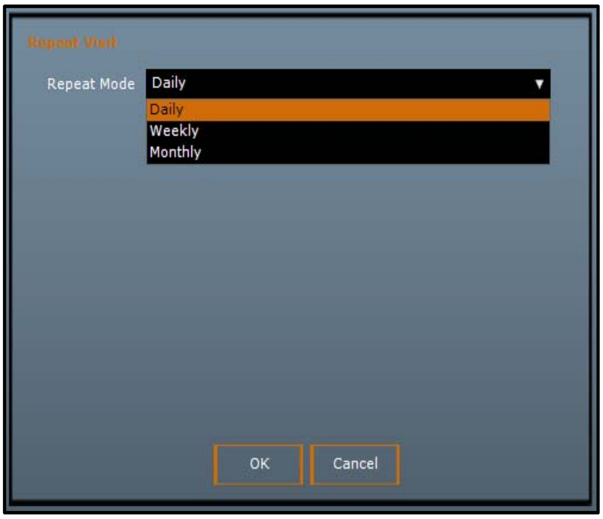
Host User

Mobile No

Visit Period 11/10/2022 - 29/10/2022

Expected Visitor Arrival Time

Visiting Hours 13:51 - 14:51

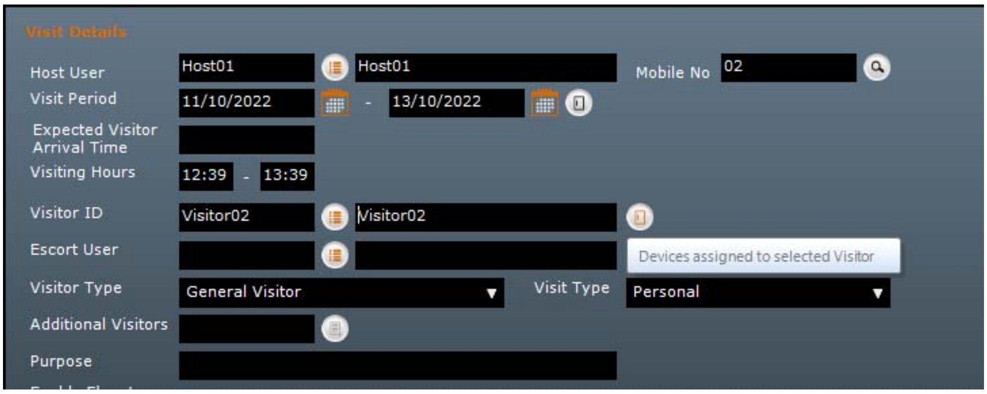


Repeat Visit

Repeat Mode: Daily

Mention **Expected Visitor Arrival Time** and **Visiting Hours.**

Visitor ID: The visitor can be assigned devices by assigning the Visitor ID and clicking the **Devices assigned to selected Visitor** button as shown below.



Visit Details

Host User: Host01 Host01

Mobile No: 02

Visit Period: 11/10/2022 - 13/10/2022

Expected Visitor Arrival Time

Visiting Hours: 12:39 - 13:39

Visitor ID: Visitor02 Visitor02

Escort User

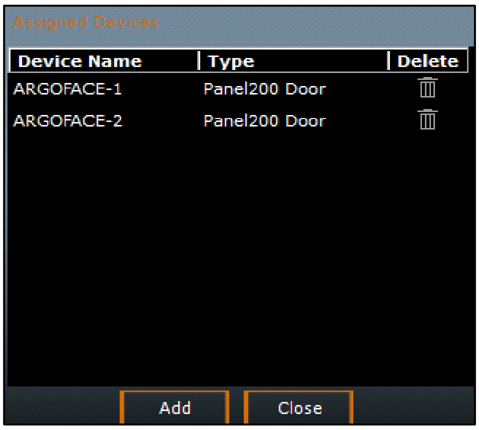
Visitor Type: General Visitor

Visit Type: Personal

Additional Visitors

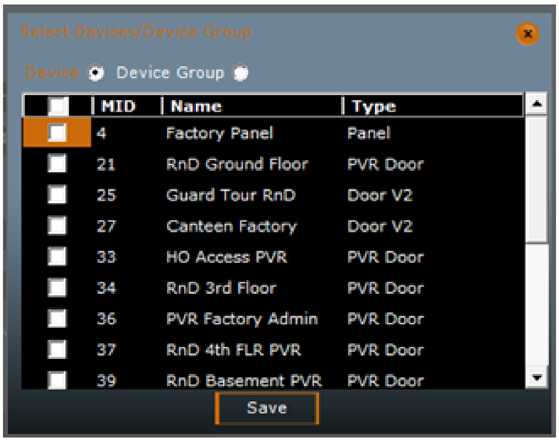
Purpose

The Assigned Devices window appears as shown below. Click **Add**. Then select the devices by checking the box from the pop up window. Click **Save**.



Assigned Devices

Device Name	Type	Delete
ARGOFACE-1	Panel200 Door	🗑
ARGOFACE-2	Panel200 Door	🗑



Select Devices/Device Group

Device ● Device Group ○

□	MID	Name	Type
□	4	Factory Panel	Panel
□	21	RnD Ground Floor	PVR Door
□	25	Guard Tour RnD	Door V2
□	27	Canteen Factory	Door V2
□	33	HO Access PVR	PVR Door
□	34	RnD 3rd Floor	PVR Door
□	36	PVR Factory Admin	PVR Door
□	37	RnD 4th FLR PVR	PVR Door
□	39	RnD Basement PVR	PVR Door

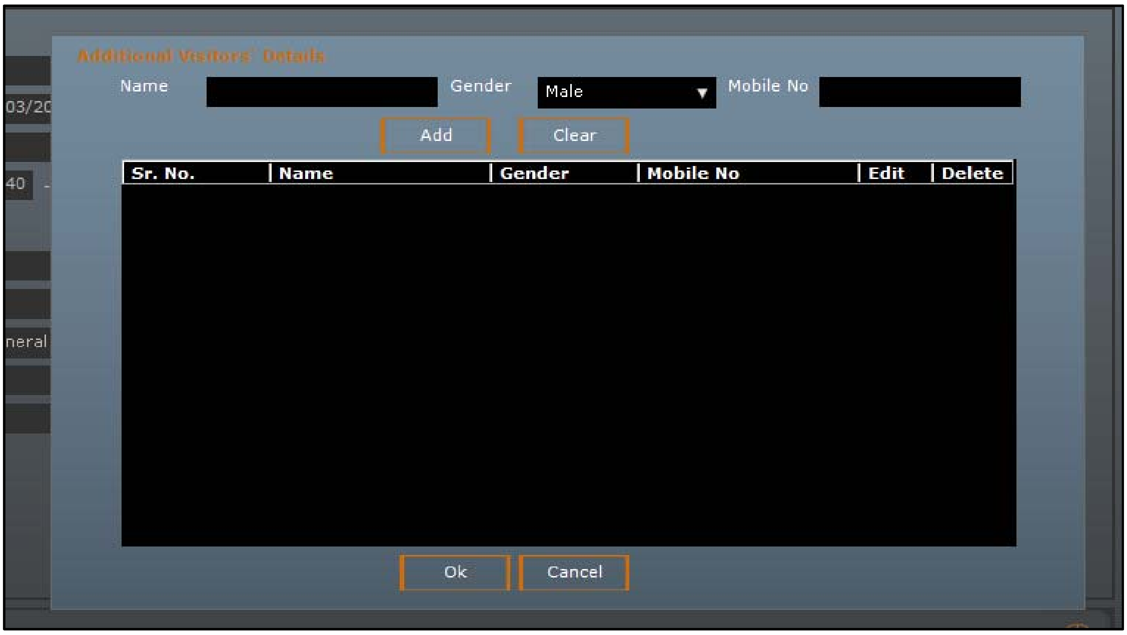
To delete the assigned devices, click **Delete** 🗑 button.

If any device or a device belonging to any device group is un-assigned against any visitor, is selected for deletion and is a part of the Access Rule which is assigned to that visitor, then that door(s) will be retained against that visitor. For details, refer to Access Rule in the User Guide.

Select desired **Escort User** from the provided picklist and enter their respective mobile numbers.

Select the desired **Visitor Type** and **Visit Type**.

In case of **Additional Visitors**, click **Add** ⊕ button.



Additional Visitors' Details

Name:

Gender: Male

Mobile No:

Sr. No.	Name	Gender	Mobile No	Edit	Delete

Enter Name, Gender and Mobile Number of the respective Additional Visitor.

Click **Add.** The details of the Additional Visitor will be displayed in the grid below.

Click **Ok.**

Enter the **Purpose** of the Visit of the above configured Visitors.

Select **Enable Elevator Access Control** check box and select the desired **Elevator Floor Group** from the provided picklist.

Enter the vehicle details if not available in the system. You can also enter **Basic details** and **Additional details** of visitor when new pass is created.*See "Visitor Details" on page 81.*

Then click **Create Pass** to create the pass of pre-registered visitor.

Whenever, security creates pass, visitor is treated as **Checked - in** firm and the Visit State changes.

The Visitor Pass alert is sent to visitor.

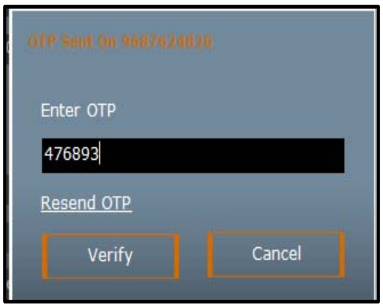
The Visit State change alert is sent to Host with Start button.

The Visit State change alert is sent to Security (having VMS Utility rights) without any button.

If **Send OTP for Verification** is enabled from Global Policy then OTP will be sent to the mobile number of the visitor. This is to verify that the visitor is genuine and the mobile number available in the system matches with the number of the visitor.

Also while sending the OTP to the visitor, same OTP will be stored in memory of VMS Utility.

The OTP received on the visitor's mobile must be entered in the system. Then click **Verify** button. This will verify the entered OTP with the OTP stored in the memory. If OTP matches, pass can be created.



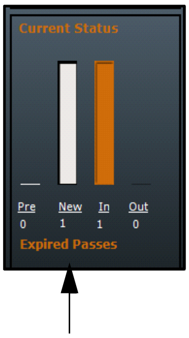
OTP Sent On 9687624826

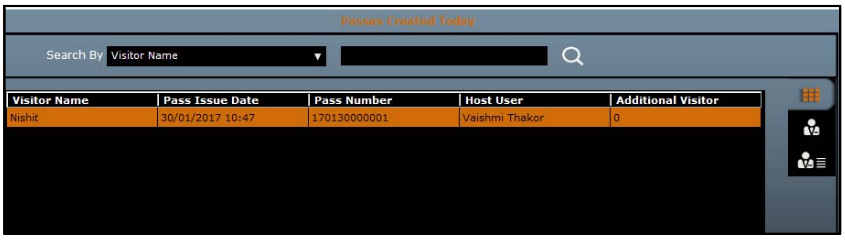
Enter OTP: 476893

The pass can be generated after configuring Pass template. For more information refer *"Visitor Pass Template"*. To know more about how to configure the printer for printing the pass refer *"Visitor Pass Template".*

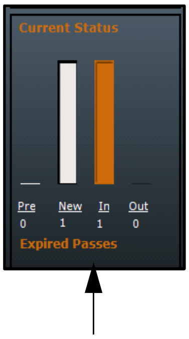
If **Send OTP for Verification** is disabled from Global Policy then pass will be created without sending OTP.

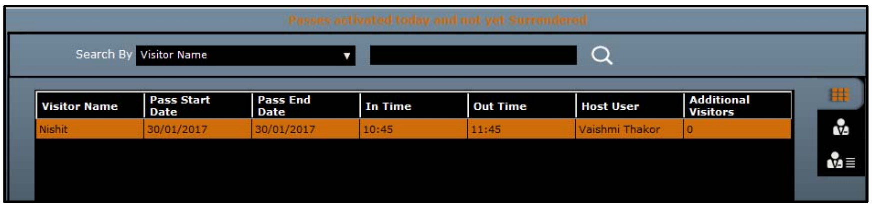
After the pass gets created, the Current Status will show **New** pass created today and **In** shows the visitor who is inside the premises and the pass is not yet surrendered.





Visitor Name	Pass Issue Date	Pass Number	Host User	Additional Visitor
Nishit	30/01/2017 10:47	170130000001	Vaishmi Thakor	0

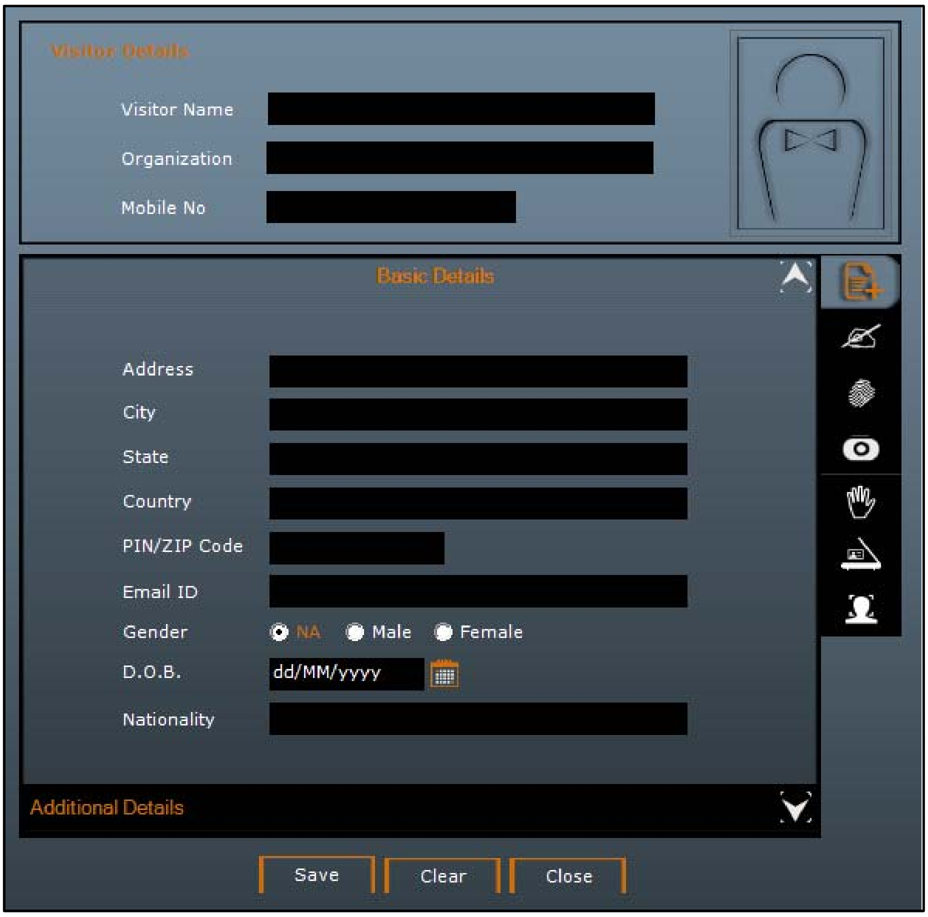




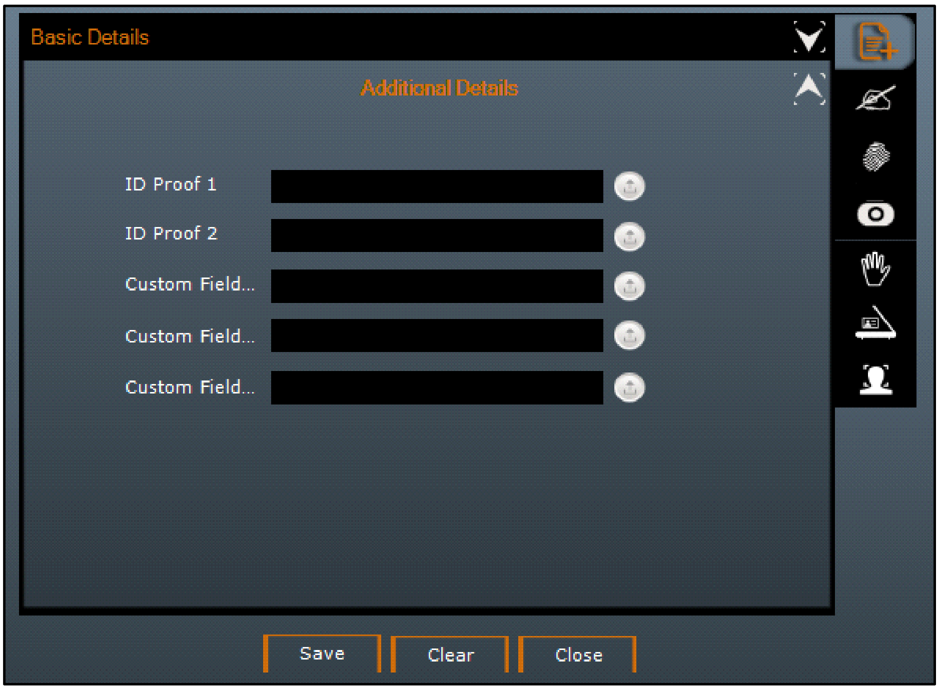
Visitor Name	Pass Start Date	Pass End Date	In Time	Out Time	Host User	Additional Visitors
Nishit	30/01/2017	30/01/2017	10:45	11:45	Vaishmi Thakor	0

New Visitors

This section enables you to enter details of a new visitor, take the signature of visitor, enroll fingerprint and capture photograph of the visitor. Also you can create the pass of visitor.



Gender ● NA ○ Male ○ Female



Enter Visitor’s Name, Visitor’s Organization and Mobile No.

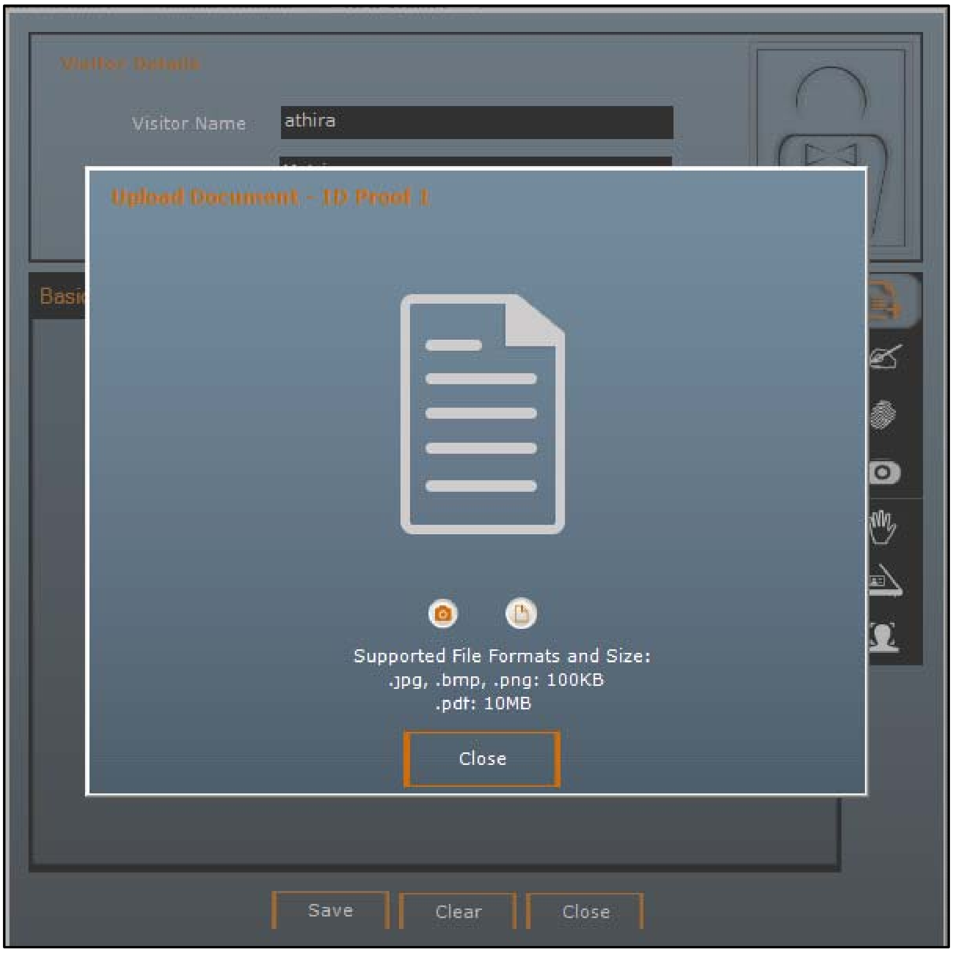
Now configure the following parameters:

- *“Add Additional Visitor Details”*
- *“Add Visitor Signature”*
- *“Enroll Visitor Finger”*
- *“Capture Visitor Photo”*
- *“Enroll Visitor Palm”*
- *“Read Visitor’s Information”*
- *“Enroll Visitor Face”*

Add Additional Visitor Details

Enter visitor’s **Basic** and **Additional Details**.

For certain parameters under **Additional Details,** you will be asked to upload respective documents, if available. To upload, click **Upload** button. The **Upload Document** pop-up appears as shown below:



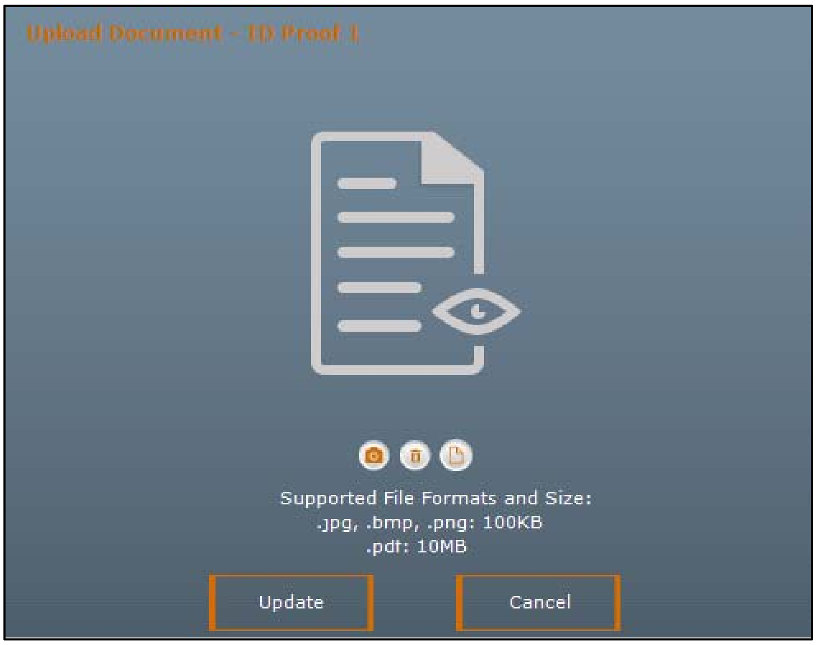
Supported File Formats and Size:
.jpg, .bmp, .png: 100KB
.pdf: 10MB

To upload the document, click **Document** . Make sure the documents are as per the formats and size supported by the system.

You can even capture the image of the required document by clicking **Capture** and then upload it.

You will be able to delete the document/image you selected to upload, by clicking **Delete** .

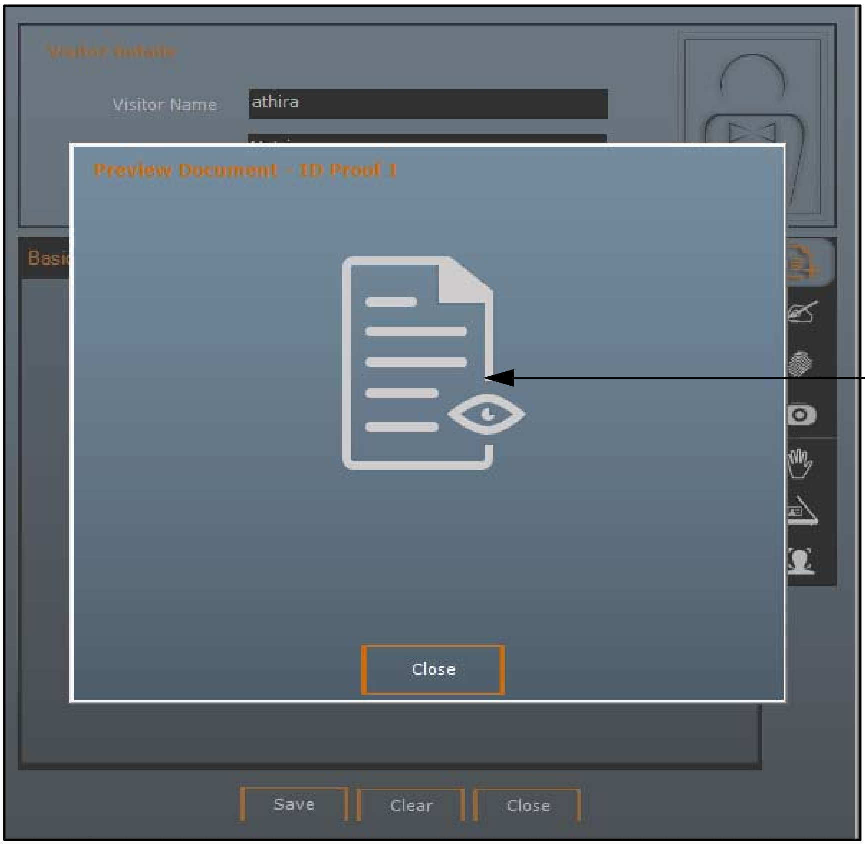
Click **Update.**



Upload Document - ID Proof 1

Supported File Formats and Size:
.jpg, .bmp, .png: 100KB
.pdf: 10MB

Once you update the file, you can preview the uploaded file. To preview, click **Preview** button. **Preview Document** window appears where you can preview as well as download the uploaded document by clicking on the document icon shown below:



Click here to download the Uploaded document/image

Custom Fields in Additional Details are visible only after they are configured by your System Administrator.

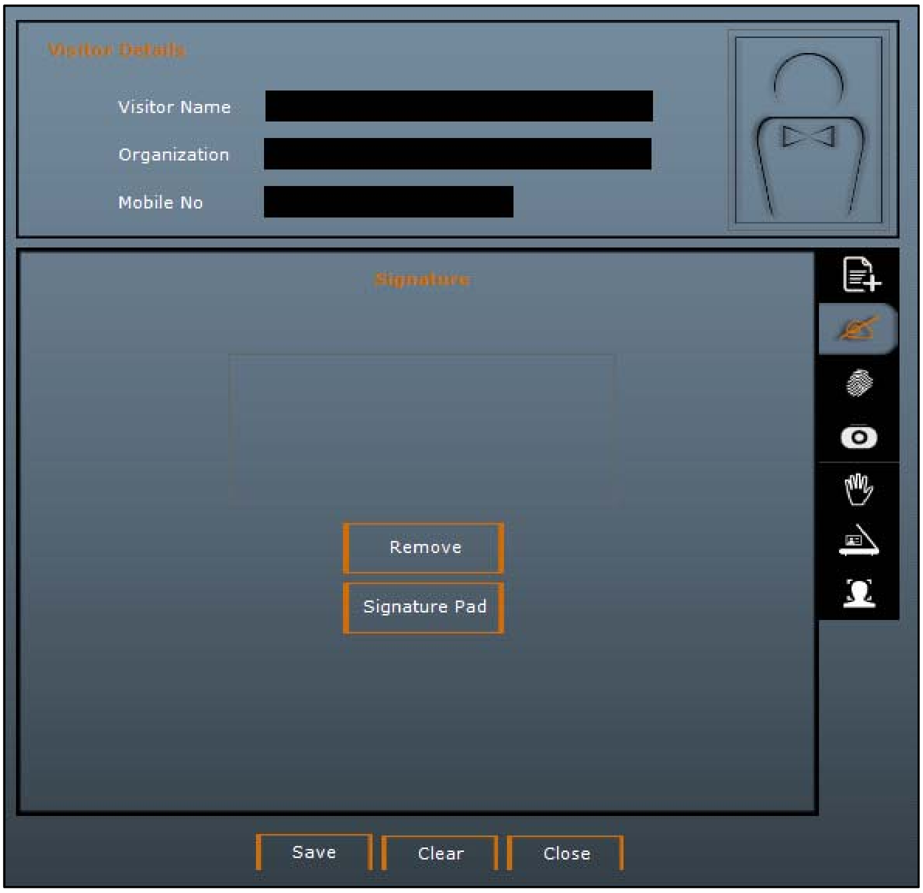
If the user has identity card then his card can be scanned to get the visitor details automatically. This will reduce the work of entering visitor's detail manually. For more information, *See "Read Visitor's Information" on page 38.*

Click **Save**.

Add Visitor Signature

To add visitor's signature click on **Add Visitor Signature** button.

Then click on Signature pad to connect the signature pad to the software from where you can take visitor’s signature.



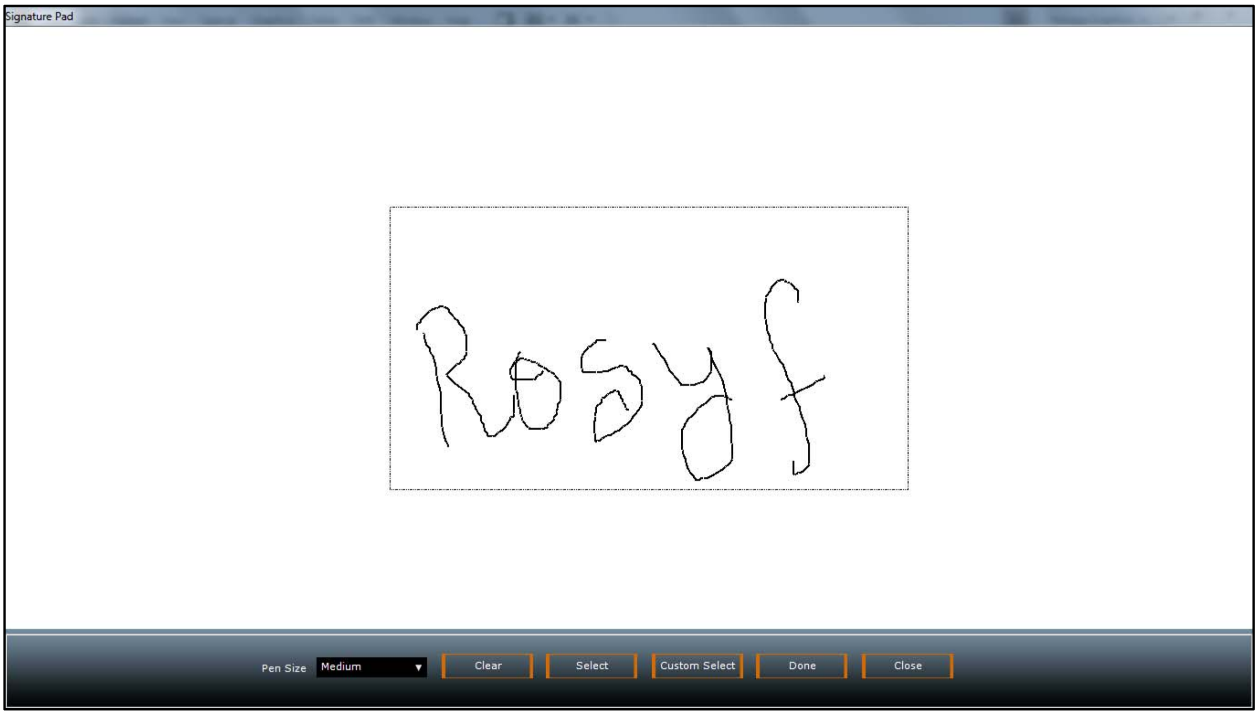
Visitor Details

Visitor Name [redacted]

Organization [redacted]

Mobile No [redacted]

The Signature pad opens as shown below.



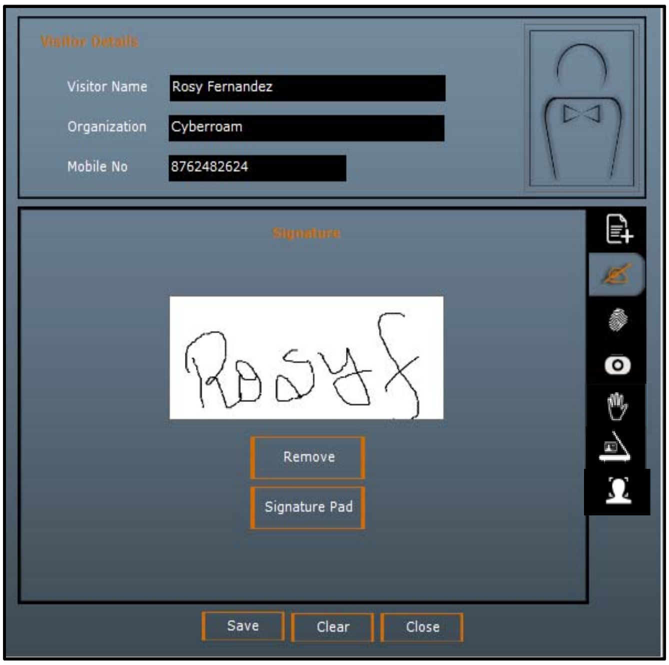
Pen Size: Medium

Select the **Pen size** as Normal, Medium or High as per which the thickness of font will be changed.

Then click **Custom Select** and draw a rectangular region using mouse.

Now the visitor can write the signature in that box.

Once the signature is done, click on **Done.** The signature will appear on Visitor Details page.



Visitor Details

Visitor Name: Rosy Fernandez

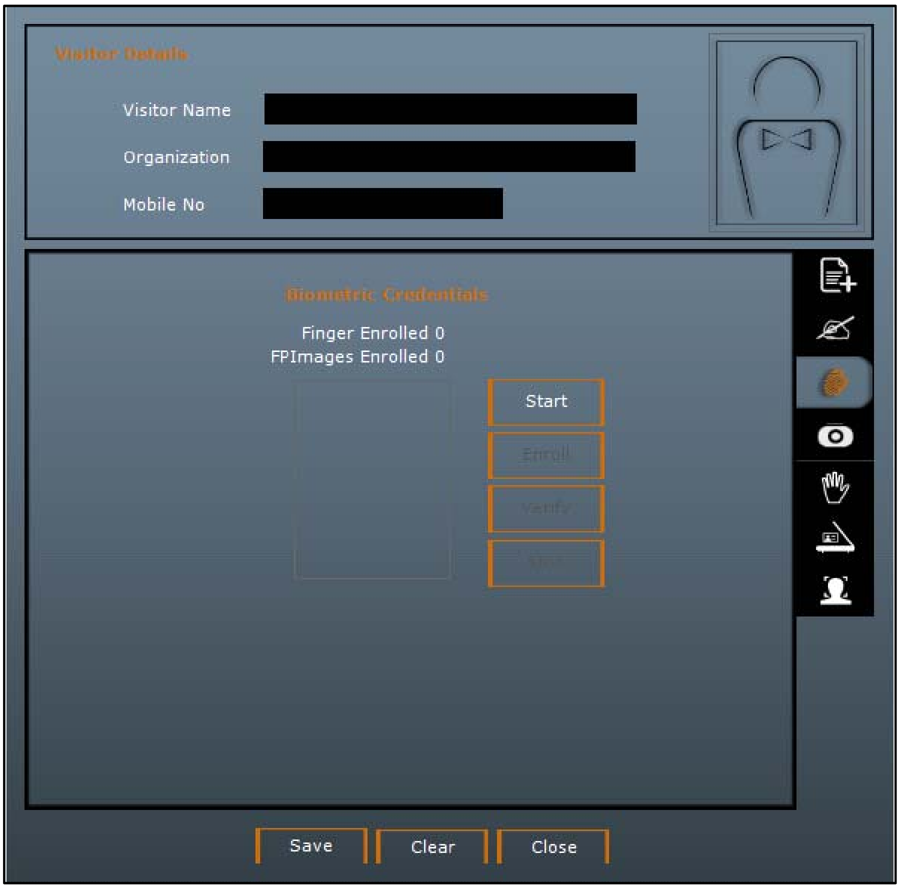
Organization: Cyberroam

Mobile No: 8762482624

Click on **Save** to save the Signature of visitor.

Enroll Visitor Finger

To enroll fingerprint of visitor, click on Enroll Visitor Finger button.



Visitor Details

Visitor Name [redacted]

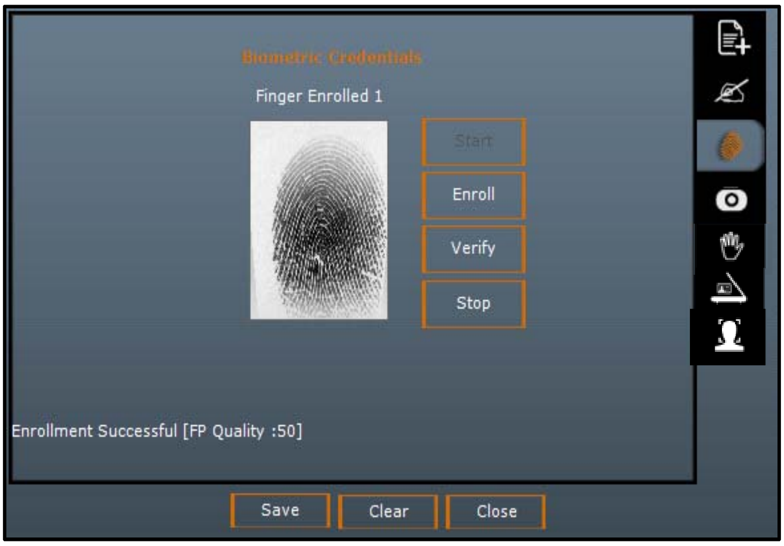
Organization [redacted]

Mobile No [redacted]

Biometric Credentials

Finger Enrolled 0
FPImages Enrolled 0

Now using enrollment station, the fingerprint can be enrolled. Click **Start** button and place the finger on sensor. Click **Enroll** to enroll the fingerprint. After enrollment click **Verify** to verify the credential.



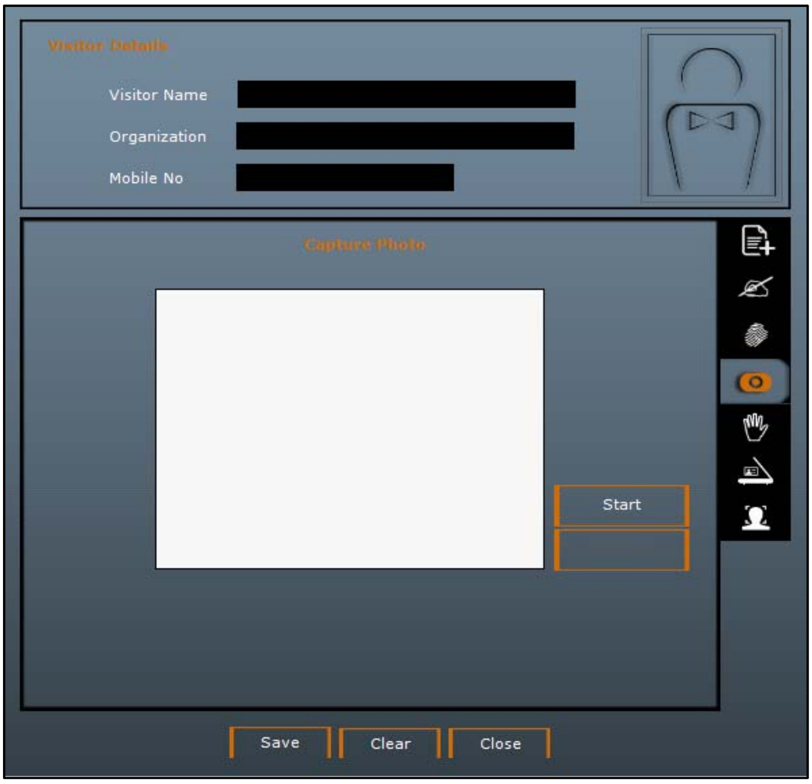
Biometric Credentials

Finger Enrolled 1

Enrollment Successful [FP Quality :50]

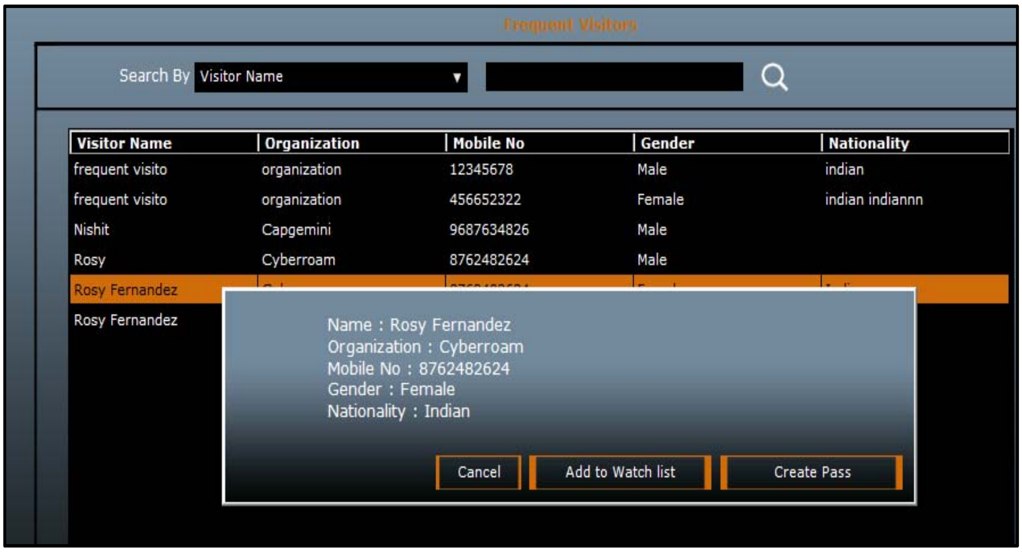
Capture Visitor Photo

To capture the photograph of visitor, click on Capture Visitor Photo button.



Click **Start**. When the visitor is in front of camera, then click **Capture** button to capture the image.

Click on the **Save** button. The Visitor will be visible in the Frequent Visitors list as shown below. See Frequent Visitors section.



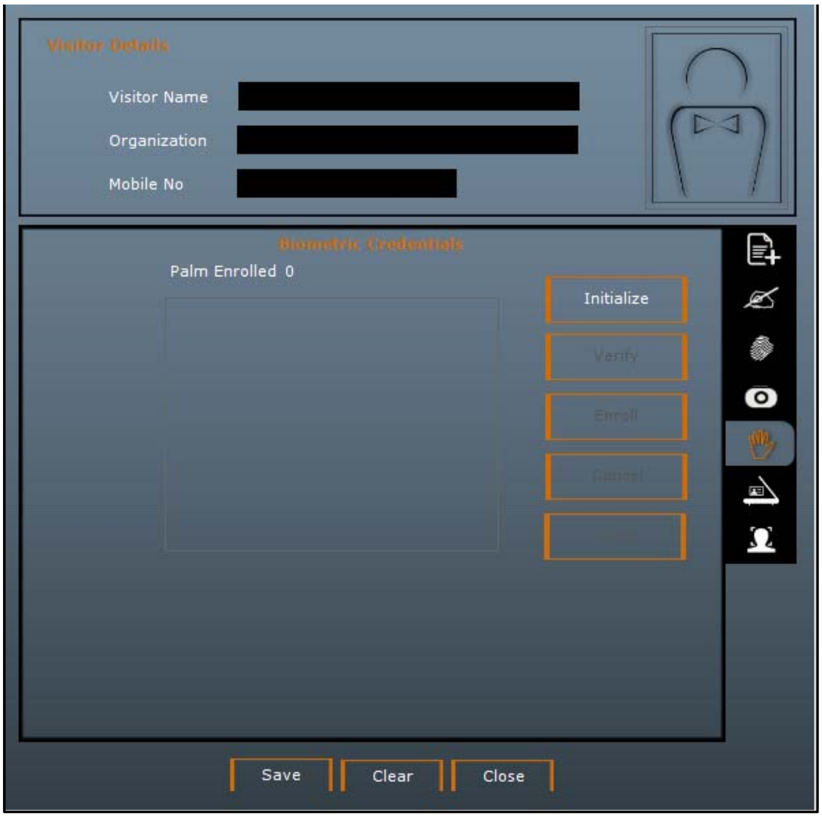
Visitor Name	Organization	Mobile No	Gender	Nationality
frequent visito	organization	12345678	Male	indian
frequent visito	organization	456652322	Female	indian indiannn
Nishit	Capgemini	9687634826	Male	
Rosy	Cyberroam	8762482624	Male	
Rosy Fernandez	[illegible]	[illegible]	[illegible]	[illegible]
Rosy Fernandez				

Name : Rosy Fernandez
Organization : Cyberroam
Mobile No : 8762482624
Gender : Female
Nationality : Indian

Enroll Visitor Palm

To enroll Palm of visitor, click on Enroll Visitor Palm button.

“Enroll Visitor Palm” icon will be enabled only when “Enable Palm Module” is enabled in Settings.



Visitor Details

Visitor Name [redacted]

Organization [redacted]

Mobile No [redacted]

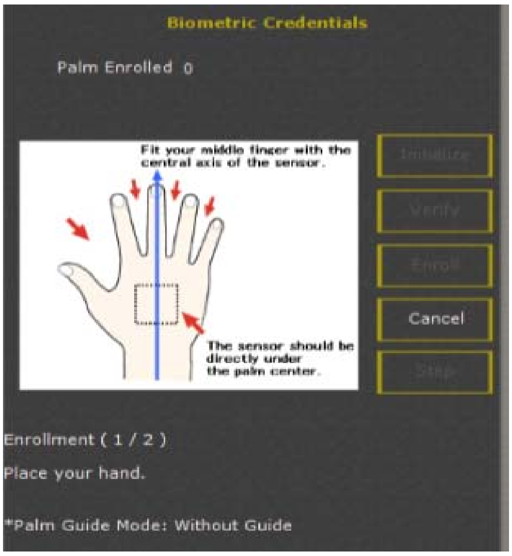
Biometric Credentials

Palm Enrolled 0

Now using PVR enrollment station, the Palm can be enrolled. Click **Initialize** button and place the Palm on sensor.

You can enable the **‘Enroll In Adaptive Mode’** checkbox once initialized. This will allow the Palm Templates to be compressed and saved into the COSEC server for the identification through the smart card (MiFare 4k). *Refer COSEC Server User Guide for more details about Door PVR in an Adaptive mode.*

Click **Enroll** to enroll the palm template. After enrollment click **Verify** to verify the credential.


Biometric Credentials

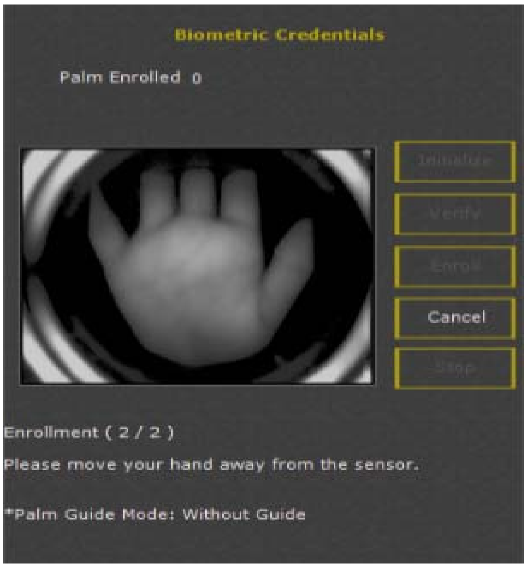
Palm Enrolled 0

Fit your middle finger with the central axis of the sensor.
The sensor should be directly under the palm center.
Initialize
Verify
Enroll
Cancel
Stop

Enrollment (1 / 2)

Place your hand.

*Palm Guide Mode: Without Guide

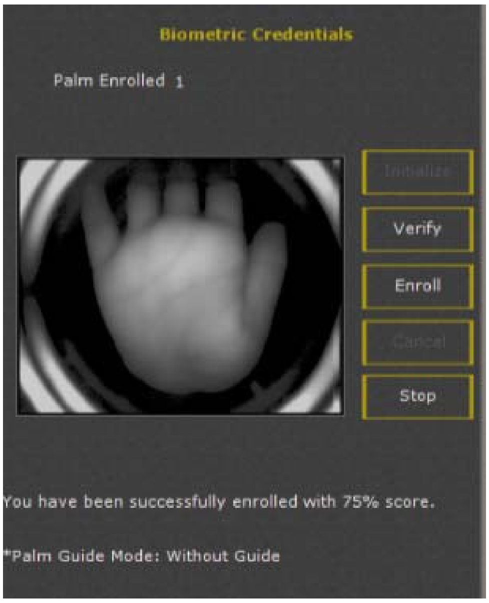

Biometric Credentials

Palm Enrolled 0

Enrollment (2 / 2)

Please move your hand away from the sensor.

*Palm Guide Mode: Without Guide

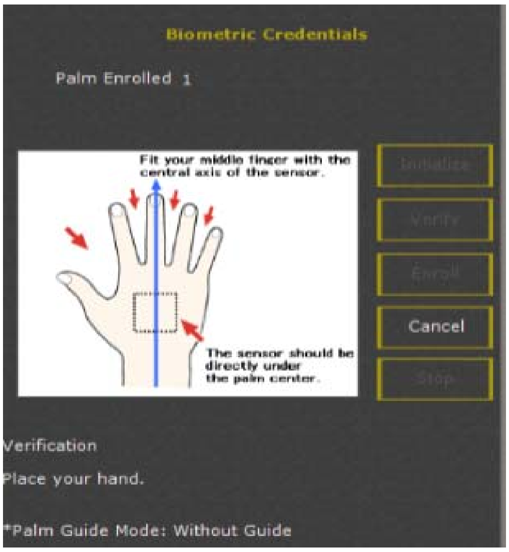

Biometric Credentials

Palm Enrolled 1

You have been successfully enrolled with 75% score.

*Palm Guide Mode: Without Guide

Click on the **Save** button. After enrollment click **Verify** to verify the credential.


Biometric Credentials

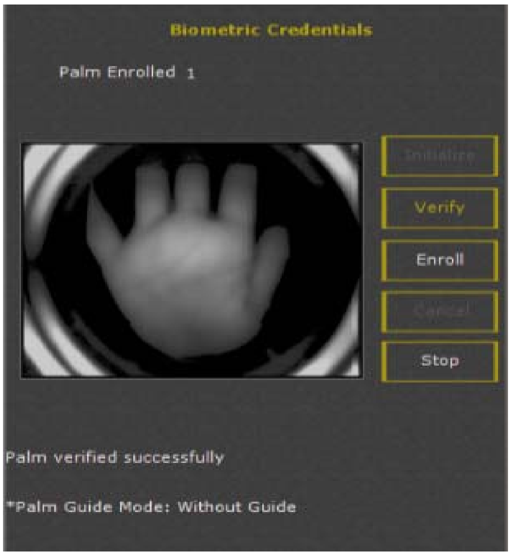
Palm Enrolled 1

Fit your middle finger with the central axis of the sensor.
The sensor should be directly under the palm center.
Initialize
Verify
Enroll
Cancel
Stop

Verification

Place your hand.

*Palm Guide Mode: Without Guide


Biometric Credentials

Palm Enrolled 1

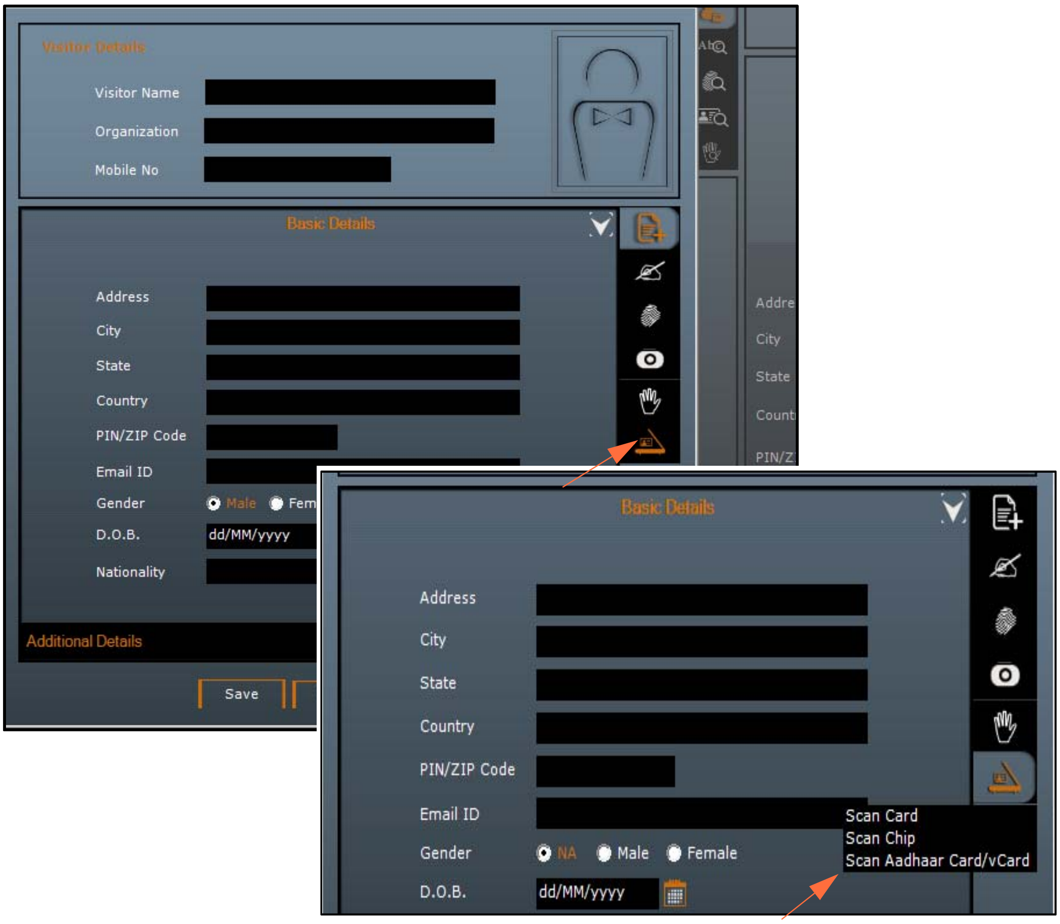
Palm verified successfully

*Palm Guide Mode: Without Guide

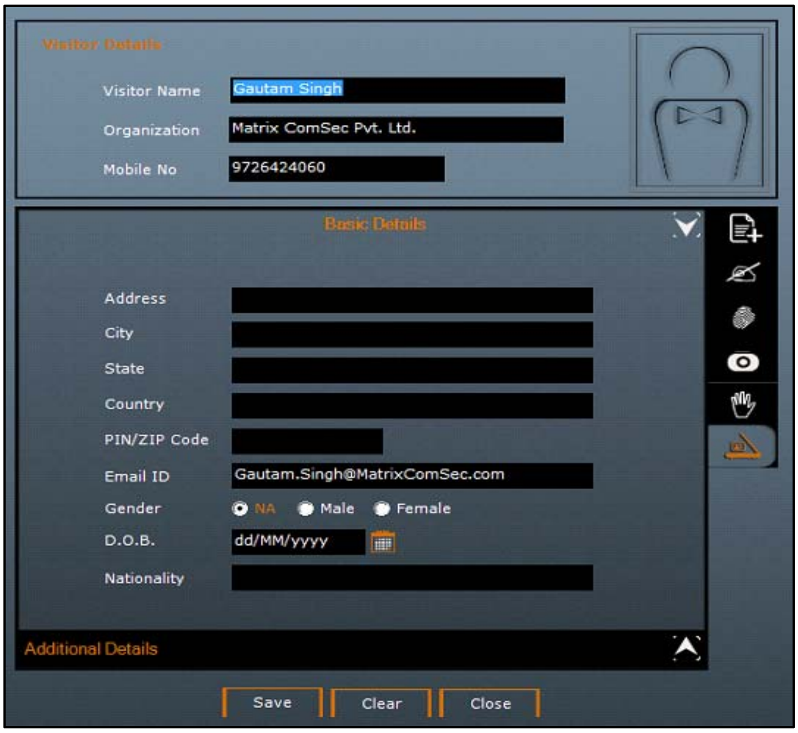
Read Visitor’s Information

When Samsotech Scanner / QR code Scanner is connected with VMS Utility then user Identity card (Driving License, PAN Card, Aadhar Card, Passport etc) can be scanned to get the information in VMS Utility.

Click on **Read Visitor’s Information** icon as shown below. Then you can click on **Scan Card**, **Scan Chip** or **Scan Aadhar Card/ vCard** depending on the identity card to scan the visitor’s information.



After successful scanning the visitor’s information will automatically appear in the Visitor Details fields as shown below. This is based on the Reader Configuration done in COSEC Web > Visitor Management > Visit Components.



Visitor Details

Visitor Name	Gautam Singh
Organization	Matrix ComSec Pvt. Ltd.
Mobile No	9726424060

Basic Details

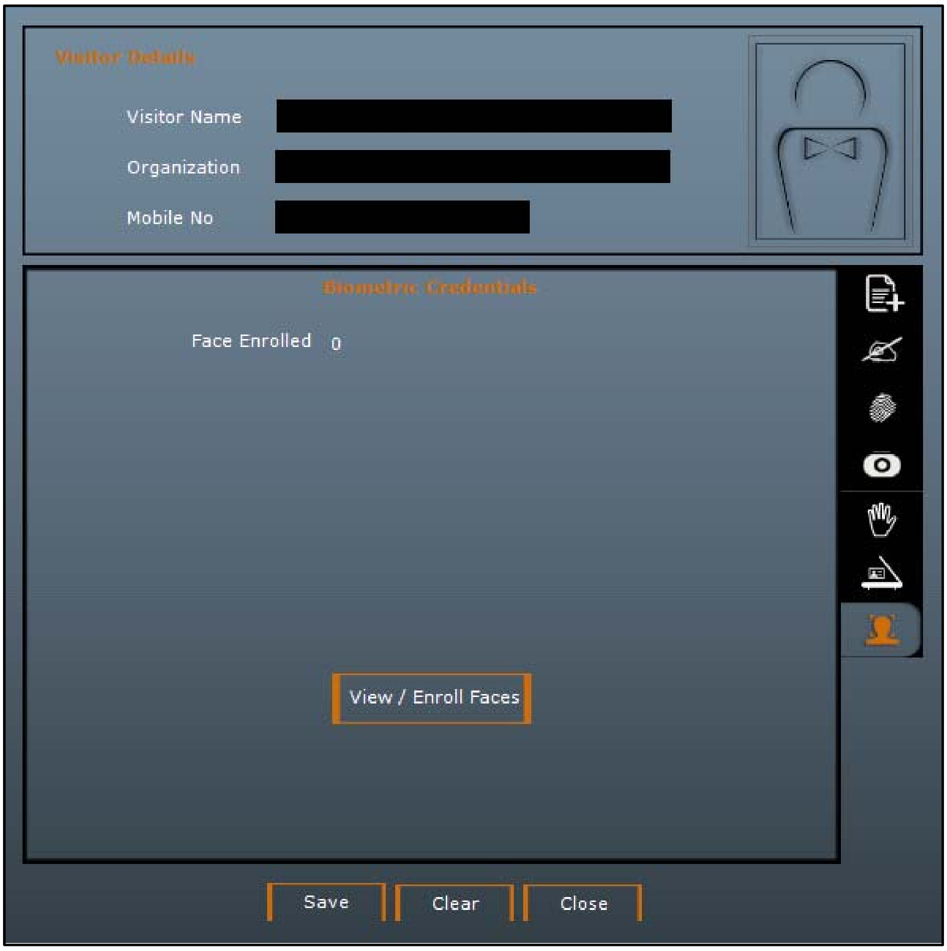
Address	
City	
State	
Country	
PIN/ZIP Code	
Email ID	Gautam.Singh@MatrixComSec.com
Gender	● NA ○ Male ○ Female
D.O.B.	dd/MM/yyyy
Nationality	

Additional Details

Additional detail's Id Proof field can be added automatically though scanning of Aadhar card. This can be done from Settings> Input Settings> Camera Settings> ***Scanning QR code*** *(See "Input Settings" on page 69. for more information).*

Enroll Visitor Face

You can enroll a visitor's face credential using **Enroll Visitor Face**. Click 👤 icon and the following page appears:



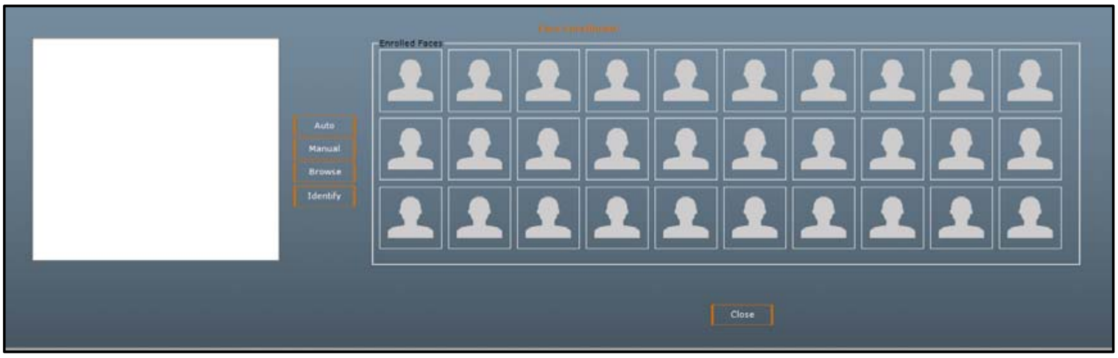
Visitor Name [redacted]

Organization [redacted]

Mobile No [redacted]

Face Enrolled 0

To view already enrolled face images or to enroll new face images, click **View/Enroll Faces** and the following window appears.

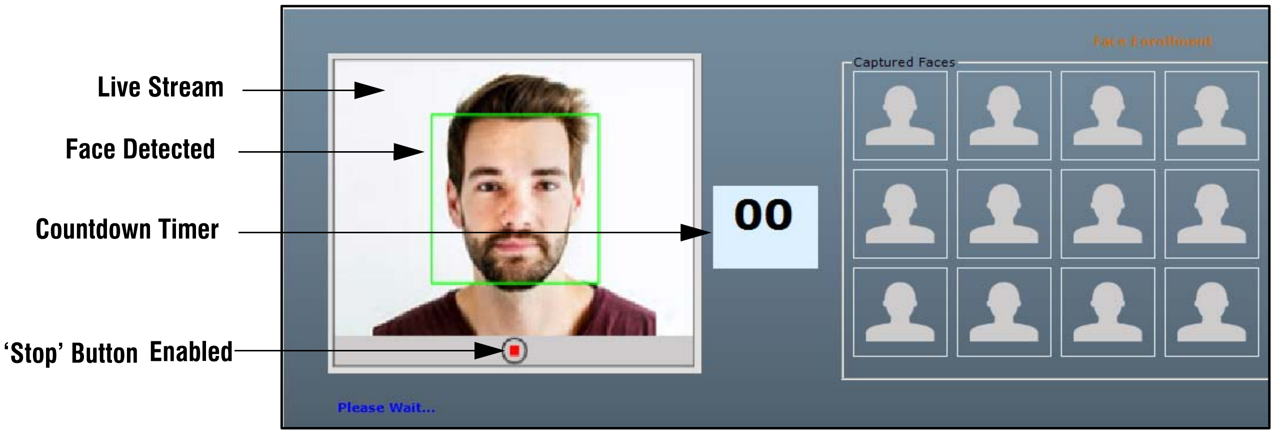


For new enrollment, 3 methods for capturing an image of visitor's face are provided, which are: **Auto**, **Manual** and **Browse.**

1. **Enrollment via Automatic Face capturing:** This option will automatically capture the images from the IP Camera or USB Camera.

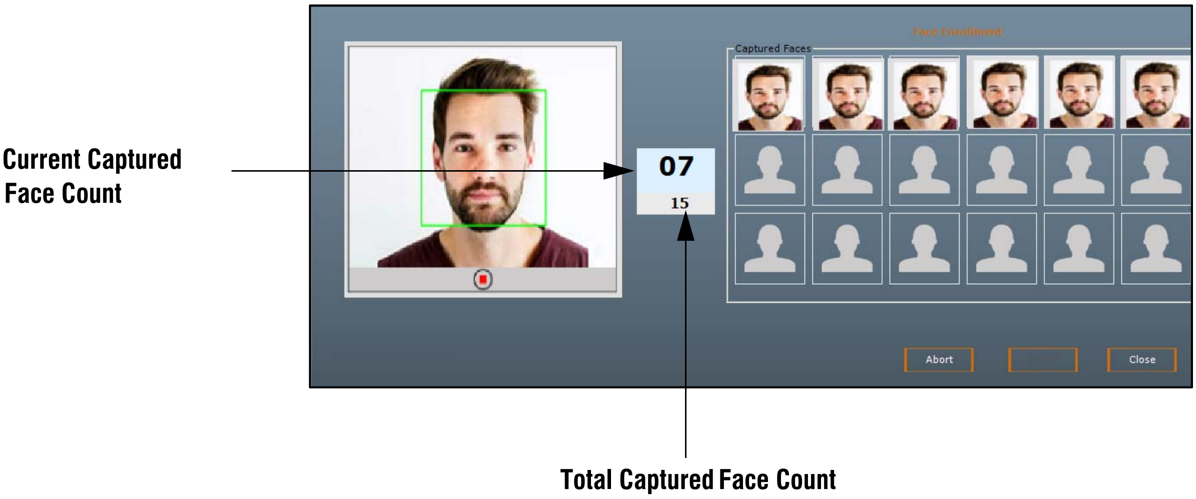
Click **Auto**, the Automatic enrollment screen appears.

A countdown timer will be displayed, after which Enrollment process will begin. So, the visitor needs to be ready in front of camera to capture his/her face image.



As the enrollment process begins, status of captured image count and total captured image count will be displayed.

For Auto, total captured face count will be as per the time configured for one enrollment cycle in FR Settings. e.g. If Time for one enrollment cycle is selected as 6 seconds, face count displayed will be 30 and if Time for one Enrollment Cycle is selected as 3 seconds, face count displayed will be 15.

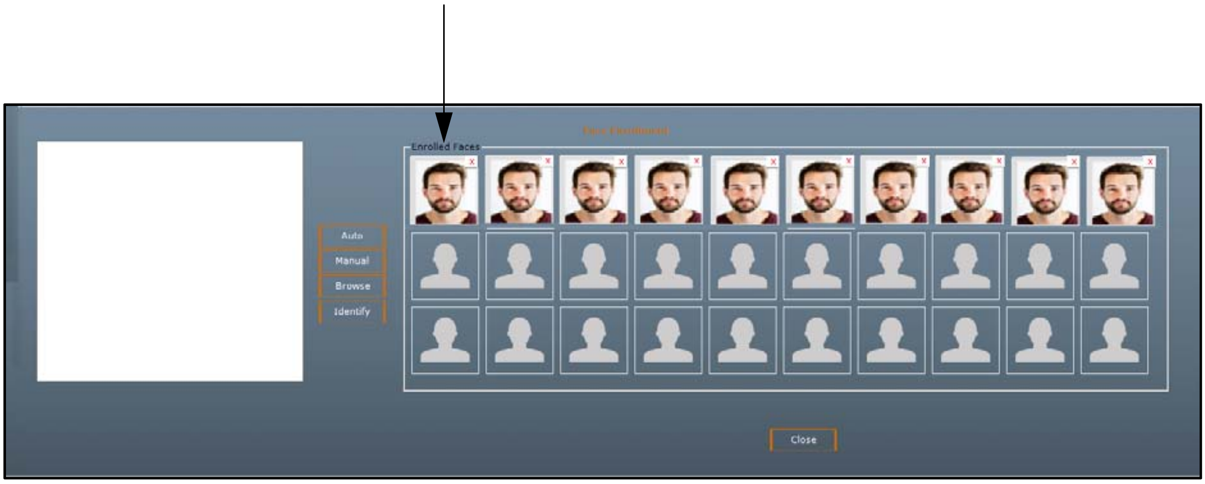


The captured image count will be updated along with the enrollment process.

Captured face will be displayed in the 'Captured Faces' grid.

*At Face Count 0 (that is Index Number 0), make sure you enroll the desired face image of a visitor as it will be set as Visitor's Profile Photo if the **Auto Add/Update Enrolled Face as Profile Photo** checkbox is enabled in the COSEC Web (Admin Module> System Configuration> Global Policy) by the System Administrator.*

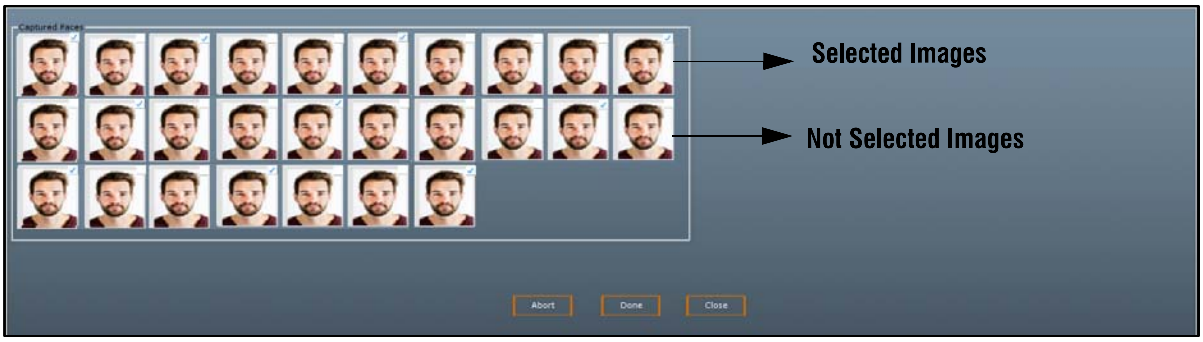
Enrolled Faces



When **Verify before Auto Enroll** is disabled in Settings > FR Settings, enrollment of the Captured Faces will be done directly without any verification process only on the click of the **Enroll** button.

If **Verify Before Auto Enroll** is enabled, you will be required to verify the captured face images before the system enrolls them automatically against the visitor.

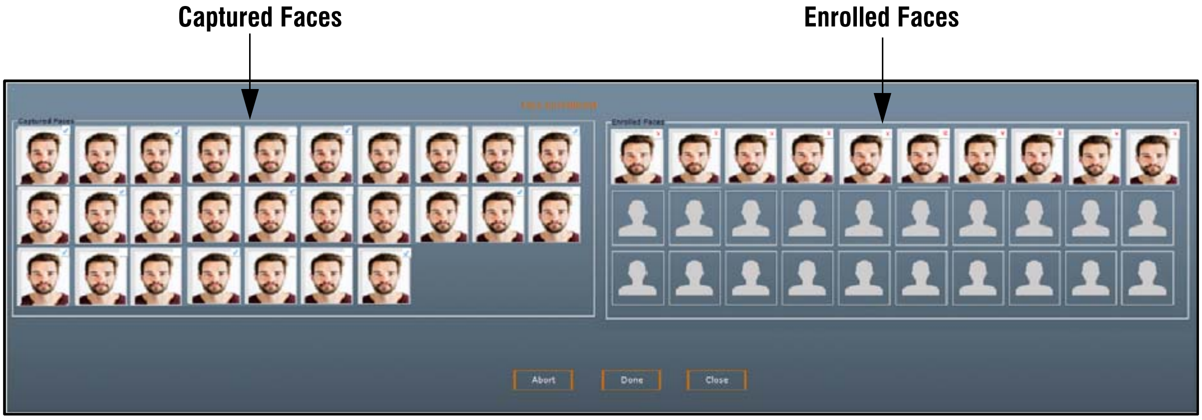
Now, when you are conducting the enrollment process for a new visitor, you need to select the desired images to enroll them against the visitor as shown below.



Selected Images

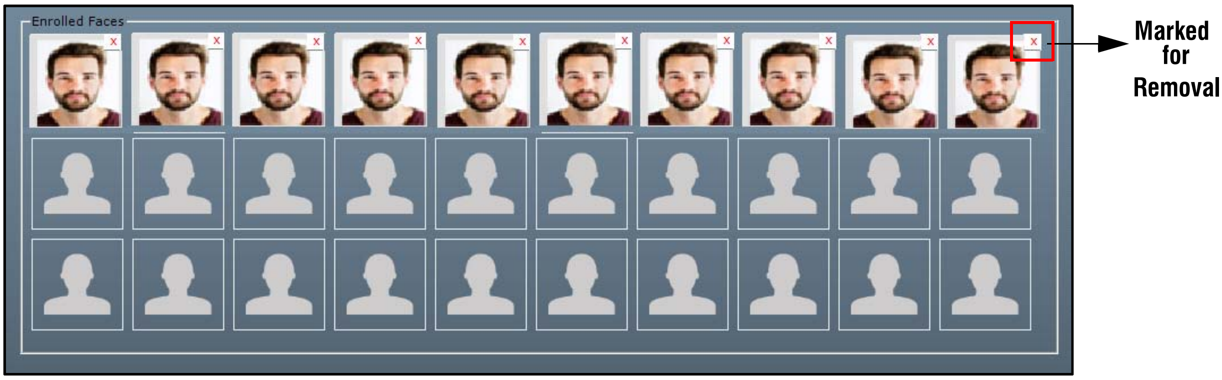
Not Selected Images

But when you are enrolling the face credential for those visitors whose face credential is previously enrolled, the below page will be displayed, where the right side of the page displays the Captured Faces and on the left side, already Enrolled Faces will be displayed if any.



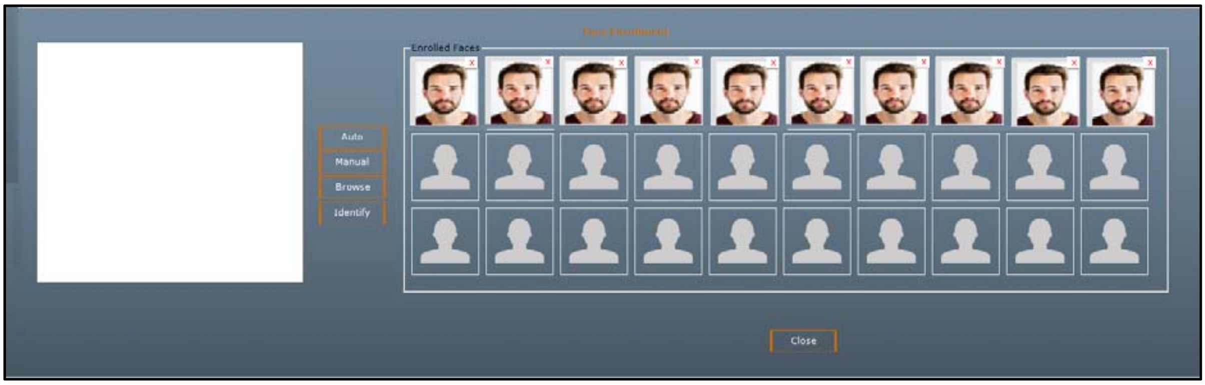
- Now on the Captured Faces grid, there will be ticks on the left top corner on face image which shows the respective faces are selected for enrollment while the ones with no ticks are not selected for the enrollment.

- On the Enrolled faces grid, there will be cross on the left top corner on the face image which shows the respective faces are marked for removal.



Click on **Done** button for enrolling the captured images or click on **Abort** button to remove the captured images as well as to stop the enrollment process.

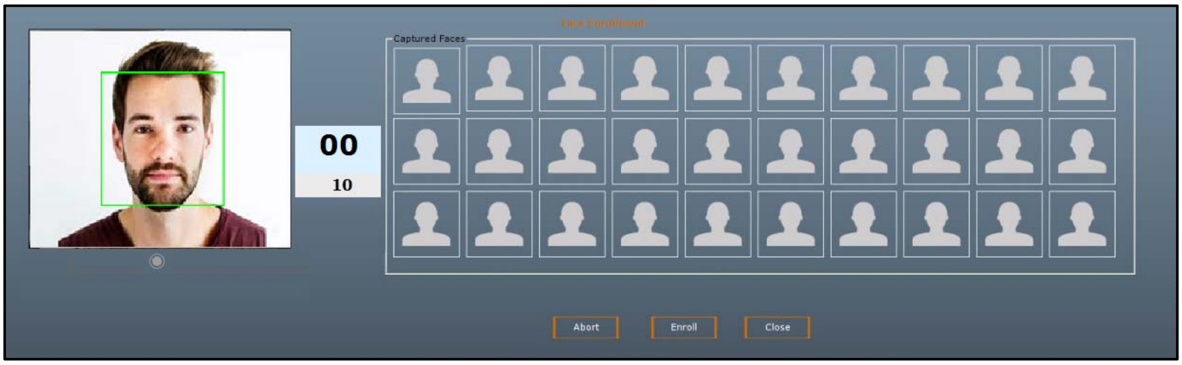
After the process is completed, below page will be displayed and the Automatic Enrollment process ends.



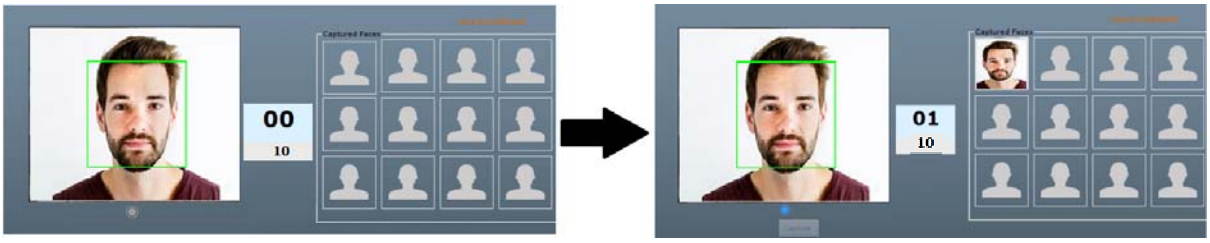
2. **Enrollment via Manual Face capturing:** This option enables you to manually capture the visitor's images via IP Camera or USB Camera.

   Click **Manual**, the Manual enrollment screen appears.

   As the enrollment process begins, status of captured image count and total captured image count will be displayed.



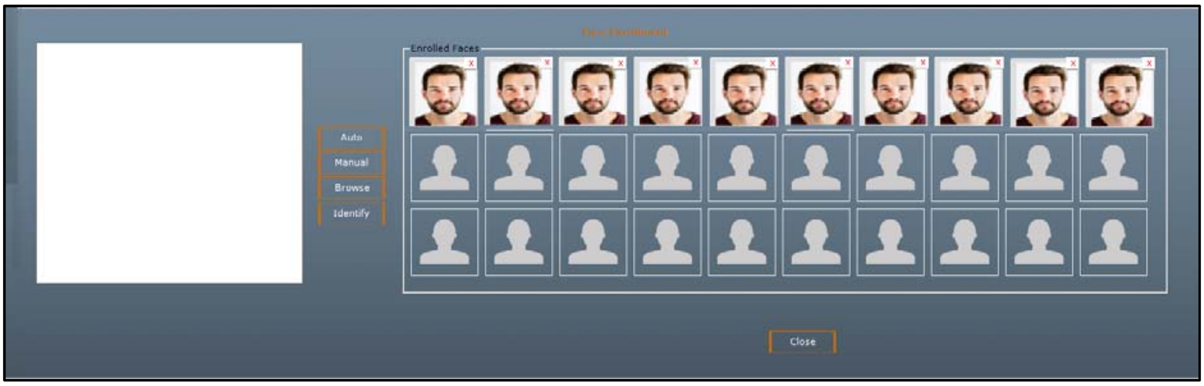
   The captured image count will be updated along with the enrollment process.



   After completing the process, verification view will be displayed with the selected faces same as Automatic face enrollment process.

   Click **Done** for enrolling the captured images or click **Abort** to remove the captured images as well as stop the enrollment process.

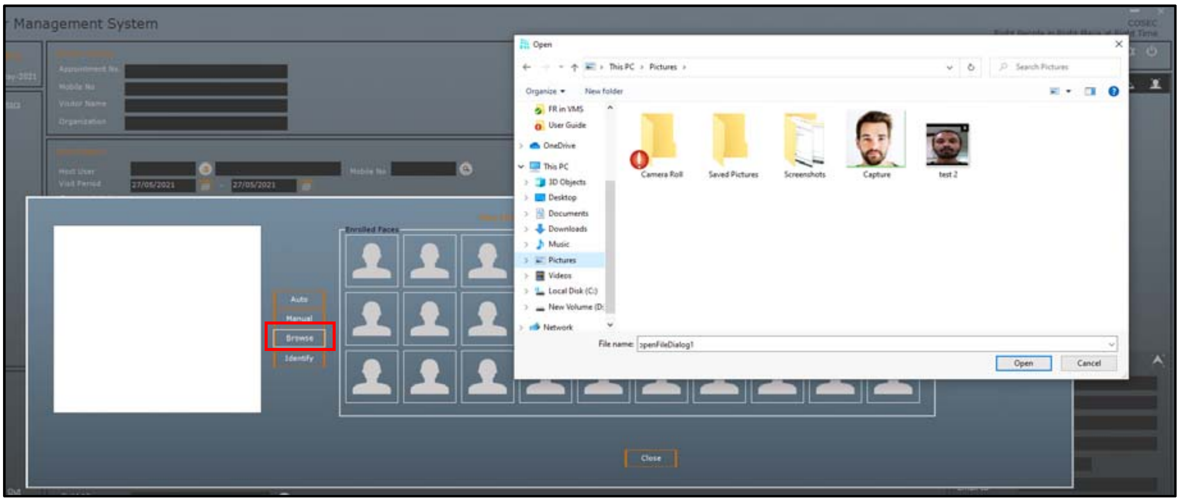
   After the process is completed, below image will be displayed and the Manual Enrollment process ends.



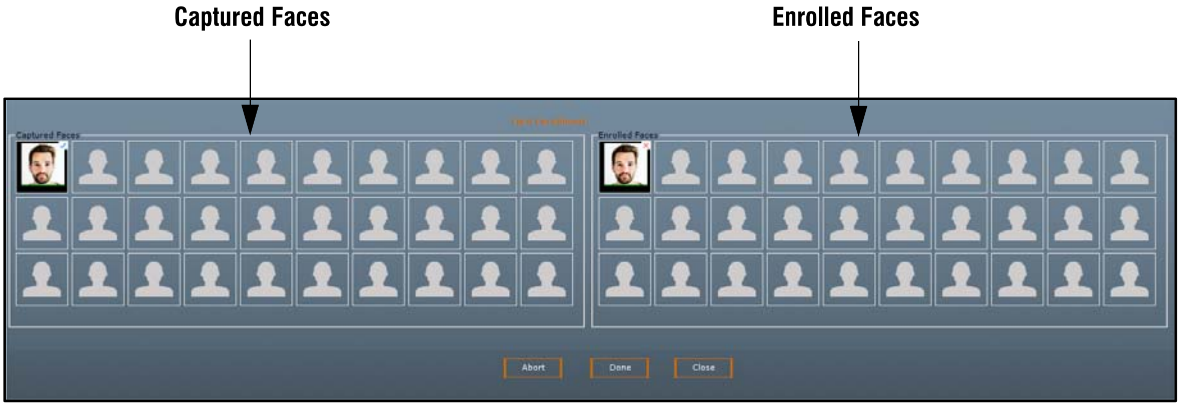
3. **Enrollment via Browsing Face Image:** This option allows enrolling images of the visitor which are already stored in your Computer through browsing.

Click **Browse**, the browse dialogue box will be displayed.

Multiple images can be selected for enrollment.



All selected images will be verified and verified images will be displayed in the Enrolled Faces grid.



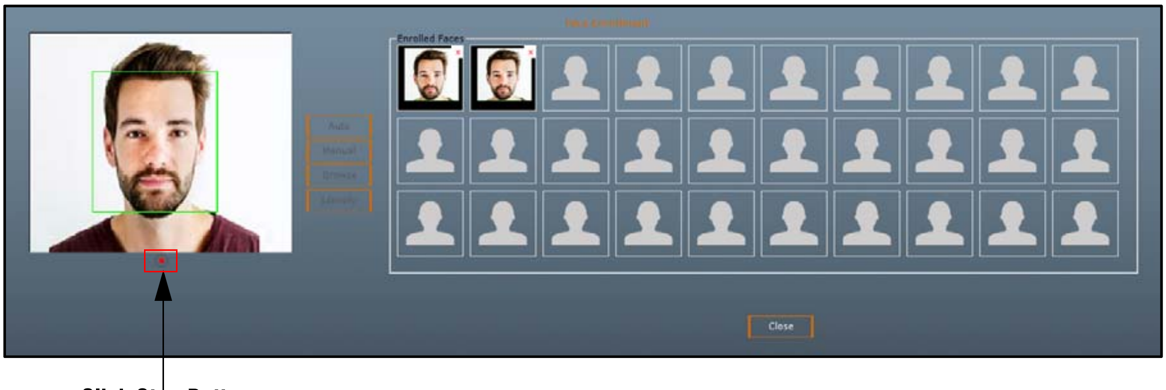
Click **Done** for enrolling the captured images or click **Abort** to remove the captured images and to stop the enrollment process.

4. **Enrollment via Face Identification:** This option is used to identify the visitor from the Live Stream.

   If in sever settings, FR is disabled for any visitor, visitor will not be considered for Identification checking process.

   When you click **Identify**, the Live streaming will start. So the visitor needs to be ready in front of the camera for the identification process.

   Click **Start** button below the live stream.

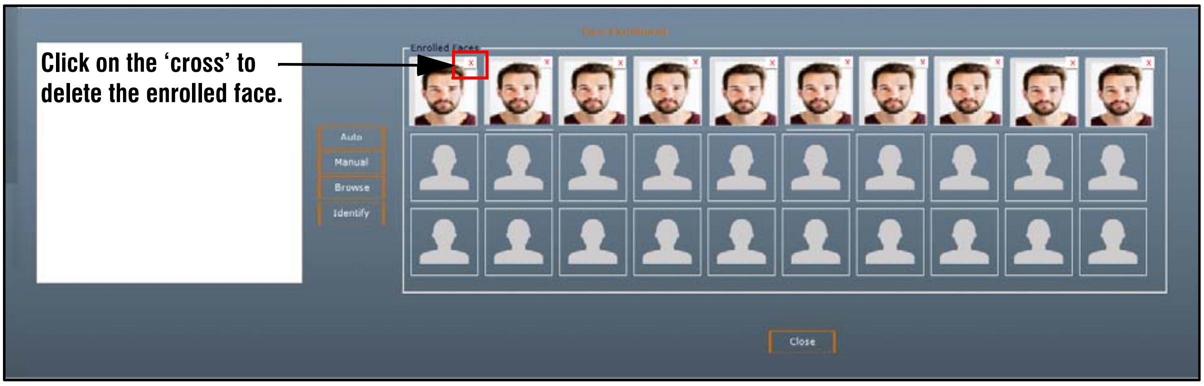


Click Stop Button

After the visitor’s face is visible in Live stream, click on **Stop** button, then a list of identified visitors will be displayed.

Delete Enrolled Faces

You can delete the enrolled faces of a visitor by clicking on the cross ✕ on the left top corner of the image.

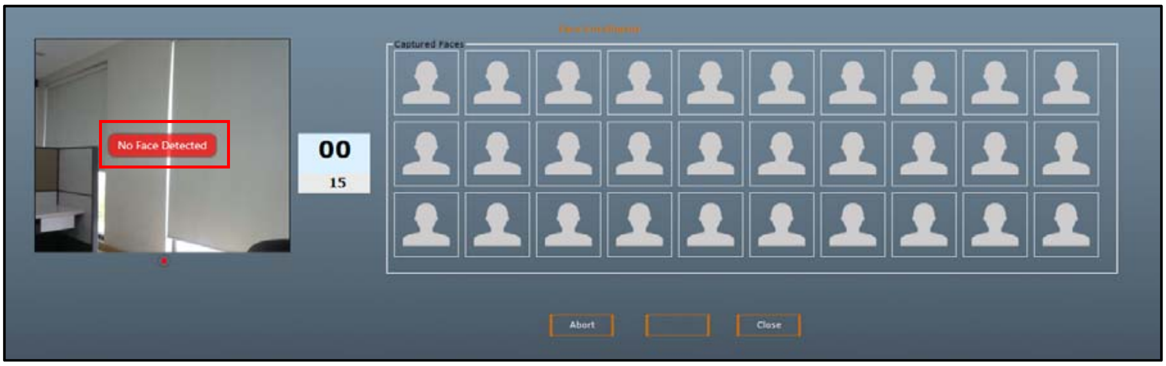


Different Scenarios during Enrollment/Identification of a Visitor

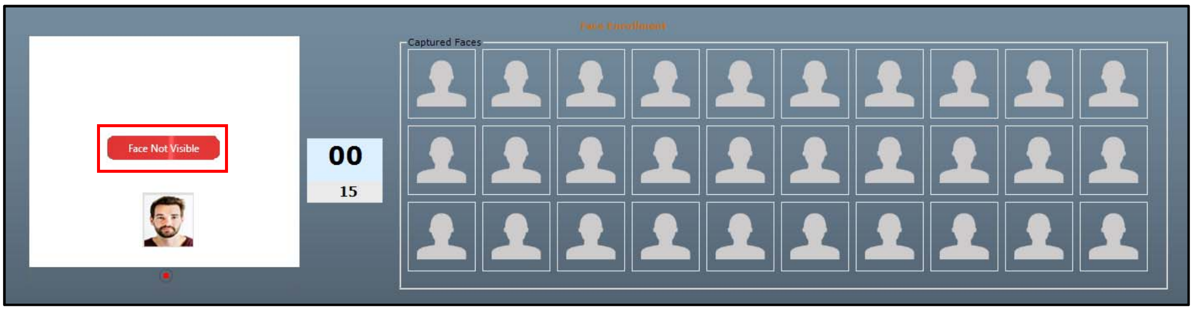
During the enrollment or the identification of a visitor, there can be different scenarios such as —

- No face is detected
- Face is not visible
- Keep face straight
- Conflict checking with other users/visitors
- Different Face is detected

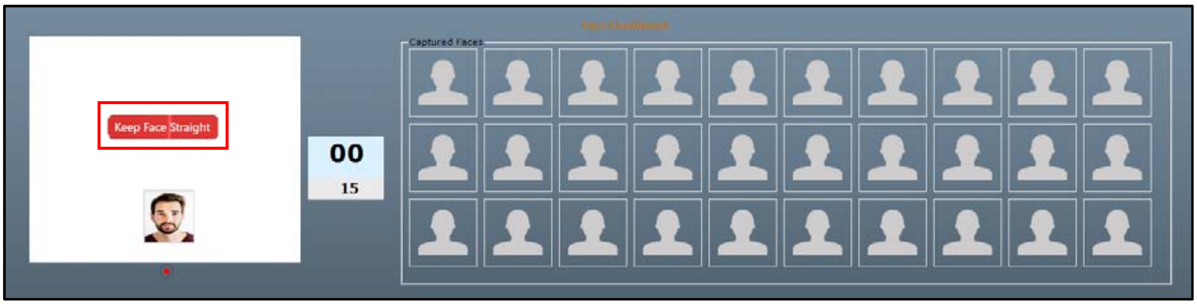
1. **No Face is Detected:** When no face is detected in **Auto**, **Manual** and **Identify** modes, then the enrollment process will be paused. The screen will appear as shown below.



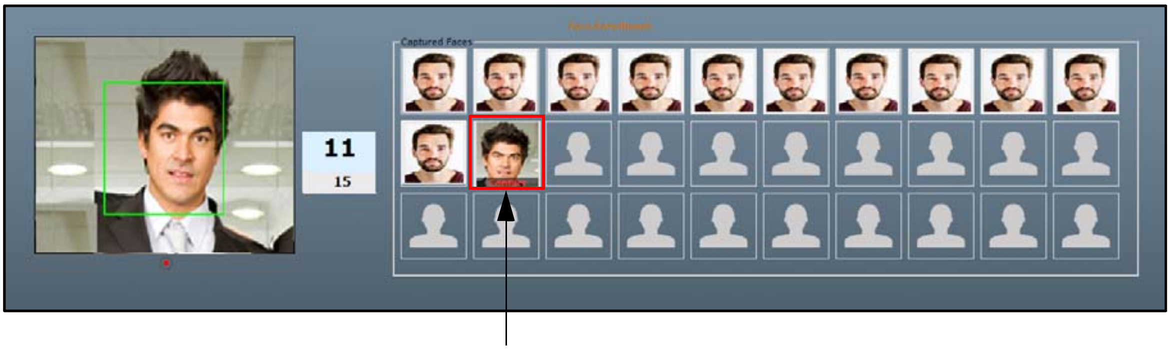
2. **Face is not Visible:** During enrollment, if a visitor's face is not visible within the camera range, then the screen displays the error as shown below:



3. **Keep Face Straight**: If the visitor's face is not within the face frame, the screen will display an error as shown below:

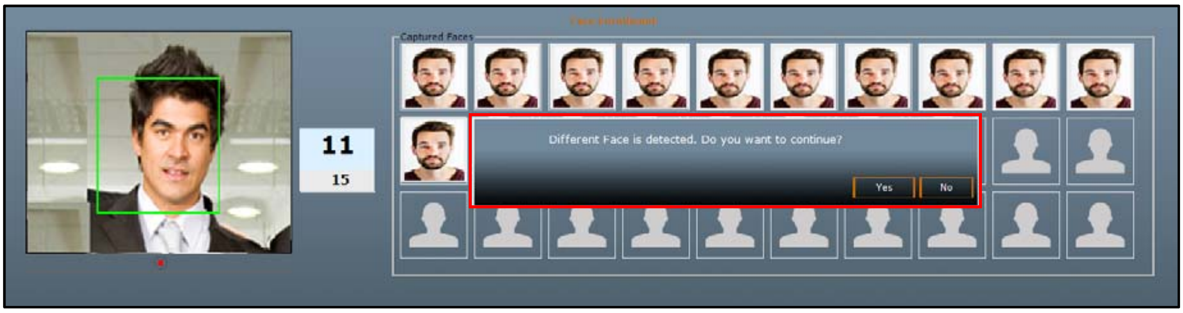


4. **Conflict Checking:** When any conflict is detected with other user/visitor during the enrollment process, below shown image will be displayed, and such images will not be counted for the final enrollment.



Conflict Face

5. **Different Face Detected:** While enrolling, if a different person's face is detected or the existing visitor wears/removes spectacles and/or mask, a dialogue box will be displayed as shown below.



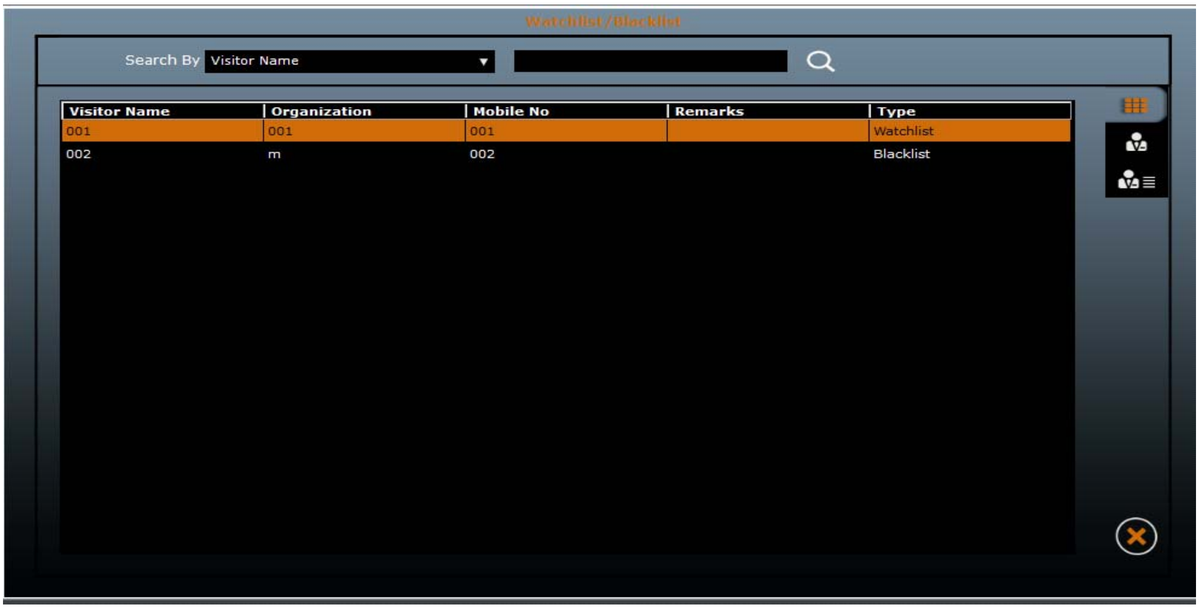
Different Face is detected. Do you want to continue?

If the face detected is of the same visitor, then click **Yes** to continue with the enrollment process and if not, click **No** and end the enrollment process.

Watchlist/Blacklist

The COSEC VMS application enables the user to maintain a watchlist of suspicious visitors or blacklist visitors. The application enables the operator to deny entry to such visitors. The operator can also choose to allow the visitor entry to the premises, based on the host's response.

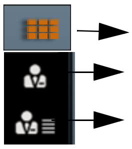
The COSEC VMS enables the user to add a visitor to the watchlist or blacklist either from the Frequent Visitors window or at the time of pass surrender. On clicking the **Watchlist/Blacklist** option the following window appears.



Visitor Name	Organization	Mobile No	Remarks	Type
001	001	001		Watchlist
002	m	002		Blacklist

The visitor can be added to watchlist or blacklist from *"Frequent Visitors"* list or through the *"Surrender Pass"* option.

The Visitors can also be viewed by selecting the option photo view or the photo view with details.

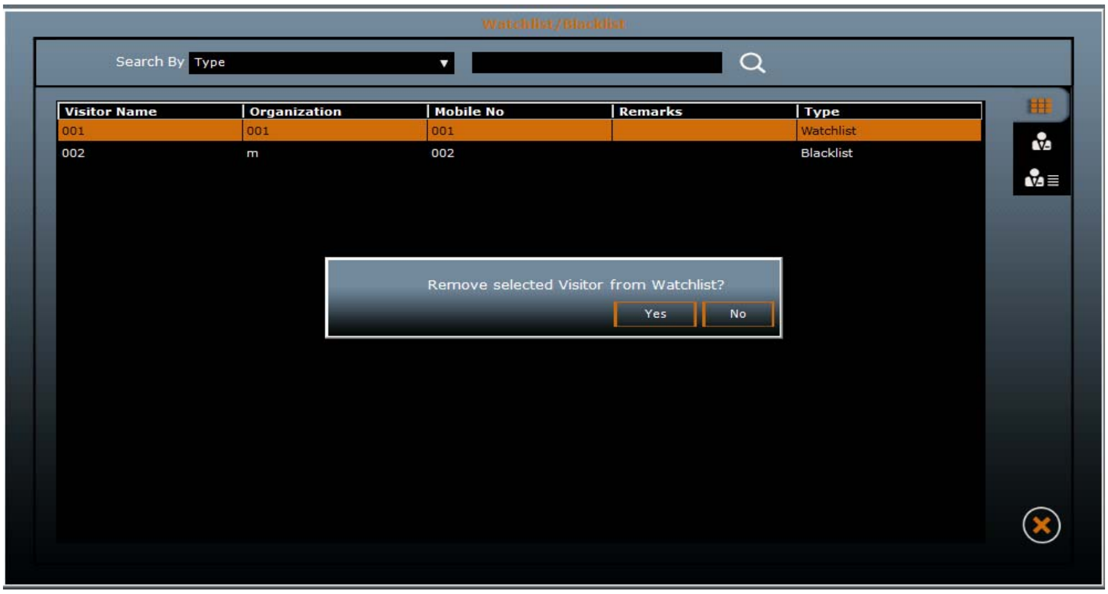


Detail view.

Photo view.

Photo and Detail view

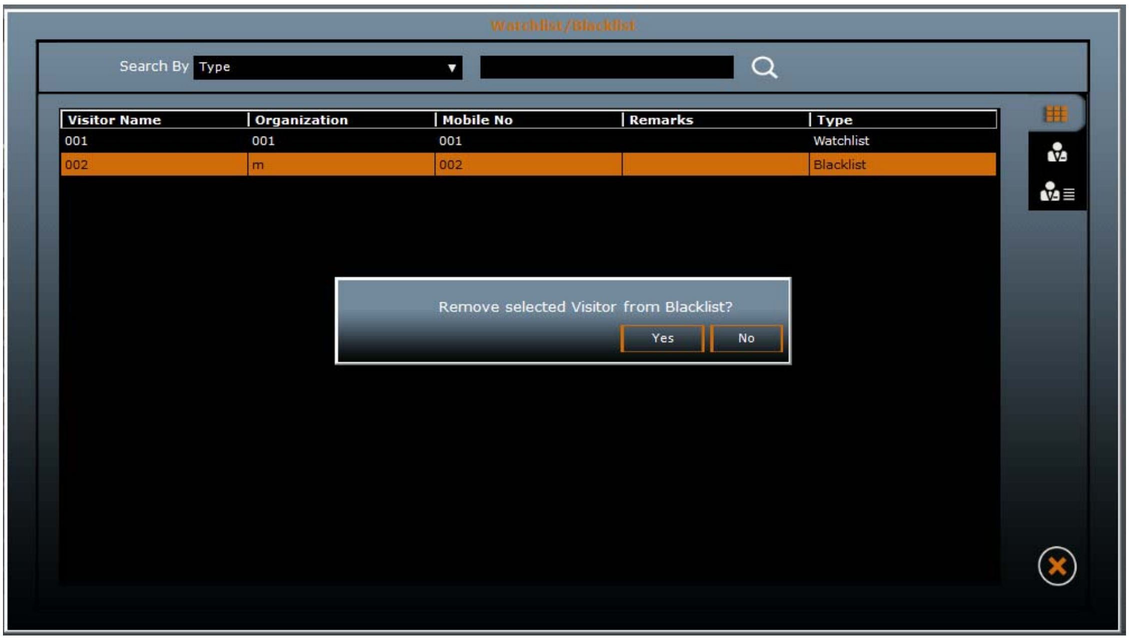
In order to remove a visitor from Blacklist or Watchlist, select the visitor and a pop up appears for removing the visitor.



Search By Type

Visitor Name	Organization	Mobile No	Remarks	Type
001	001	001		Watchlist
002	m	002		Blacklist

Remove selected Visitor from Watchlist?



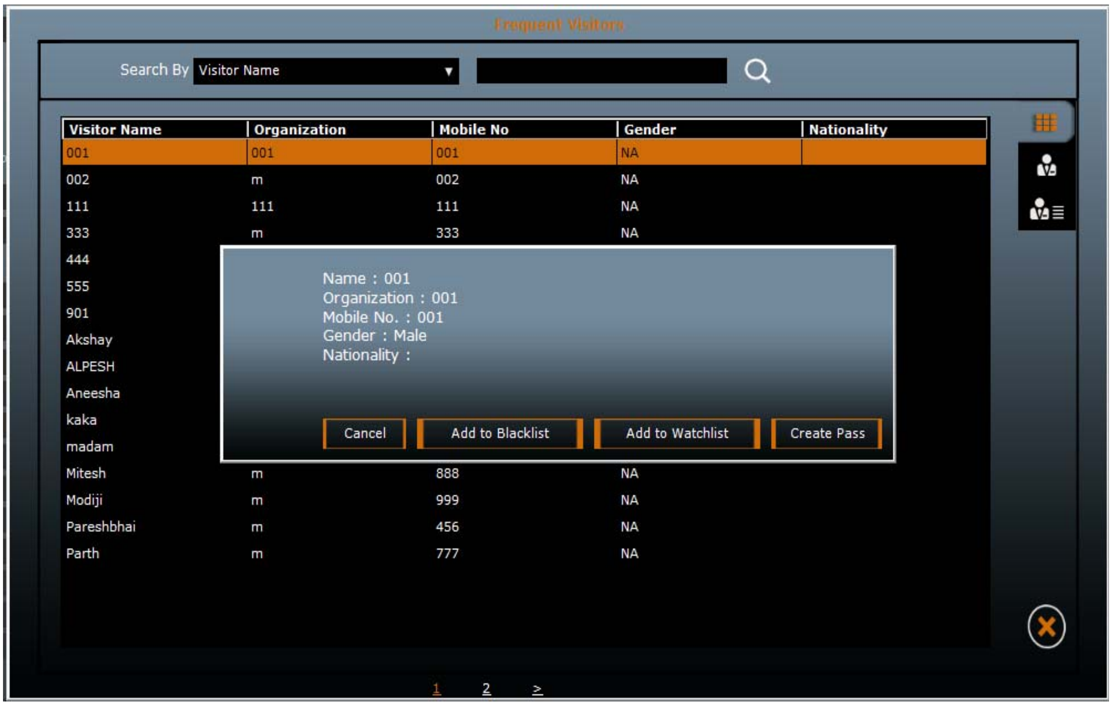
Search By Type

Visitor Name	Organization	Mobile No	Remarks	Type
001	001	001		Watchlist
002	m	002		Blacklist

Remove selected Visitor from Blacklist?

Frequent Visitors

The list of frequent visitors can be viewed by selecting Frequent Visitors section.



Frequent Visitors

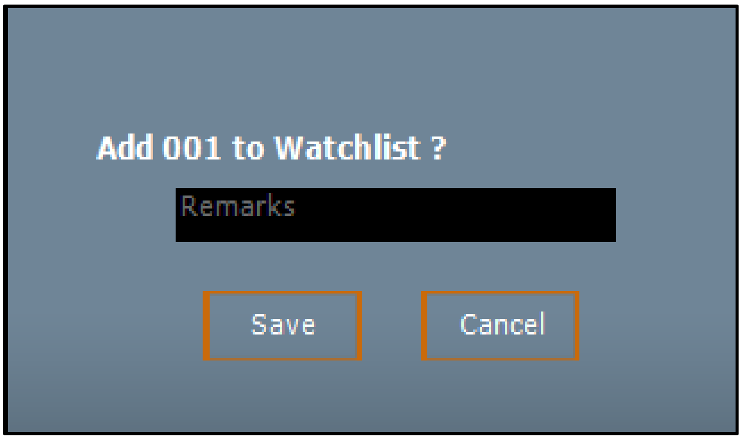
Search By: Visitor Name

Visitor Name	Organization	Mobile No	Gender	Nationality
001	001	001	NA	
002	m	002	NA	
111	111	111	NA	
333	m	333	NA	
444				
555				
901				
Akshay				
ALPESH				
Aneesha				
kaka				
madam				
Mitesh	m	888	NA	
Modiji	m	999	NA	
Pareshbhai	m	456	NA	
Parth	m	777	NA	

Name : 001
Organization : 001
Mobile No. : 001
Gender : Male
Nationality :

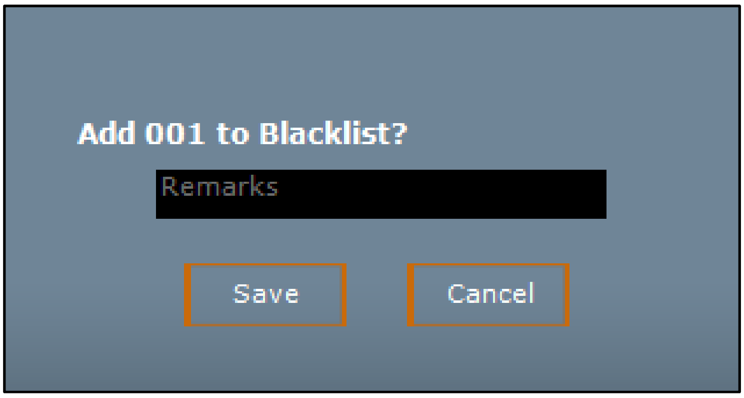
On selecting the visitor from the Frequent Visitors window, the system allows the user to either add the visitor to the Watchlist, Blacklist or generate a Visitor pass. Select the appropriate option by clicking on the relevant button.

- Click **Add to Watchlist** if you desire to add the visitor to **Watchlist.** You may also enter a remark before saving the visitor to watchlist. For more information, refer *"Watchlist/Blacklist"*. This option is also available from the Surrender Pass window.



Add 001 to Watchlist ?

- Click **Add to Blacklist** if you desire to add the visitor to **Blacklist.** You may also enter a remark before saving the visitor to blacklist. For more information, refer *"Watchlist/Blacklist"*. This option is also available from the Surrender Pass window.

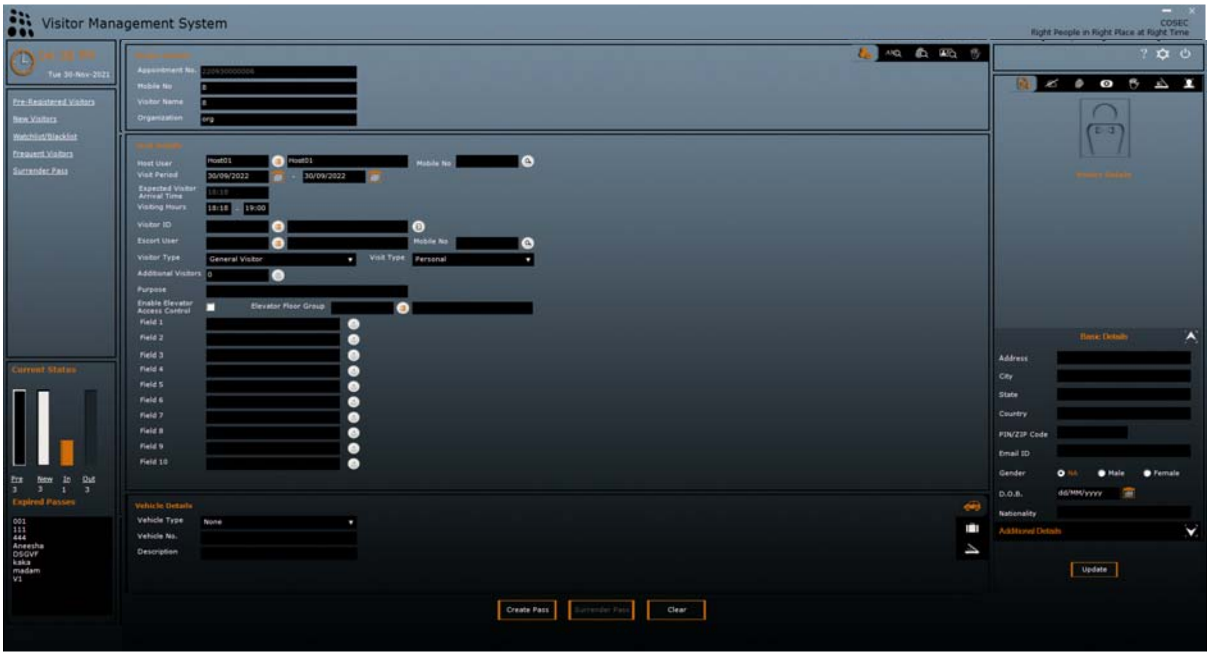


Add 001 to Blacklist?

Remarks

- Click on **Create Pass.** The home page with Visitor details (Basic and Additional) will be displayed.

- For creating pass, you must select a Visitor ID, Host user and Vehicle number. Once the pass is created, Current Status will be updated for **New** and **In**.



Visitor Management System

Tue 30-Nov-2021

Appointment No. 220930000006
Mobile No 8
Visitor Name 8
Organization org

Host User Host01 Host01
Mobile No
Visit Period 30/09/2022 - 30/09/2022
Expected Visitor Arrival Time 18:18
Visiting Hours 18:18 - 19:00
Visitor ID
Escort User
Mobile No
Visitor Type General Visitor
Visit Type Personal
Additional Visitors 0
Purpose
Enable Elevator Access Control □
Elevator Floor Group
Field 1
Field 2
Field 3
Field 4
Field 5
Field 6
Field 7
Field 8
Field 9
Field 10

Vehicle Details
Vehicle Type None
Vehicle No.
Description

Current Status
Pre 3
New 3
In 1
Out 3

Expired Passes
001
111
444
Aneesha
DSGVF
kaka
madam
V1

Basic Details
Address
City
State
Country
PIN/ZIP Code
Email ID
Gender ○ NA ● Male ● Female
D.O.B. dd/MM/yyyy
Nationality
Additional Details

The Frequent visitors can also be viewed by selecting the option photo view or the photo view with details.

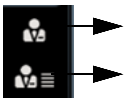
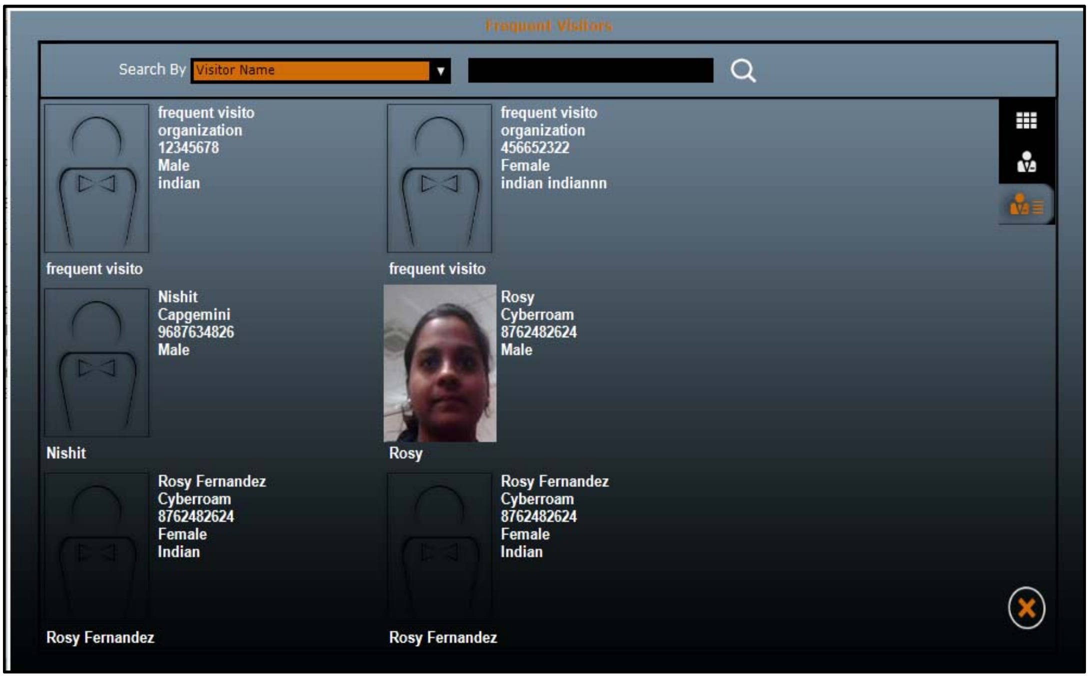


Photo View

Photo with Details



Frequent Visitors

Search By Visitor Name

frequent visito
organization
12345678
Male
indian

frequent visito

frequent visito
organization
456652322
Female
indian indiannn

frequent visito

Nishit
Capgemini
9687634826
Male

Nishit

Rosy
Cyberroam
8762482624
Male

Rosy

Rosy Fernandez
Cyberroam
8762482624
Female
Indian

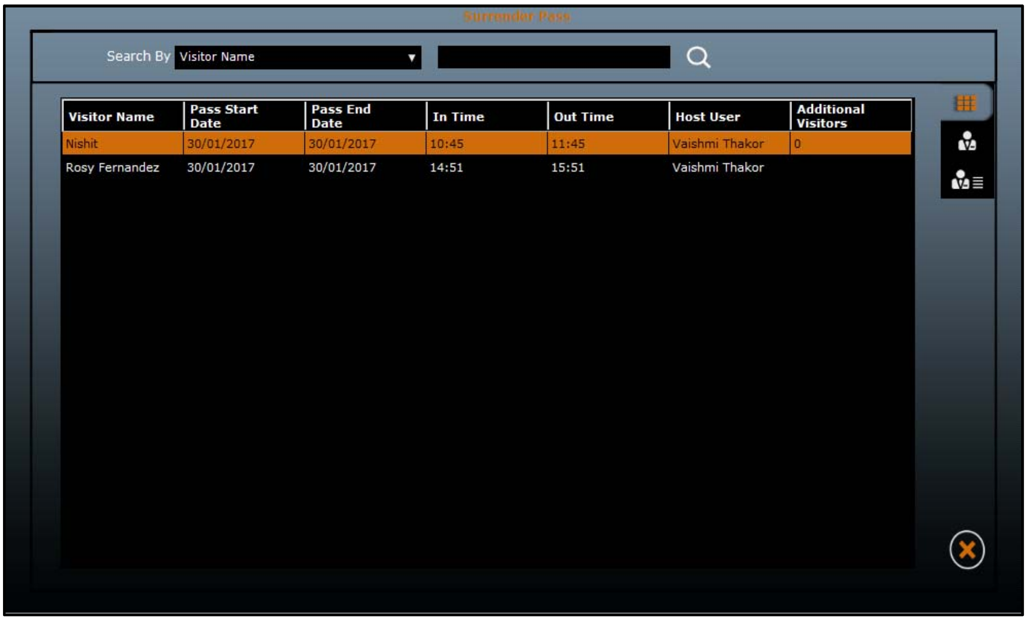
Rosy Fernandez

Rosy Fernandez
Cyberroam
8762482624
Female
Indian

Rosy Fernandez

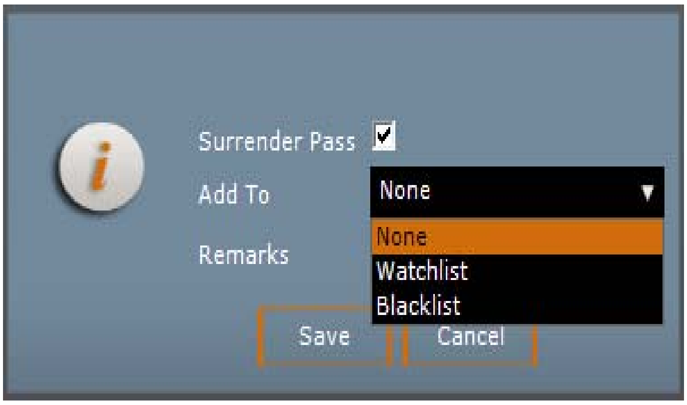
Surrender Pass

This option enables the operator to manually sign out the visitor. The visitor must sign out on leaving the premises. To sign out the visitor, the visitor needs to surrender the visitor pass or the ePass at the VMS station. Click on the Surrender Pass option. The following page shows the list of visitors who are yet to surrender their passes.



Visitor Name	Pass Start Date	Pass End Date	In Time	Out Time	Host User	Additional Visitors
Nishit	30/01/2017	30/01/2017	10:45	11:45	Vaishmi Thakor	0
Rosy Fernandez	30/01/2017	30/01/2017	14:51	15:51	Vaishmi Thakor	

- Select the Visitor from the grid whose pass is to be surrendered. The home page with visitor details will appear.
- Click the **Surrender Pass** option. The following pop-up appears.



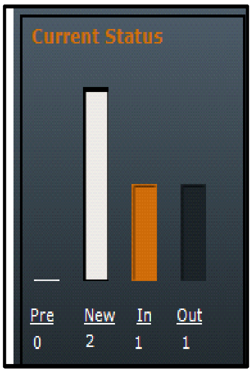
Surrender Pass ☑

Add To: None

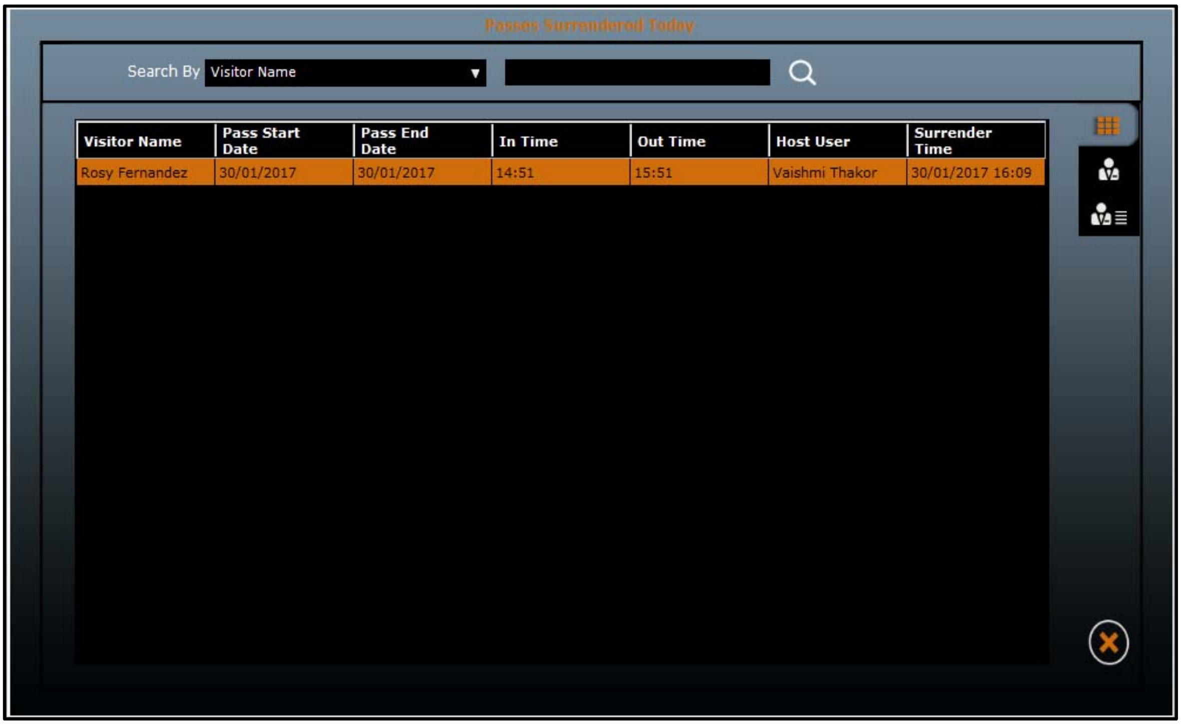
Remarks

- Enable the **Surrender Pass** checkbox in order to surrender the visitor pass.
- If you desire you may also add the visitor to Watchlist or Blacklist.To do so, select the desired option from the dropdown list under **Add To.**
- Enter appropriate **Remarks** if you desire.

In the event of adding the visitor to the watchlist, specify a reason for adding the visitor to the watchlist and click on the **Save** button. Once the pass is surrendered, Current Status will be updated for **Out** event.



Click on **Out**. The Passes surrendered today will be shown as below.

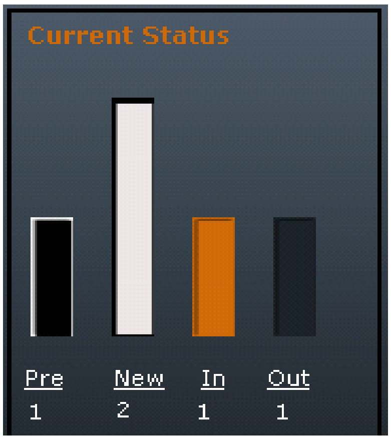

Passes Surrendered Today

Search By Visitor Name

Visitor Name	Pass Start Date	Pass End Date	In Time	Out Time	Host User	Surrender Time
Rosy Fernandez	30/01/2017	30/01/2017	14:51	15:51	Vaishmi Thakor	30/01/2017 16:09

Current Status

The Current Status section enables the user to view the daily status of the visitor transactions.

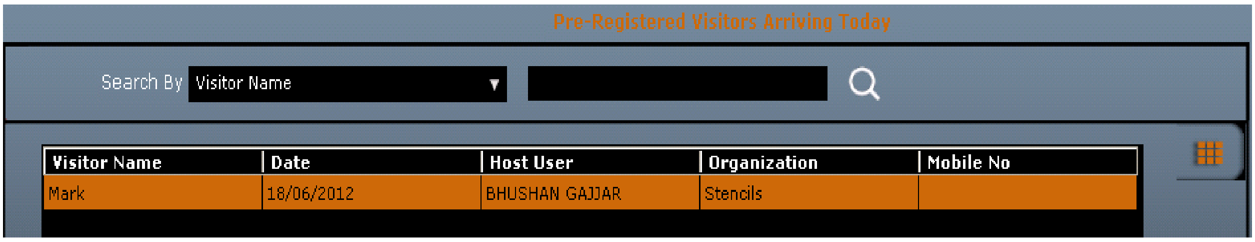


Current Status

Pre	New	In	Out
1	2	1	1

The operator can click on the following links as shown in the above figure.

Pre: Enables the operator to view the list of pre-registered visitors expected for that day as shown.

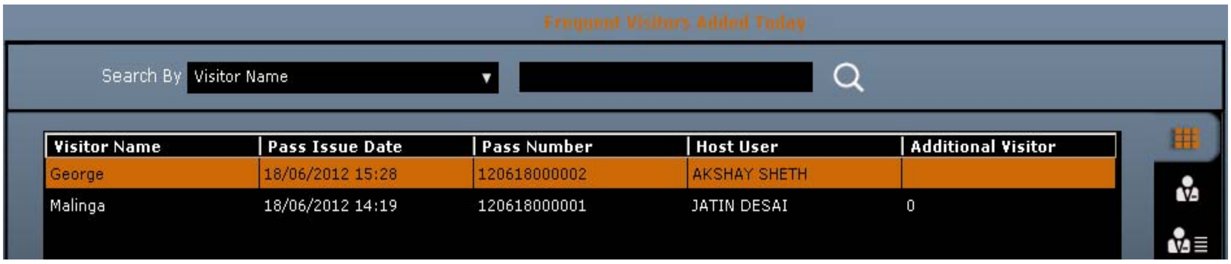


Pre-Registered Visitors Arriving Today

Search By Visitor Name ▼

Visitor Name	Date	Host User	Organization	Mobile No
Mark	18/06/2012	BHUSHAN GAJJAR	Stencils	

New: The window displays the list of new visitors defined on that day.

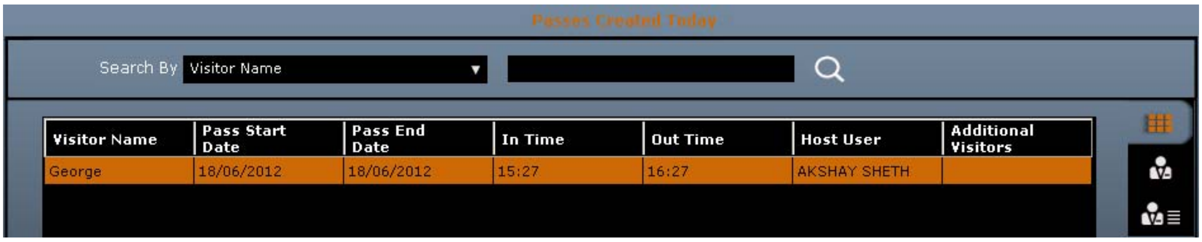


Frequent Visitors Added Today

Search By Visitor Name ▼

Visitor Name	Pass Issue Date	Pass Number	Host User	Additional Visitor
George	18/06/2012 15:28	120618000002	AKSHAY SHETH	
Malinga	18/06/2012 14:19	120618000001	JATIN DESAI	0

In: Displays the details of the visitor passes activated for that day which are not yet surrendered. The IN count will be shown till the Visit End date or till the pass is surrendered. Suppose the pass is created and visit is repeated daily for a month so it will be shown in IN count for that month.

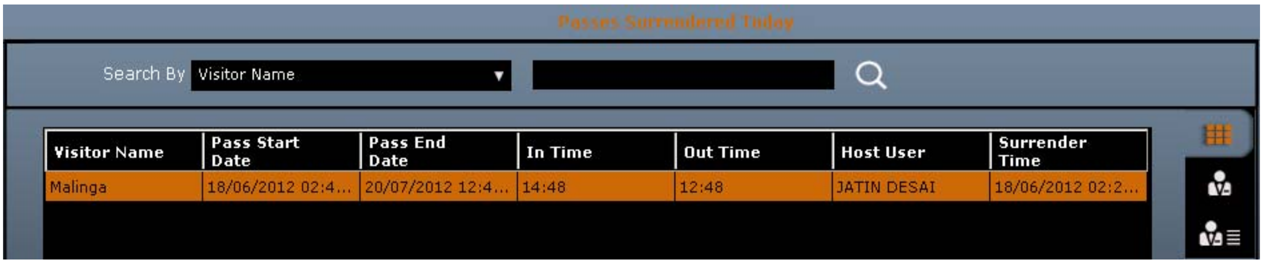


Passes Created Today

Search By Visitor Name ▼

Visitor Name	Pass Start Date	Pass End Date	In Time	Out Time	Host User	Additional Visitors
George	18/06/2012	18/06/2012	15:27	16:27	AKSHAY SHETH	

Out : Displays the list of surrendered passes on that day.



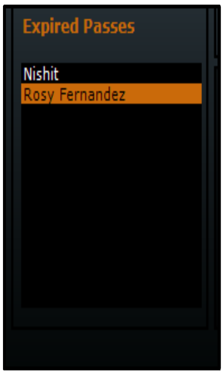
Passes Surrendered Today

Search By: Visitor Name

Visitor Name	Pass Start Date	Pass End Date	In Time	Out Time	Host User	Surrender Time
Malinga	18/06/2012 02:4...	20/07/2012 12:4...	14:48	12:48	JATIN DESAI	18/06/2012 02:2...

Expired Passes

This section displays the visitors whose visit hours have expired but the visitor passes have not been surrendered for some reason or the other.



Expired Passes

Nishit
Rosy Fernandez

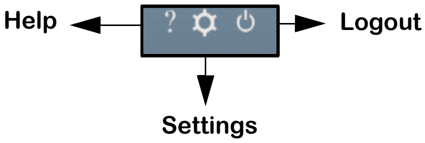
The operator can select the visitor form the list and click on the **Surrender Pass** button as and when required. The visitor can also be added to watchlist or blacklist if required, as explained earlier.

VMS Settings

VMS Toolbar

The COSEC VMS toolbar enables the user to access the following functionalities as shown.

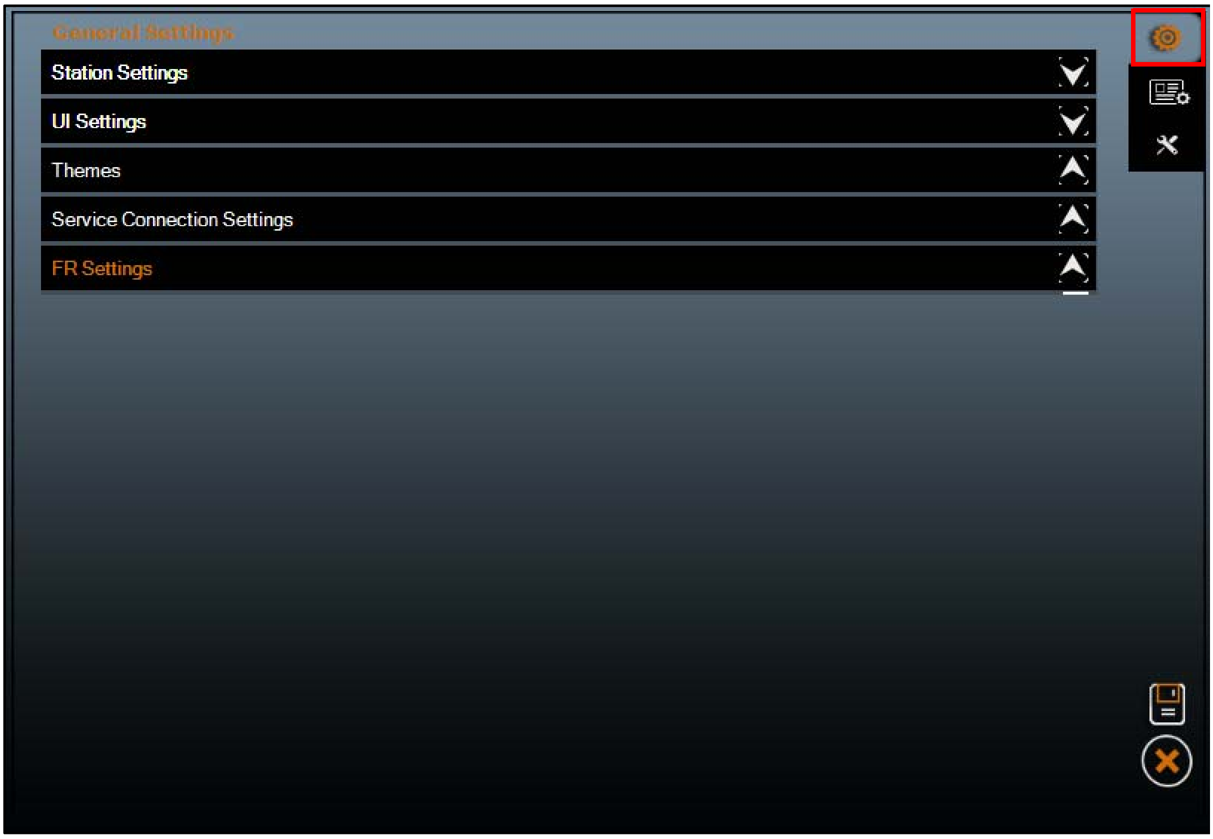
- Help file
- Settings
- Logout



Click on **Help** icon to access the VMS help file.

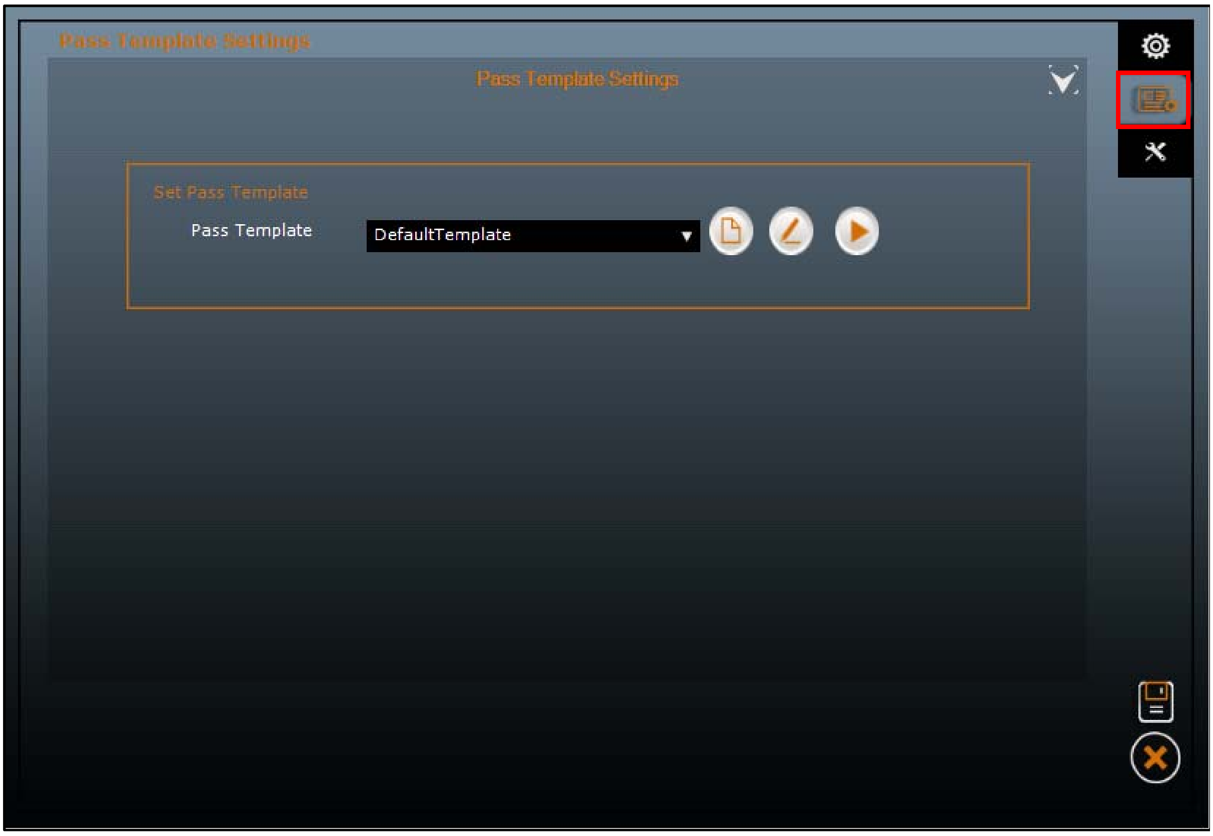
Click on **Logout** icon to log out of the VMS application.

The **Settings** option enables the user to configure the following parameters.



- **General Settings**, for more information, refer *"General Settings".*
    - Station Settings
    - UI Settings
    - Themes
    - Service Connection Settings
    - FR Settings

- **Pass Template Settings**, for more information, refer *"Visitor Pass Template".*



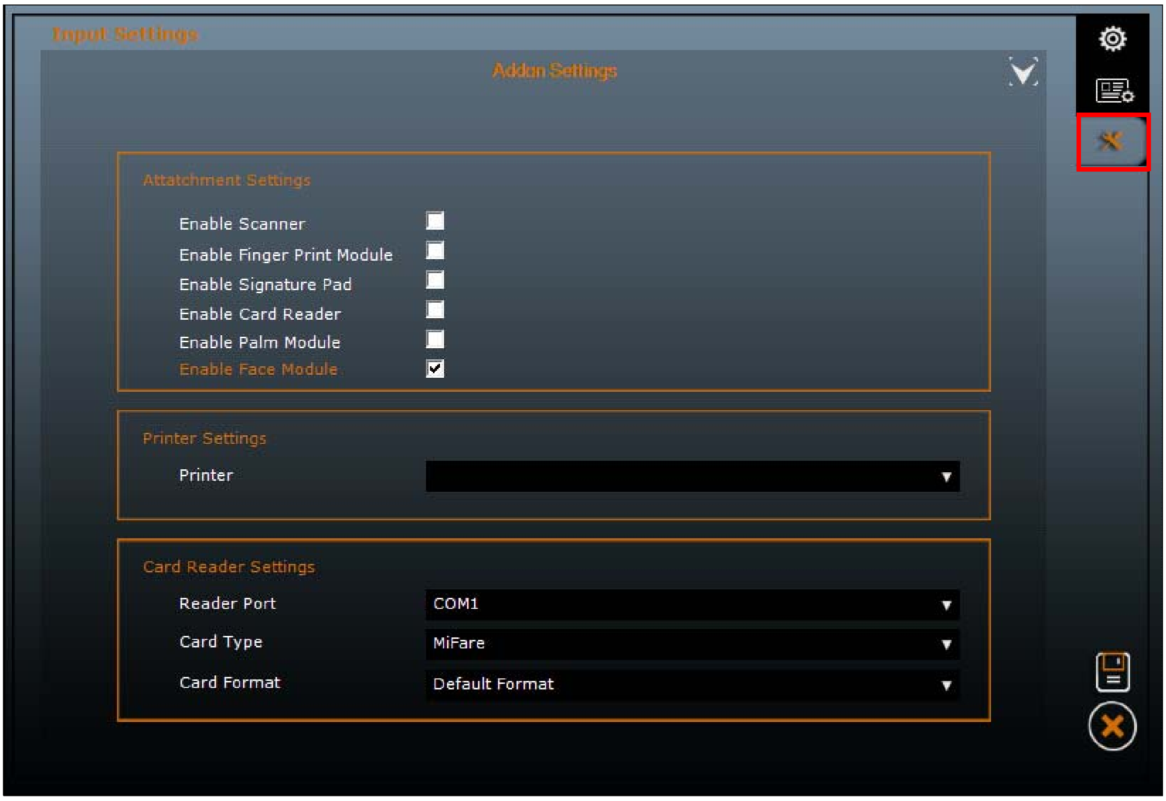
Pass Template Settings

Pass Template Settings

Set Pass Template

Pass Template: DefaultTemplate ▾

- **Input Settings**, for more information, refer *"Input Settings".*



Input Settings

Addon Settings

Attachment Settings

Enable Scanner	□
Enable Finger Print Module	□
Enable Signature Pad	□
Enable Card Reader	□
Enable Palm Module	□
Enable Face Module	☑

Printer Settings

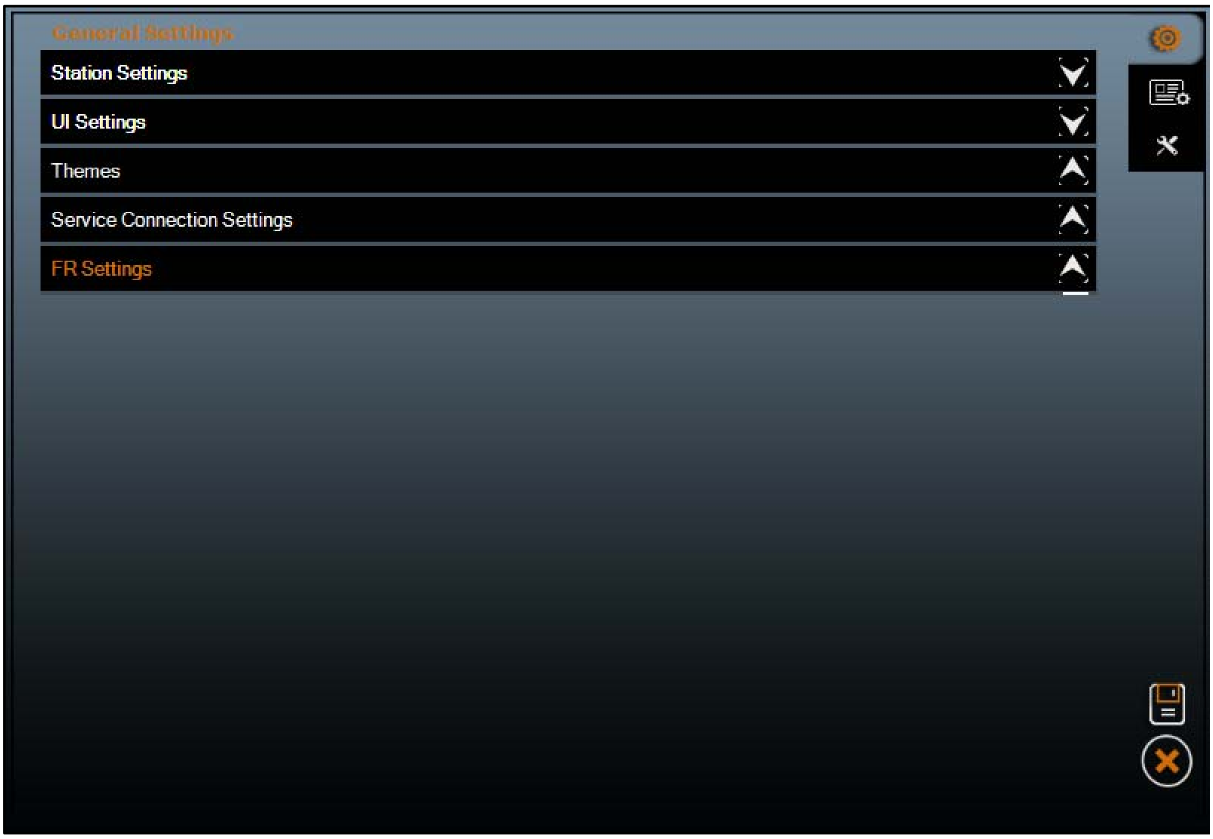
Printer: ▾

Card Reader Settings

Reader Port	COM1 ▾
Card Type	MiFare ▾
Card Format	Default Format ▾

General Settings

Click on the **Settings** ⚙ icon. The following window appears.

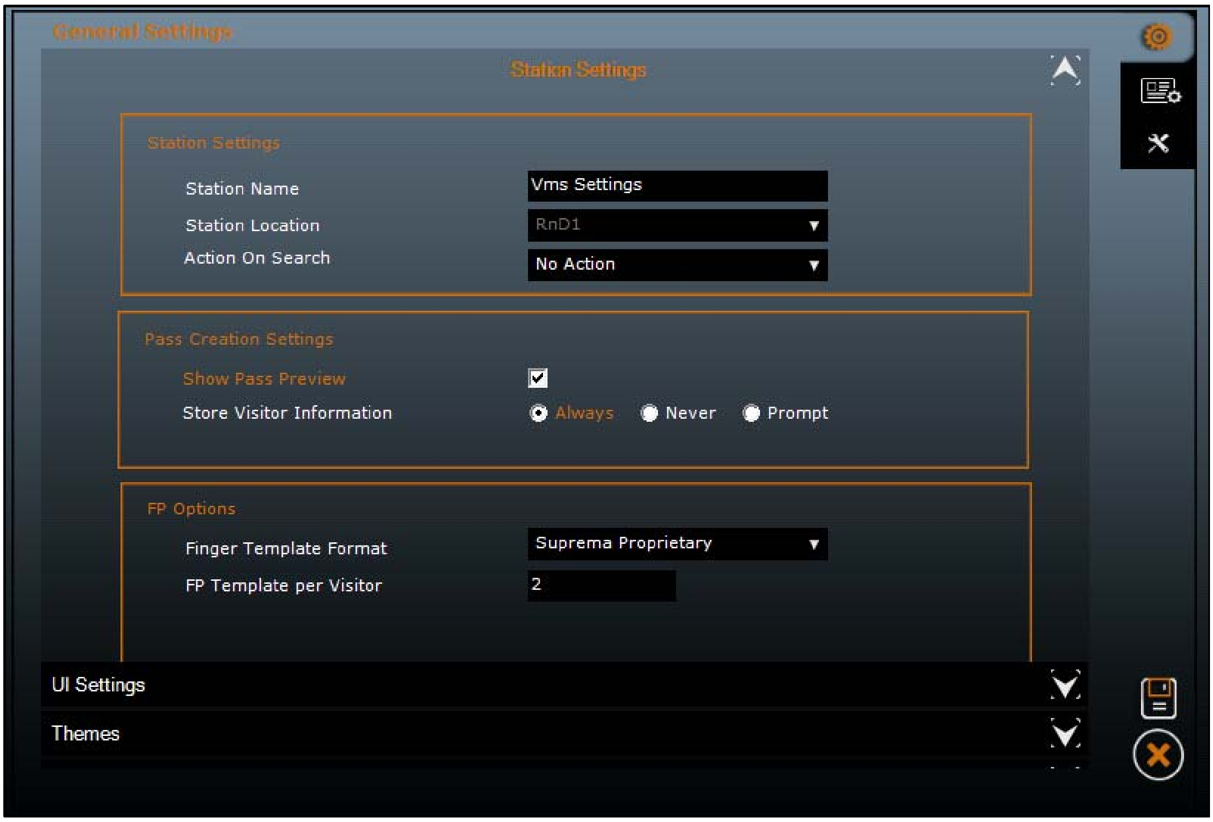


You can configure the following Settings:

- *“Station Settings”*
- *“UI settings”*
- *“Themes”*
- *“Service Connection Settings”*
- *“FR Settings”*

Station Settings

The **Station Settings** page enables the user to configure the following Station parameters.



General Settings

Station Settings

Station Settings

Station Name: Vms Settings

Station Location: RnD1 ▼

Action On Search: No Action ▼

Pass Creation Settings

Show Pass Preview ☑

Store Visitor Information ● Always ○ Never ○ Prompt

FP Options

Finger Template Format: Suprema Proprietary ▼

FP Template per Visitor: 2

UI Settings

Themes

Station Settings

- **Station Name**: Specify a user friendly station name for the VMS station.
- **Station Location**: Select the VMS station location from the drop down list. The list appears as per the stations defined from the COSEC Web application.
- **Action On Search:** Select the action from the drop down list as No Action, Surrender Pass or Reprint Pass.

  The security at exit gate of any premises will scan the QR code on pass. If the QR code contains Appointment number and when respective appointment number match is found; the default action which is set in Station Settings will be performed.

Pass Creation Settings

- **Show Pass Preview**: Check this box to enable pass preview mode.
- **Store Visitor Information**: This option enables the user to configure whether the registered visitor information is to be stored in the frequent visitor list. Select the appropriate option as per the site requirements.

The entry of Visitor details & visit details will be done only if the option “Always” is selected and If “Prompt” is selected then in Add to Frequent Visitor Popup > 'YES' must be selected.

FP Options

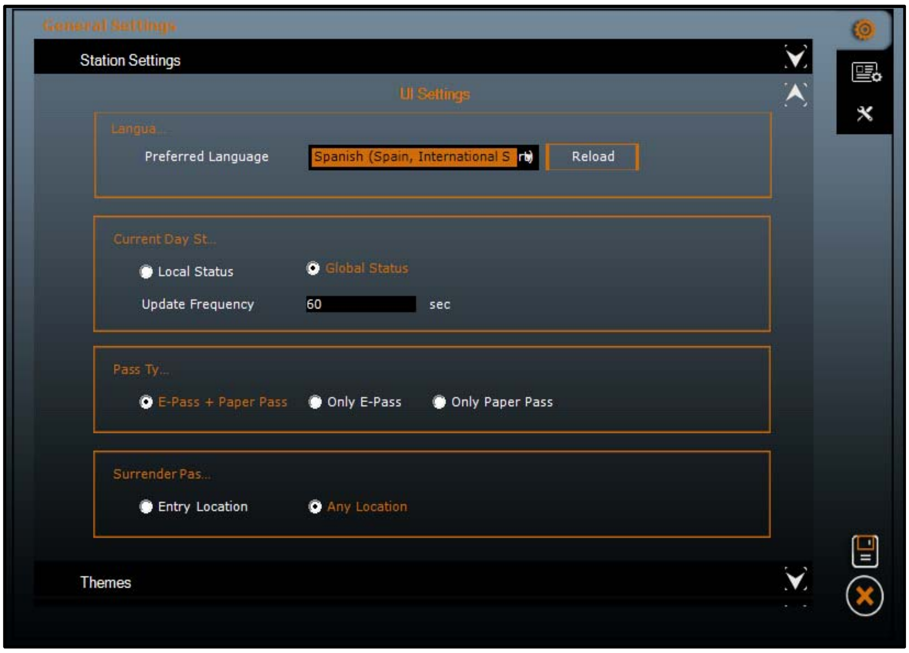
- **Finger Template Format:** Select the format in which the finger templates of the visitor are to be stored. Lumidigm ISO & Lumidigm Proprietary format must be set for Door FMX.

- **FP Template per Visitor**: User can set the maximum number of fingerprint templates that can be stored per visitor. The maximum number is 2.

- **Transfer Visitor FP to Devices**: The system can transfer the enrolled fingerprints of visitor to the assigned devices. Check this box to enable this functionality.

UI settings

The **UI settings** page enables the user to configure the following parameters as shown.



Langua...

Preferred Language: Spanish (Spain, International S Reload

Current Day St...

○ Local Status ● Global Status

Update Frequency: 60 sec

Pass Ty...

● E-Pass + Paper Pass ○ Only E-Pass ○ Only Paper Pass

Surrender Pas...

○ Entry Location ● Any Location

- **Language:** The preferred language as selected from COSEC Web is displayed here. You can select another language of your choice.

  On clicking the Reload button; a request for selected language from Preferred Language dropdown will be sent to Master Service.

- **Current Day Status**: This option enables the user to configure the following parameters of the **Current Status** section.

  - Display the local VMS station status or the global status in the event of having multiple VMS stations. Select the appropriate option as per the site requirements.

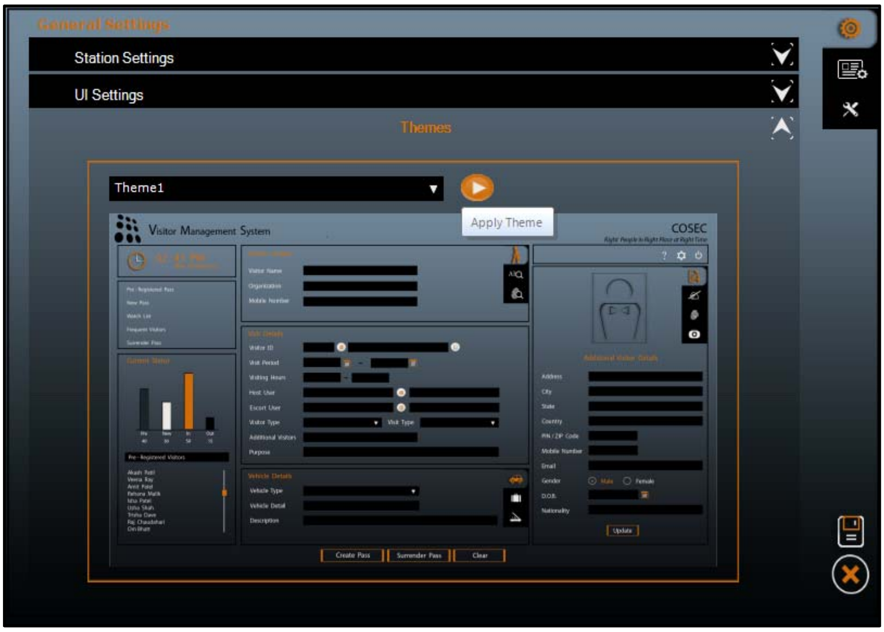
  - The frequency at which the current status is to be updated can be specified here. The maximum value is 999 seconds.

- **Pass Type**: Select the type of pass to be issued to the visitor as per the site requirements.

- **Surrender Pass @**: This parameter enables the user to configure whether the visitor passes are to be surrendered at the entry location or at any of the VMS stations.

Themes

The COSEC VMS application enables the user to set the theme for the VMS station as per the user preferences. Select the theme from the drop down list and click on the **Apply Theme** button as shown.

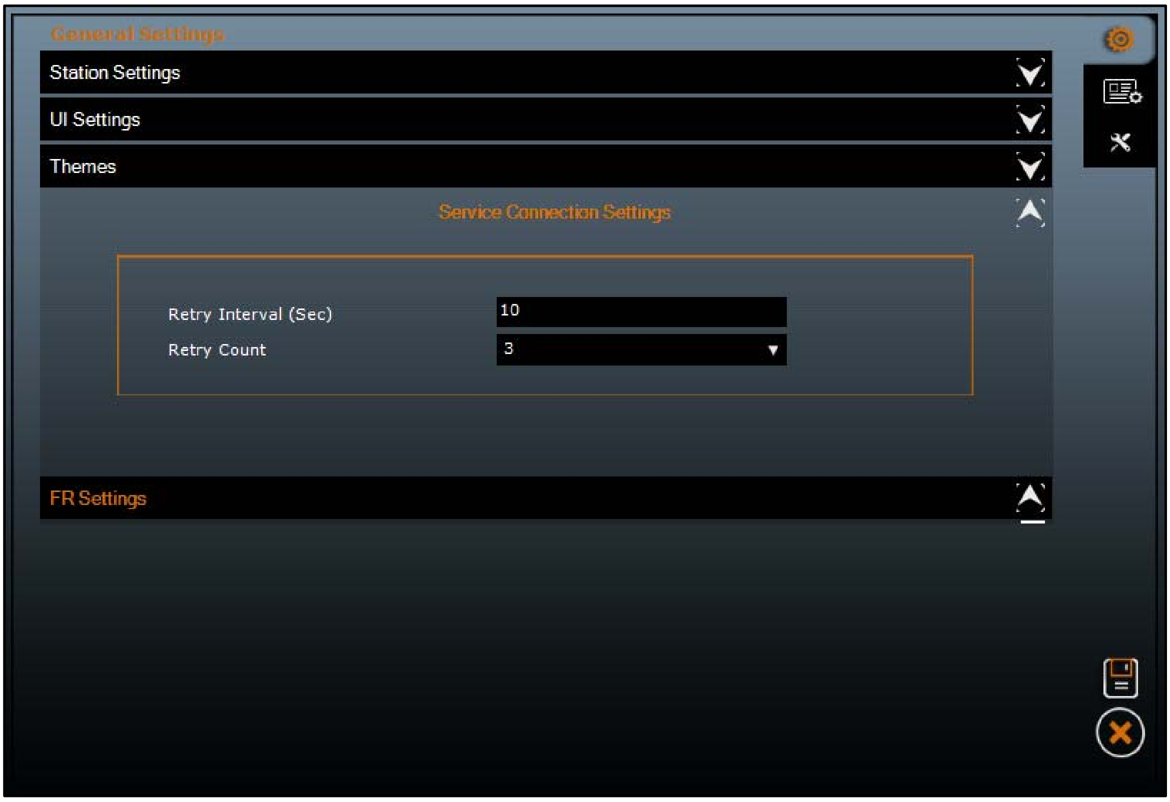


Service Connection Settings

When VMS Service or Tenant's Database connection is not available with the VMS Utility, then system will retry to connect with the VMS service or the database again.

- **Retry Interval (sec):** Enter the duration in seconds for which the retry for the connection will be done.

- **Retry Count:** Enter the number of counts for which the retry for the connection will be done.

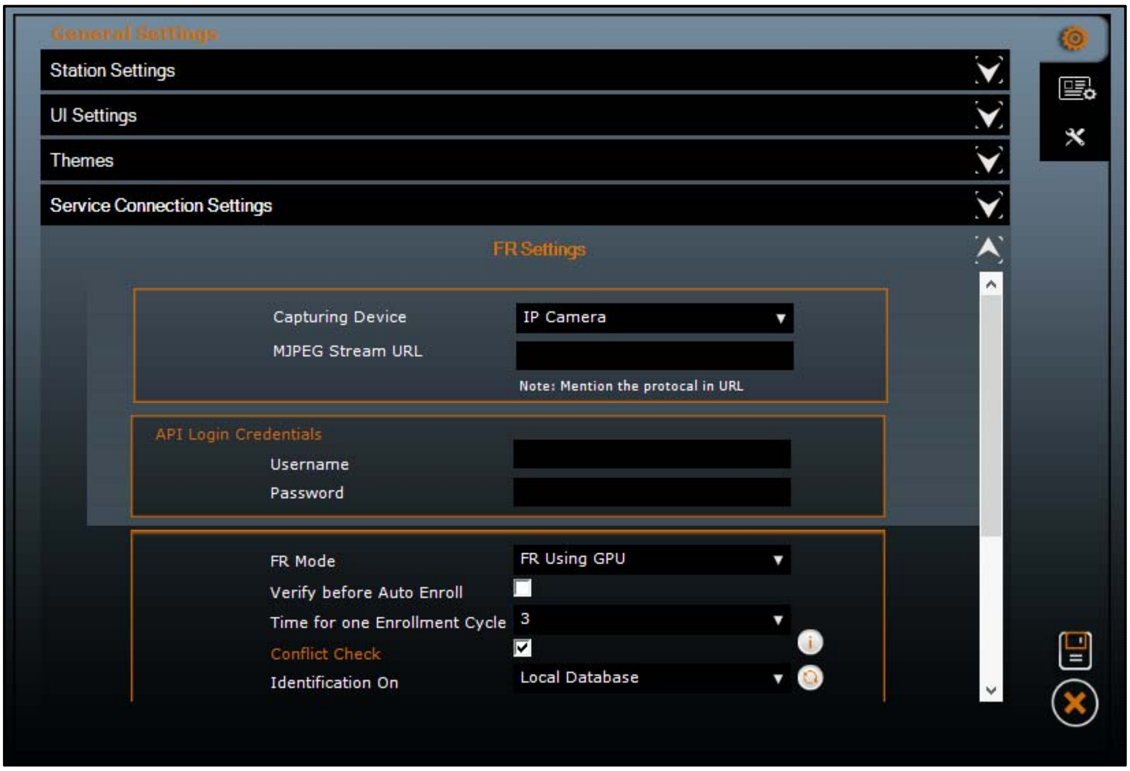


Retry Interval (Sec) 10

Retry Count 3

FR Settings

Configure the following parameters of FR Settings to perform Face Enrollment of a Visitor.



Capturing Device: IP Camera

MJPEG Stream URL:

Note: Mention the protocal in URL

API Login Credentials

Username:

Password:

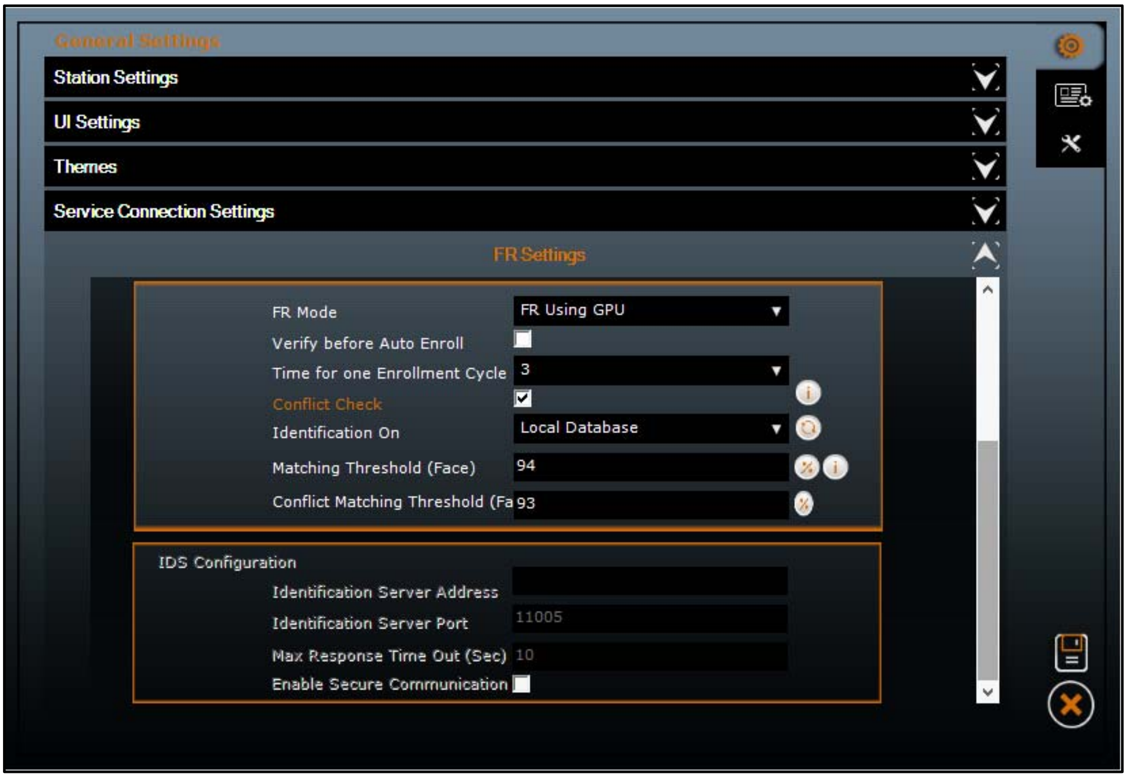
FR Mode: FR Using GPU

Verify before Auto Enroll: □

Time for one Enrollment Cycle: 3

Conflict Check: ☑

Identification On: Local Database



FR Mode: FR Using GPU

Verify before Auto Enroll: □

Time for one Enrollment Cycle: 3

Conflict Check: ☑

Identification On: Local Database

Matching Threshold (Face): 94

Conflict Matching Threshold (Fa: 93

IDS Configuration

Identification Server Address:

Identification Server Port: 11005

Max Response Time Out (Sec): 10

Enable Secure Communication: □

- **Capture Device:** Select the desired face capturing device — IP Camera or USB Camera.
- **MJPEG Stream URL:** Enter the MJPEG Stream URL.

API Login Credential

  - Enter the **Username** and **Password** to access the API.

- **FR Mode:** Select a desired FR Mode — FR Using GPU or FR Without Using GPU.

- **Verify Before Auto Enroll:** Select this checkbox to conduct a verification step before the Auto Enrollment process of a visitor’s face.

  You will be able to select the desired face images from the list of captured images which will be enrolled against the respective visitor.

  If disabled, then the system will automatically select the best captured face images and enroll them against the respective visitor while considering the values of matching score, conflict etc.

- **Time for one Enrollment Cycle:** Select the desired time to be taken by the system for one enrollment cycle.

  Example: Time for one Enrollment Cycle = 3 sec.

  When an enrollment process starts and a visitor’s face is detected properly, images of the visitor’s face will be captured for 3 sec.

  At the end of 3 sec, out of all the captured images, maximum 5 images can be selected for enrollment.

  Frames without faces or partial face or with low clarity etc. will be discarded.

- **Conflict Check:** Select this checkbox for the system to check if the captured visitor’s face image conflicts with already enrolled faces of all the users and visitors stored in the database of the system, during the enrollment of a new visitor’s face credential.

  Conflict checking can be carried out depending on the option selected in **Identification On**.

- **Identification On:** Select the desired option — Local Database or Identification Server — on which the Identification process of a visitor’s face will be conducted.

  - **Local Database** - This stores only the templates of local visitors and will be used for location-based visitor identification. This can be set up at the time of server configuration.

  - **Identification Server** (Global database) - This stores the templates of all COSEC users as well as the visitors and will be used at the time of face enrollment of all users/ visitors from an enrollment station.

  - If **Identification On** is set as Local Database;

    VMS Utility will save the face templates locally for identification. It syncs all the face templates automatically when the Utility starts.

    If you wish to sync the face templates manually, click the **Sync** 🔄 icon.

    It will start syncing the face templates and on completion of the process, a message mentioning successful sync process will be displayed.

    If not synced due to any reason, an error message will be displayed.

- If **Identification On** is set as Identification Server;

  Face Identification and Conflict Check requests will be sent to the IDS server configured in *"IDS Configuration"*.

  As Identification Server i.e. Global Database has all the templates of all COSEC users as well as visitors, an accurate identification of visitor's face will be achieved.

- **Matching Threshold:** Matching threshold is the point at which the system becomes reasonably certain that the visitor's face for identification matches with the visitor's already enrolled face available in its local database.

  A biometric match is never exact, hence you need to choose a measure of similarity i.e.**Matching Threshold** at which a match will be declared.

  So, if **Identification On** is set as Local Database, enter the **Matching Threshold** for visitor's Face Identification.

- **Conflict Matching Threshold:** To check if a visitor's face, during identification process, matches with any of the already enrolled users and visitors available in the system's database, enter **Conflict Matching Threshold.**

  To provide some deviation between the face templates of multiple users, Admin can configure **Conflict Matching Threshold** lower than **Matching Threshold**.

IDS Configuration

- **Identification Server Address:** Enter the IP Address of the system where the IDS is installed.

- **Identification Server Port:** Enter the Identification Server Port.

- **Max Response Time-Out (Sec):** Enter the Maximum Response Time-Out Duration. It is a timer for which the VMS Utility will wait for the response from IDS.

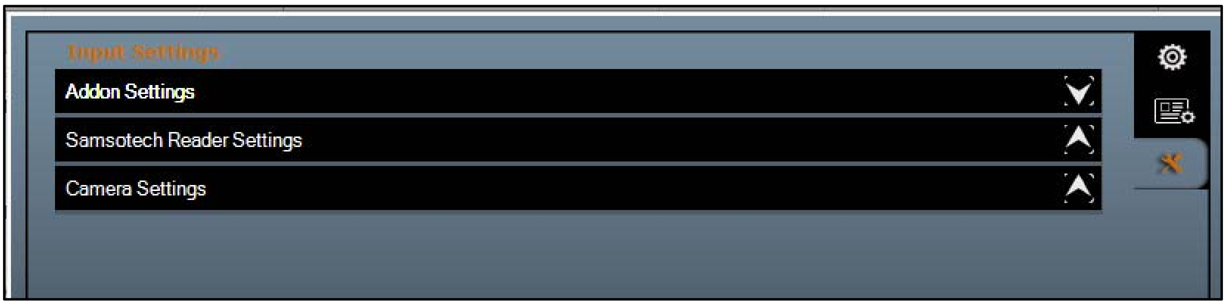
  IDS will identify the face template of the visitor and will give a response to the VMS Utility.

  If IDS fails to give a response to the VMS Utility within the specified time, a time-out error message will be displayed.

- **Enable Secure Communication:** Select this checkbox to enable secure communication between IDS and VMS Utility.

Input Settings

This option enables the user to define the connected devices which will be used by the VMS application. Click on the Input Settings icon as shown. The following page appears.



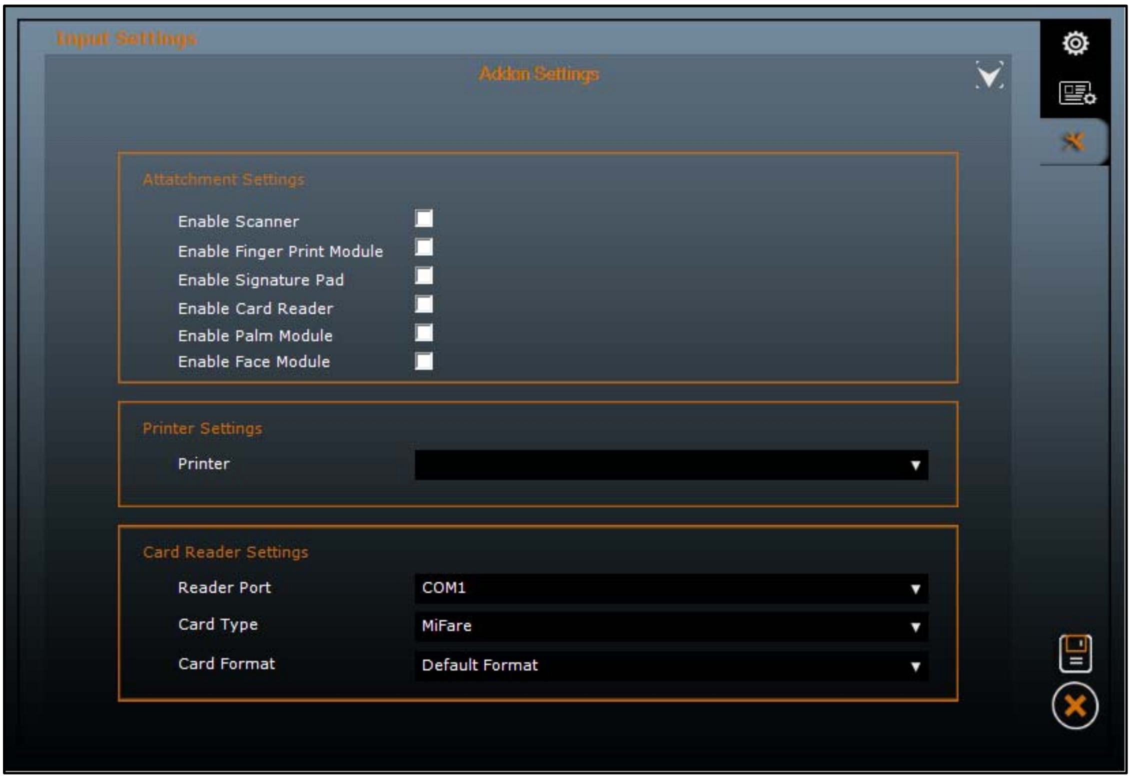
Input Settings

Addon Settings

Samsotech Reader Settings

Camera Settings

Addon Settings



Input Settings

Addon Settings

Attatchment Settings

Enable Scanner □
Enable Finger Print Module □
Enable Signature Pad □
Enable Card Reader □
Enable Palm Module □
Enable Face Module □

Printer Settings

Printer

Card Reader Settings

Reader Port: COM1
Card Type: MiFare
Card Format: Default Format

The COSEC VMS application can connect to the devices. Check the boxes against the installed devices to enable the COSEC VMS application to connect to the devices.

- Scanner

Scanner will be supported in VMS Utility through TWAIN compatible drivers in 32 bit computers and WIA compatible drivers in 64 bit computers.

- Fingerprint Module (Suprema Bio Mini)

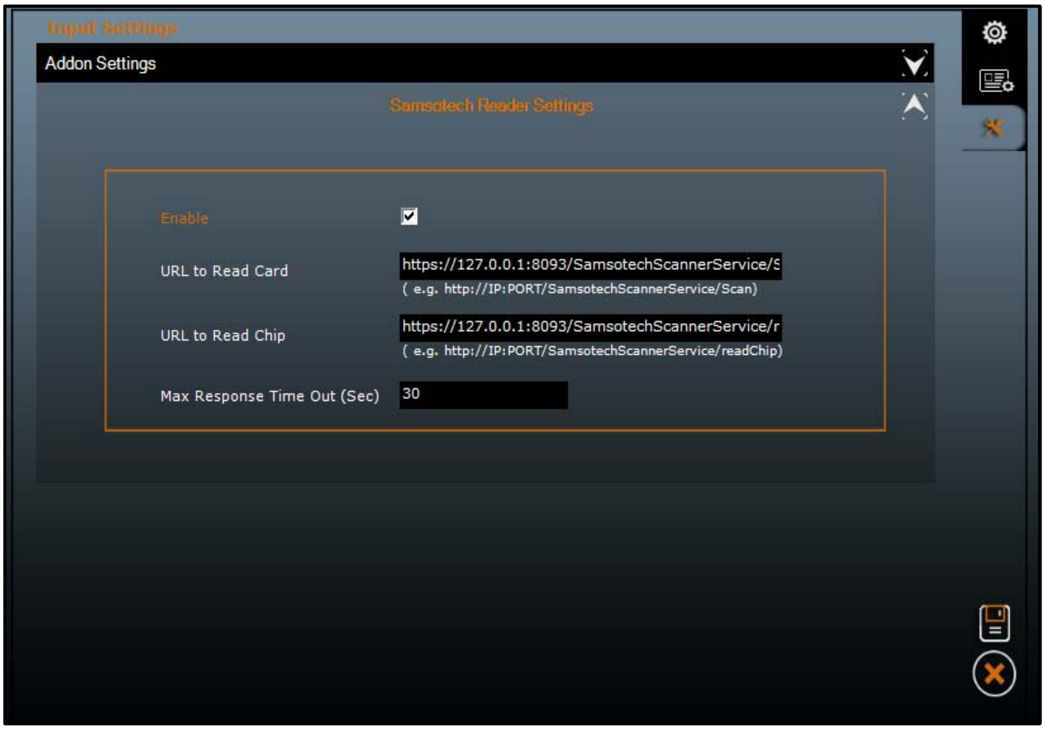
The support of Suprema Bio Mini Plus 2 is added in VMS Utility.
If at any point of time the operating 'FP Template Type' is changed then application (Utility/Web) must be restarted before enrollment.

- Signature Pad
- Card Reader
- Palm Module
- Face Module
- Printer - Select the appropriate model from the installed printers in the drop down list.

Then configure the Card reader settings as required.

Then click on the Save icon once the settings have been defined. The Save icon appears on the upper right corner of the settings window.

Samsotech Reader Settings



Enable ☑

URL to Read Card: https://127.0.0.1:8093/SamsotechScannerService/S
(e.g. http://IP:PORT/SamsotechScannerService/Scan)

URL to Read Chip: https://127.0.0.1:8093/SamsotechScannerService/r
(e.g. http://IP:PORT/SamsotechScannerService/readChip)

Max Response Time Out (Sec): 30

- **Enable**: Check this box to enable Samsotech Reader Settings.

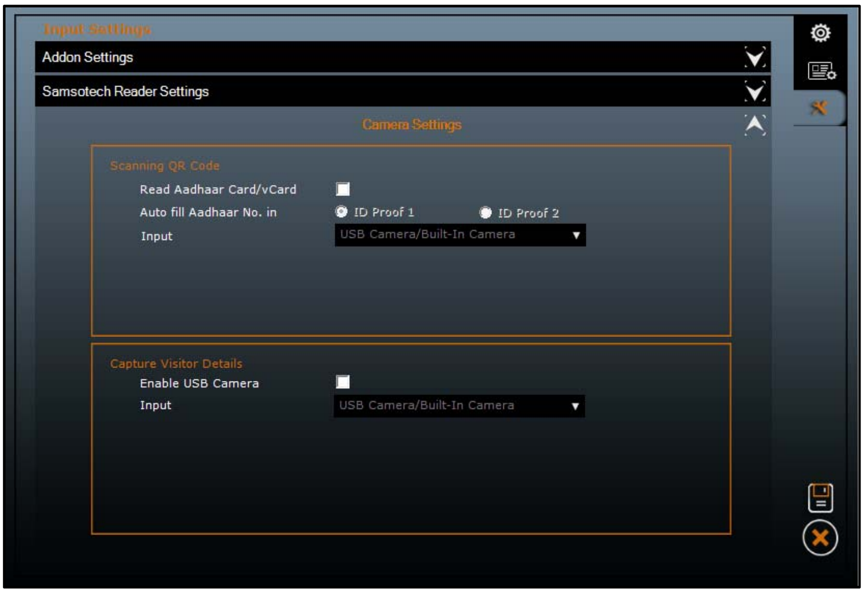
- **URL to Read Card:** Enter the URL to communicate with Samsotech scanning Device for reading Card. Eg: Aadhar Card do not have any chip so information can be read from the card.

- **URL to Read Chip:** Enter the URL to communicate with Samsotech scanning Device for reading chip. Eg : Driving License has chip from where the information can be scanned and read.

- **Max Response Time Out (Sec):** Enter the maximum time duration till which response from Scanning device can be received.

Click **Save** button to save the reader settings.

Camera Settings



Input Settings

Addon Settings

Samsotech Reader Settings

Camera Settings

Scanning QR Code

Read Aadhaar Card/vCard □

Auto fill Aadhaar No. in ● ID Proof 1 ○ ID Proof 2

Input: USB Camera/Built-In Camera ▼

Capture Visitor Details

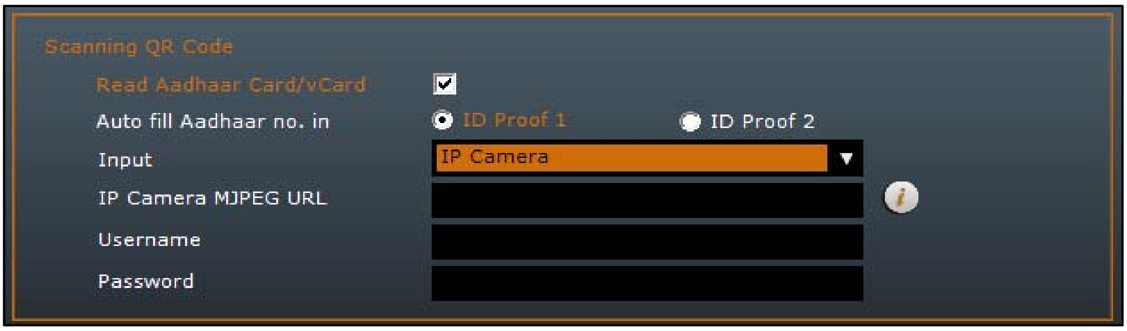
Enable USB Camera □

Input: USB Camera/Built-In Camera ▼

Configure the following parameters of Camera Settings.

Scanning QR Code:

Nowadays, people carry Aadhar Card as this document has QR Code which contains their basic details. Configure the following parameters.



Scanning QR Code

Read Aadhaar Card/vCard ☑

Auto fill Aadhaar no. in ● ID Proof 1 ○ ID Proof 2

Input: IP Camera ▼

IP Camera MJPEG URL

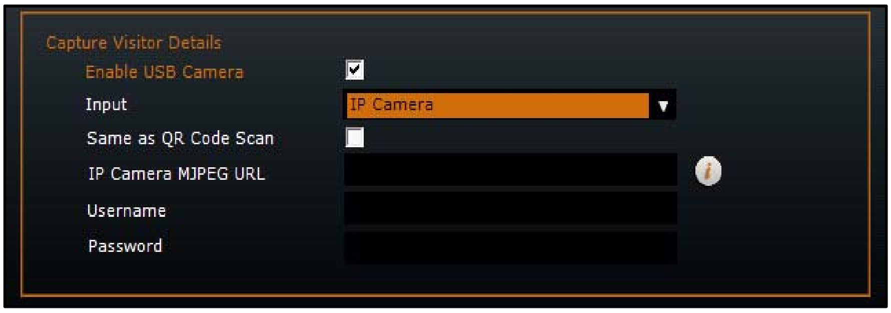
Username

Password

- **Read Aadhar Card/vCard:** Enable this check-box to fetch details of visitor's Id cards containing QR code.
- **Auto fill Aadhar no. in:** On scanning the QR code of an Aadhar card, the Aadhar number will be auto added in either fields of Additional details i.e ID Proof 1 or ID Proof 2 as per selection done here.
- **Input:** This allows User to select Input for QR code Scanning on Aadhar card/vCard via input options:
  - USB Camera/Built-In Camera
  - IP Camera
  - QR Code Scanner

For IP Camera, mention the **IP Camera MJPEG URL, Username** and **Password** to configure it.

Capture Visitor Details:



Capture Visitor Details

Enable USB Camera ☑

Input: IP Camera ▼

Same as QR Code Scan □

IP Camera MJPEG URL

Username

Password

- **Enable USB Camera:** Enable this checkbox to capture Visitor's Image using Camera.

- **Input:** Select the input for capturing visitor's image from options: *USB Camera/Built-In Camera* or *IP Camera.*

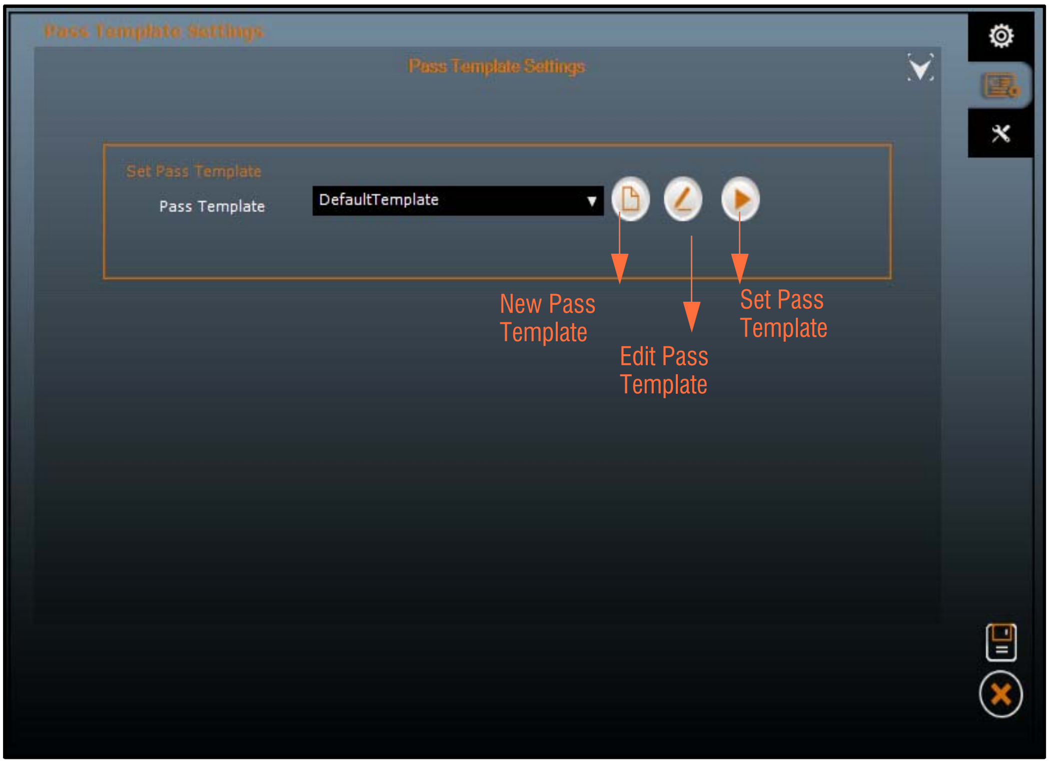
  For IP Camera, enable the **Same as QR Code Scan** if the IP Camera configuration is same as mentioned in Scanning QR code. If not, then mention the **IP Camera MJPEG URL, Username** and **Password** to configure it.

  Click **Save** button to save the reader settings.

Visitor Pass Template

The COSEC VMS application provides the user the flexibility to design visitor pass templates as per the site requirements. The software also comes with built-in visitor pass template that can be used straight away to print professional visitor passes for the visitors when they register. The pass can be printed at any stage of the visit.

In order to access the badge design functionality, click on the **Settings** icon on the toolbar as explained earlier. The **General Settings** page appears. Click on the **Pass Template Settings** icon as shown. The following page appears.



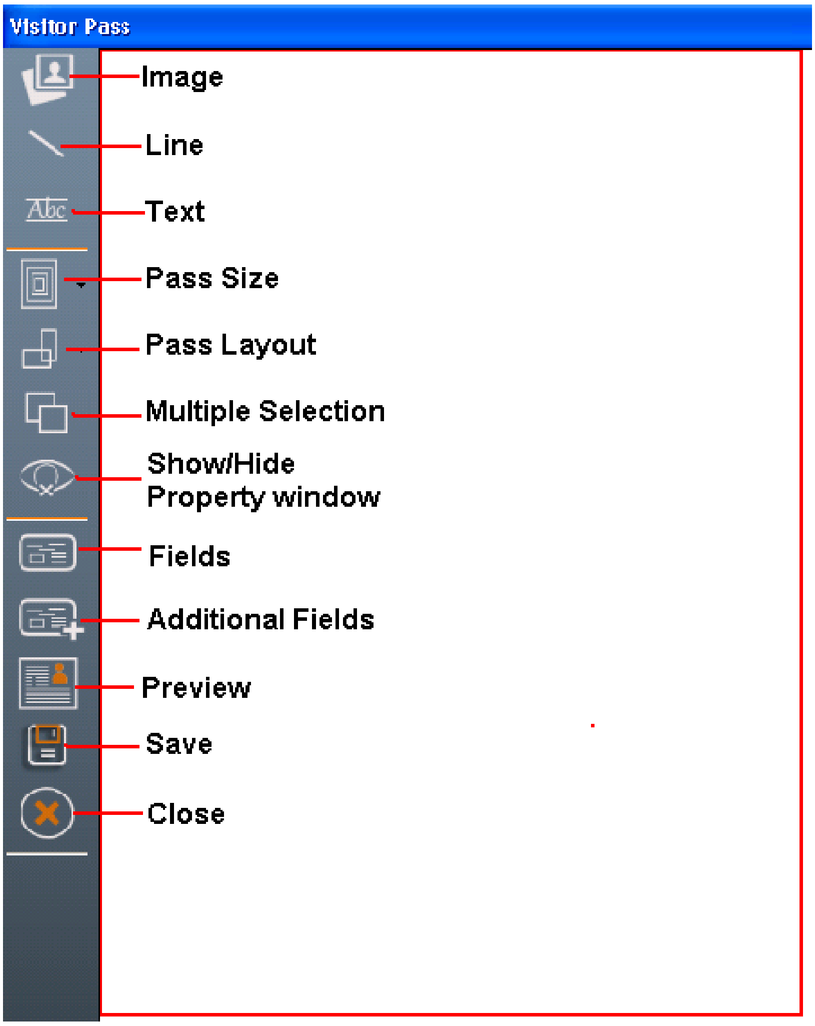
Pass Template Settings

Pass Template Settings

Set Pass Template

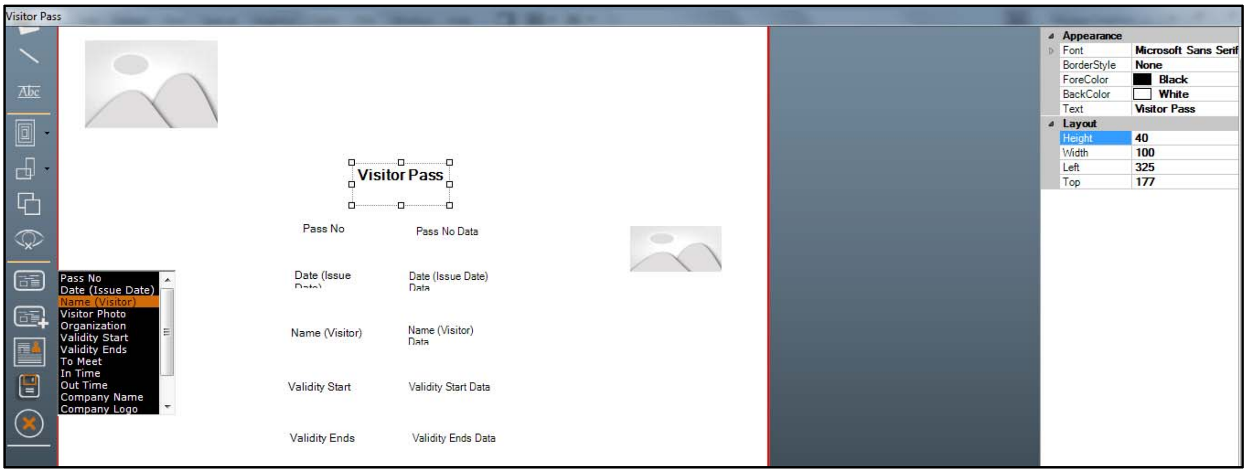
Pass Template: DefaultTemplate

Click on the **New Pass Template** button to create a new visitor pass template. The Visitor pass design page appears as shown.



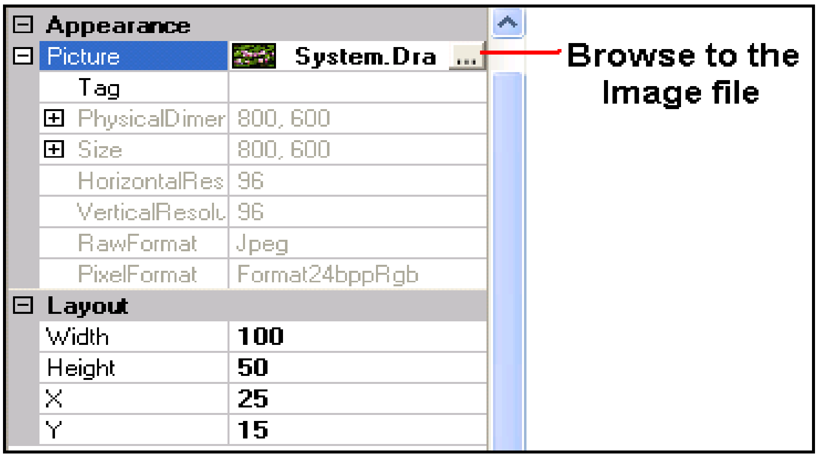
The **Image , Line and Text** options enables the user to place customized static entities on the page. The system will display the appropriate parameters in the properties window based on the selected entity.

Drag and drop image icon on the window. To view the property select **Show Property Window.**



Appearance	
Font	Microsoft Sans Serif
BorderStyle	None
ForeColor	■ Black
BackColor	□ White
Text	Visitor Pass
Layout	
Height	40
Width	100
Left	325
Top	177

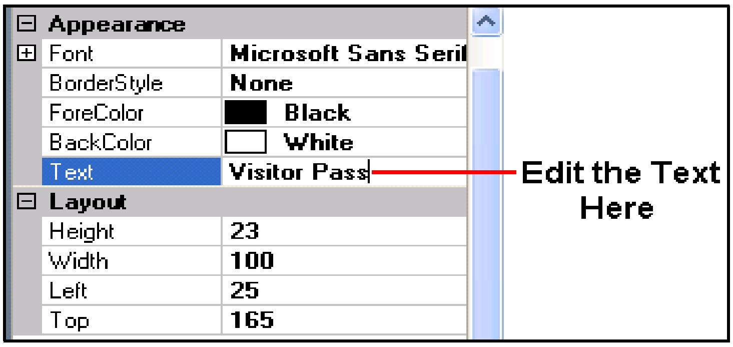
Click on the Browse button as shown and select the image file to be placed on the visitor pass. The Layout parameters to define the position and the size of the image can be edited as per the site requirements.



⊟ **Appearance**	
⊟ Picture	**System.Dra** ...
Tag	
⊞ PhysicalDimer	800, 600
⊞ Size	800, 600
HorizontalRes	96
VerticalResolu	96
RawFormat	Jpeg
PixelFormat	Format24bppRgb
⊟ **Layout**	
Width	**100**
Height	**50**
X	**25**
Y	**15**

Browse to the Image file

Place a Abc text frame on the window.The following parameters appear in the properties window as shown.

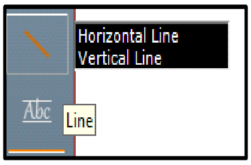


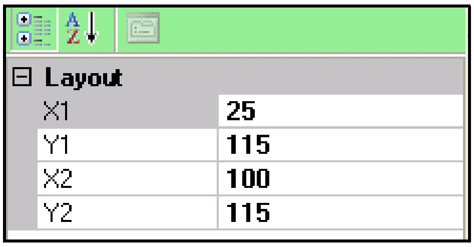
⊟ **Appearance**	
⊞ Font	**Microsoft Sans Serif**
BorderStyle	**None**
ForeColor	■ **Black**
BackColor	□ **White**
Text	**Visitor Pass**
⊟ **Layout**	
Height	**23**
Width	**100**
Left	**25**
Top	**165**

Edit the Text Here

The user can edit the Font settings as well as the layout of the text from the properties window after specifying the Text as shown.

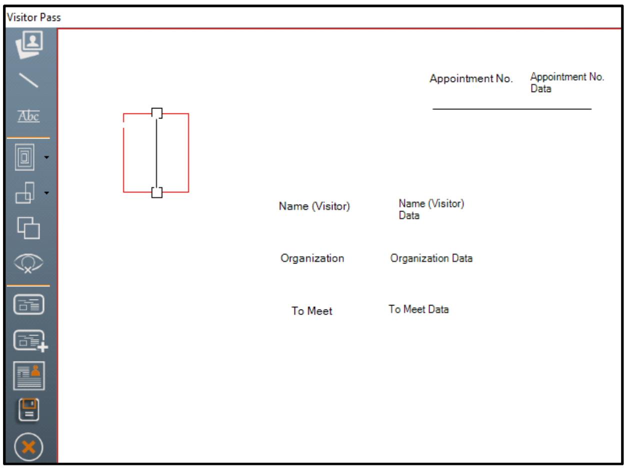
The **line** ╲ option can be selected as **Horizontal** or **Vertical.** The properties of line will be shown in properties section as shown below.

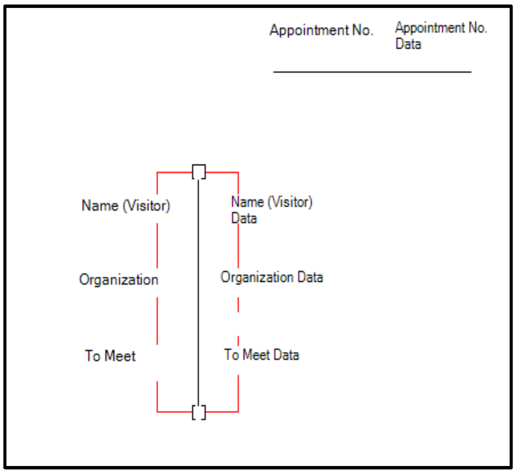




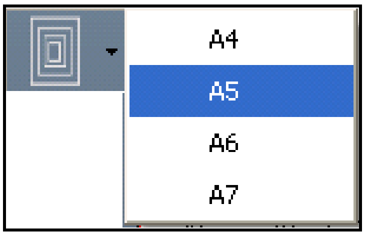
⊟ **Layout**	
X1	**25**
Y1	**115**
X2	**100**
Y2	**115**

You can edit the layout parameters of the line from the properties window or by directly dragging the edges of the line.
Select the Horizontal Line or Vertical Line as required on pass template. Then drag and place the line at desired place. To increase the size of line; drag it from the end points as shown below.

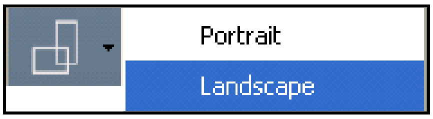




The user can now set the Pass Size by selecting the **Paper size** and the Pass Layout by selecting **Page Layout** for the visitor pass. The options available for the pass sizes are A4, A5, A6 and A7. Select the appropriate size from the drop down list.



The Pass Layout option has the portrait and the Landscape options. Select the appropriate option form the drop down list as per the site requirements.

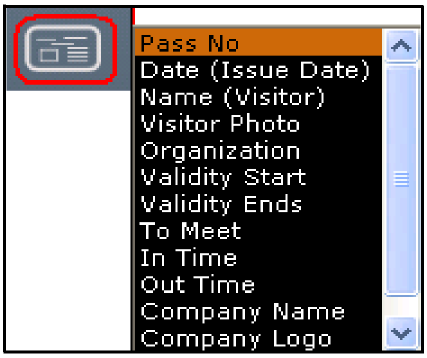


The visitor pass layout appears as per the selected options. The user can now add the static or dynamic fields to be displayed on the badge. Each of the fields can be mapped to an area of the Pass.

The Dynamic fields added to the pass have two components:

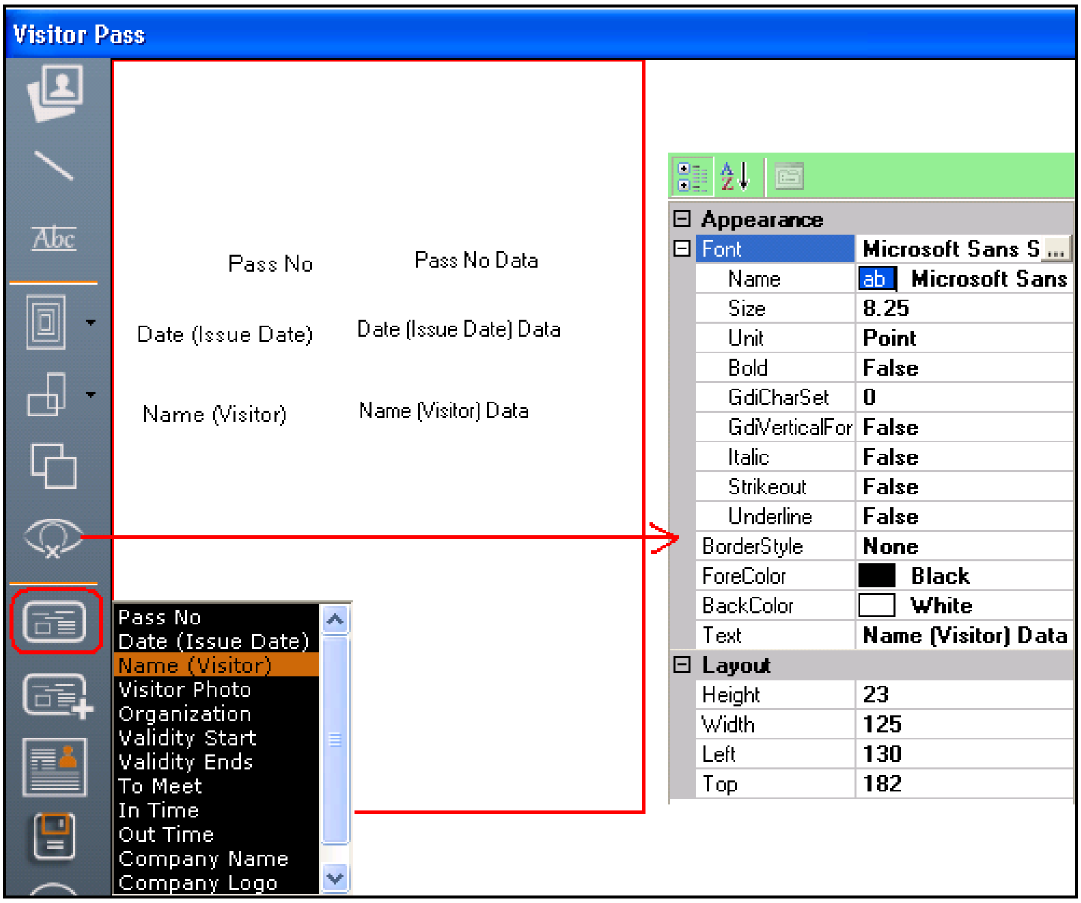
- Field Name
- Field Attribute

The Field attribute contains the name of the data field from which to get the content for this field. To select the fields whose positions are to be mapped on the pass, click on the Fields icon as shown.



The system displays the list of fields which can be placed on the Visitor pass. The user can now proceed with the placement of these controls on the pass layout.

Drag and drop the required fields on to the design page as shown in the following figure.



⊟ Appearance	
⊟ Font	Microsoft Sans S ...
Name	ab Microsoft Sans
Size	8.25
Unit	Point
Bold	False
GdiCharSet	0
GdiVerticalFor	False
Italic	False
Strikeout	False
Underline	False
BorderStyle	None
ForeColor	■ Black
BackColor	□ White
Text	Name (Visitor) Data
⊟ Layout	
Height	23
Width	125
Left	130
Top	182

The user can then drag each of the fields to the appropriate location on the visitor pass layout. The user can edit the display properties of each of the entities from the properties window as shown. Select the entity before editing its properties.

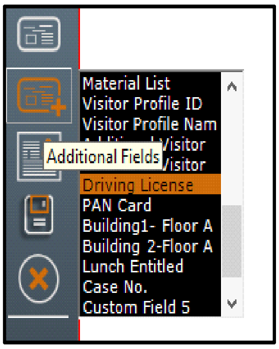
This Field List also includes **Repeat Mode, Repeat Visit, QR Code** and **Barcode**.

- Repeat Mode display is as per selection done in Repeat Visit Poup > Repeat Mode dropdown.
- QR Code and Barcode is generated using Appointment Number of the visit.

Click on the **Additional Fields** option to add some more visitor data to the Visitor pass. You can place the fields by scrolling the bar; drag and drop the field on designer page. Also the custom fields as specified from Global policy will appear in the Additional fields.

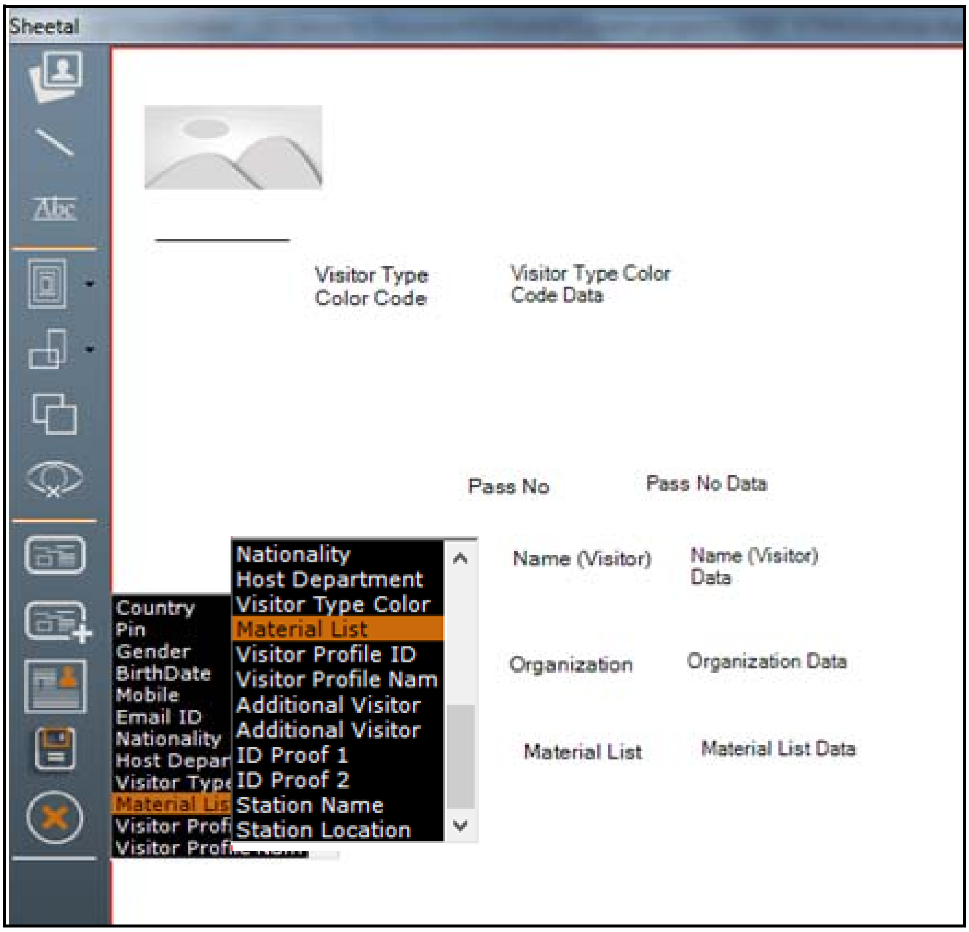
When the Custom field is edited; then on re-login into VMS Utility, field list will get updated with new custom field. But the template designed with previous custom field will remain same.

You can click on the Preview icon to view the final print layout of the visitor pass.

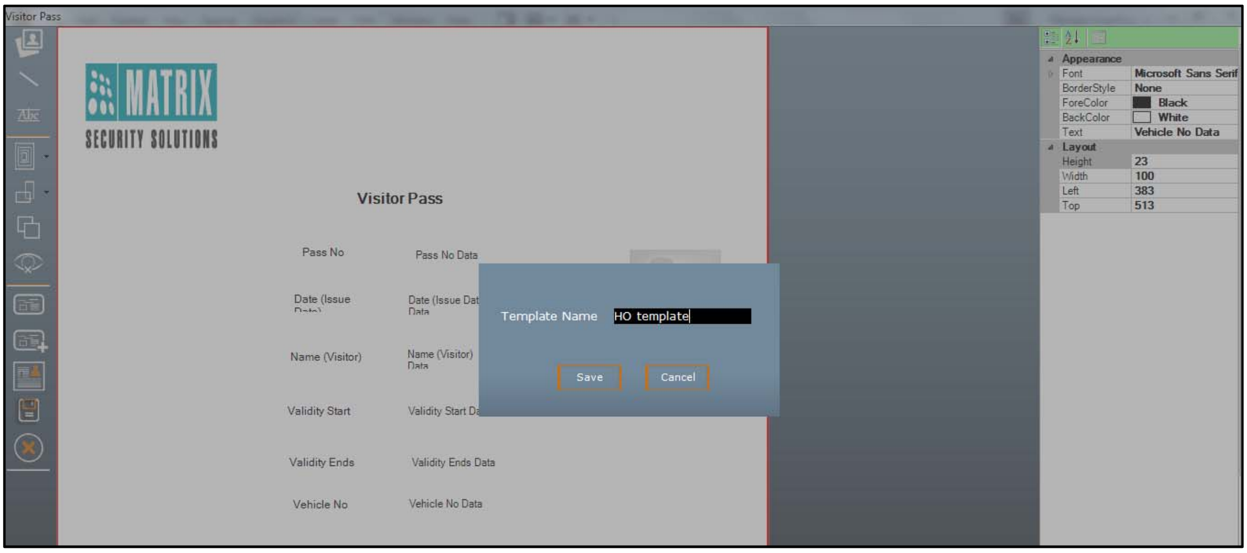


There is an option to select **Visitor Type Color** wherein the colour code assigned to the visitor type can be printed on the pass. So it becomes easy to recognize the visitor by visual inspection of colour from the visitor pass.

The **Material List** option enables to add the details of the materials (laptop, mobile etc) carried by the visitor on the pass itself. Also the **Visitor Profile Id** and **Visitor Profile Name** can be added to the pass.



Click on the Save icon to save the template. Enter a name to the configured template and Save.



Visitor Pass

Appearance	
Font	Microsoft Sans Serif
BorderStyle	None
ForeColor	Black
BackColor	White
Text	Vehicle No Data
Layout	
Height	23
Width	100
Left	383
Top	513

Visitor Pass

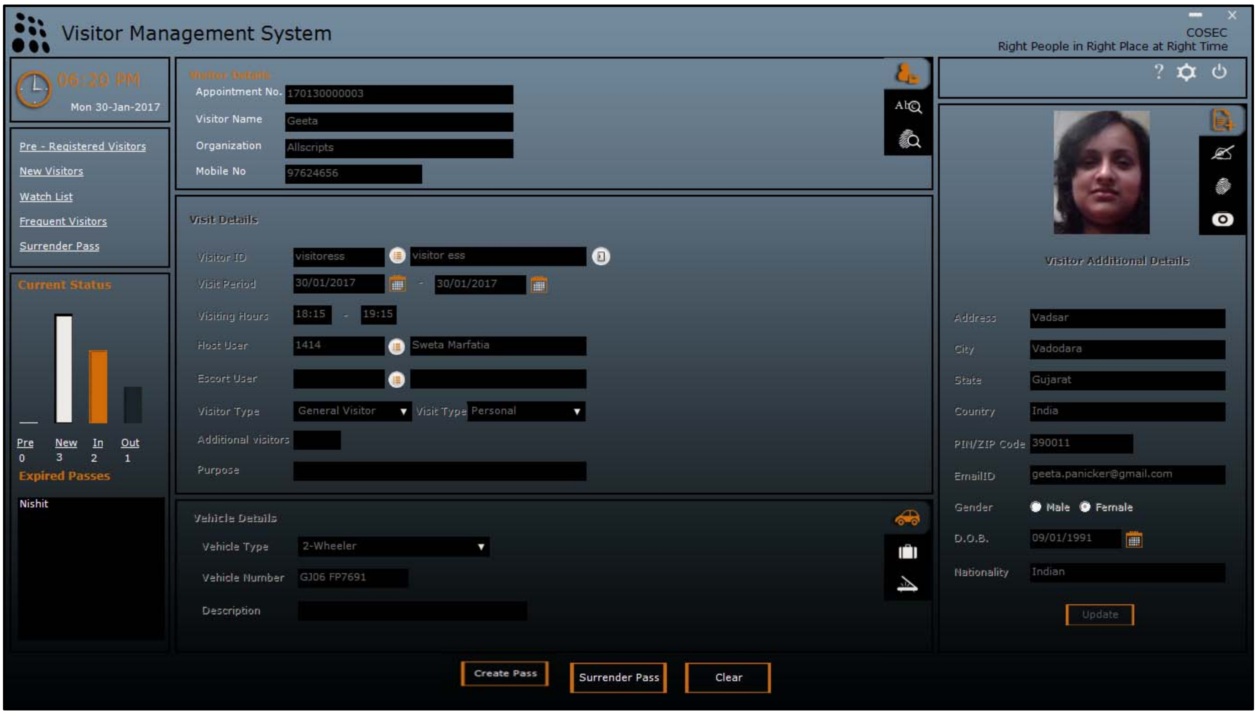
Pass No	Pass No Data
Date (Issue Date)	Date (Issue Date) Data
Name (Visitor)	Name (Visitor) Data
Validity Start	Validity Start Data
Validity Ends	Validity Ends Data
Vehicle No	Vehicle No Data

Template Name: HO template

Similarly, the user can edit an existing template or select another template from the drop down list and click on the **Set Template** icon to set the pass template as the current template. However, the user will not be able to edit a template which has been set as the current template.

Generating Visitor Pass

The visitor details are entered as shown below. The Pass template is set as **HO template** which is configured as described above.



Visitor Management System

COSEC
Right People in Right Place at Right Time

06:20 PM
Mon 30-Jan-2017

Visitor Details

Appointment No.	170130000003
Visitor Name	Geeta
Organization	Allscripts
Mobile No	97624656

Visit Details

Visitor ID	visitoress – visitor ess
Visit Period	30/01/2017 - 30/01/2017
Visiting Hours	18:15 - 19:15
Host User	1414 – Sweta Marfatia
Escort User	
Visitor Type	General Visitor
Visit Type	Personal
Additional visitors	
Purpose	

Vehicle Details

Vehicle Type	2-Wheeler
Vehicle Number	GJ06 FP7691
Description	

Visitor Additional Details

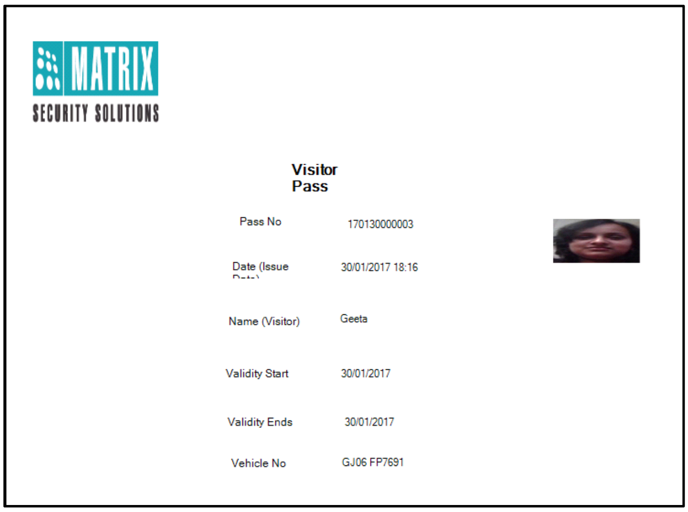
Address	Vadsar
City	Vadodara
State	Gujarat
Country	India
PIN/ZIP Code	390011
EmailID	geeta.panicker@gmail.com
Gender	○ Male ● Female
D.O.B.	09/01/1991
Nationality	Indian

Current Status

Pre	New	In	Out
0	3	2	1

Expired Passes
Nishit

Click on **Create Pass.** The Print Preview window will appear. You can preview and print the pass from the configured printer.



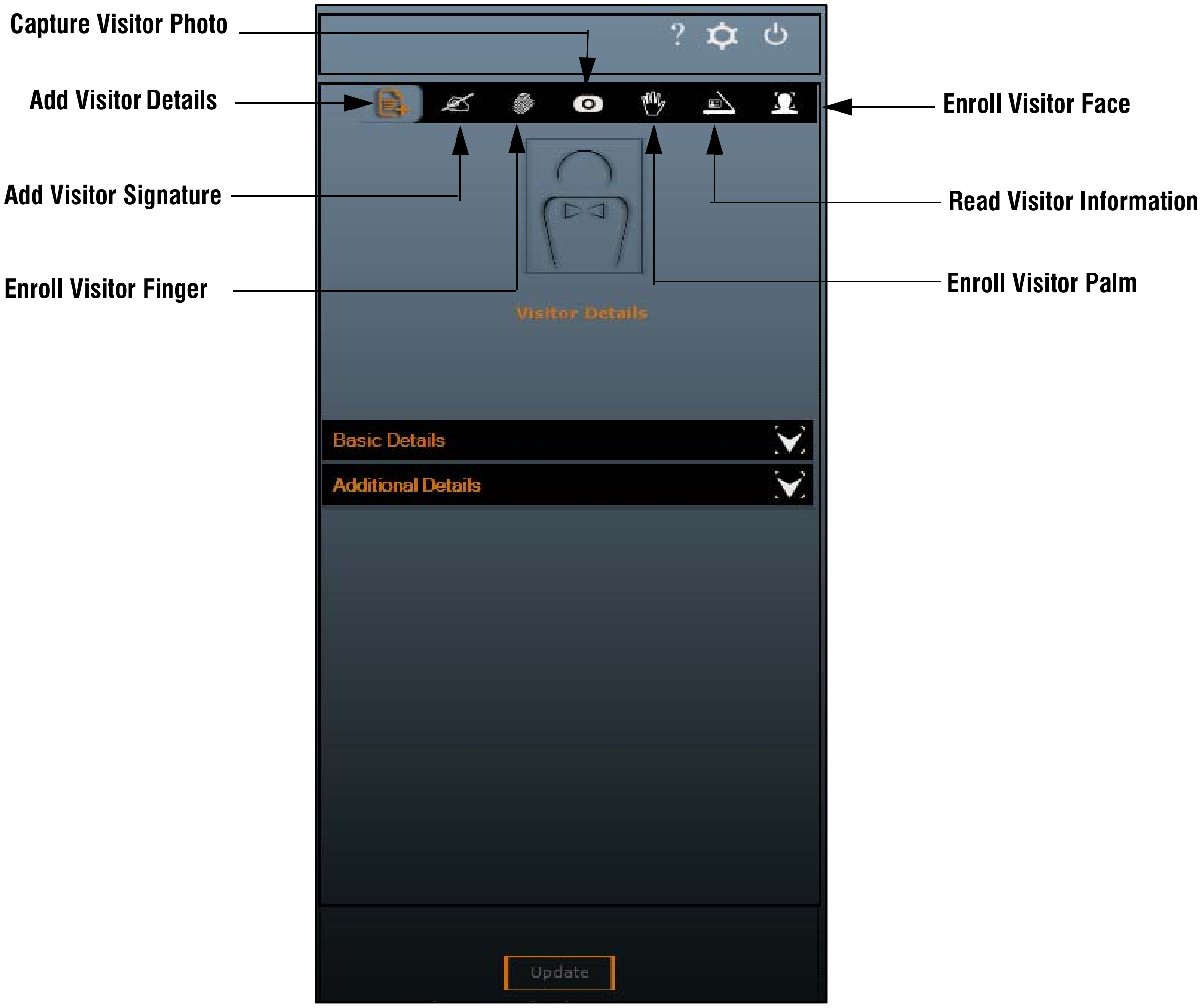
MATRIX SECURITY SOLUTIONS

Visitor
Pass

Pass No	170130000003
Date (Issue Date)	30/01/2017 18:16
Name (Visitor)	Geeta
Validity Start	30/01/2017
Validity Ends	30/01/2017
Vehicle No	GJ06 FP7691

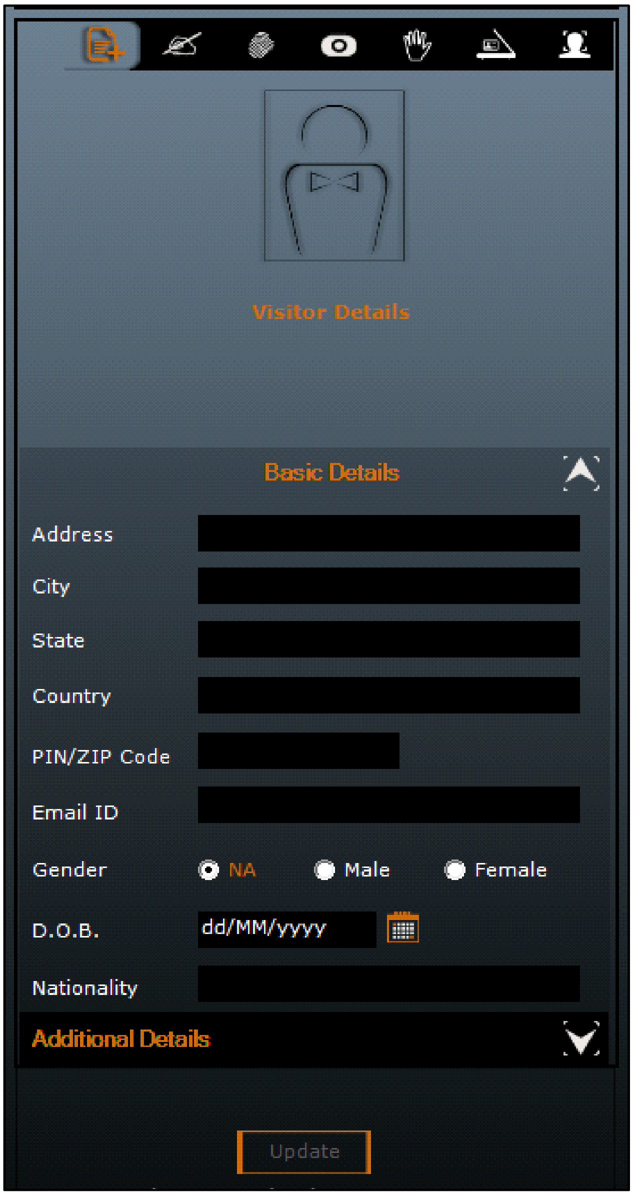
Visitor Details

The COSEC VMS application home page has the **Visitor Details** section, where the operator can add basic details like Address, Date of Birth, Photo image, Fingerprint template, signature etc at the time of Visitor registration.



Add Visitor Details

There are 2 tabs under **Add Visitor Details —** Basic Details and Additional Details.



Visitor Details

Basic Details

Address

City

State

Country

PIN/ZIP Code

Email ID

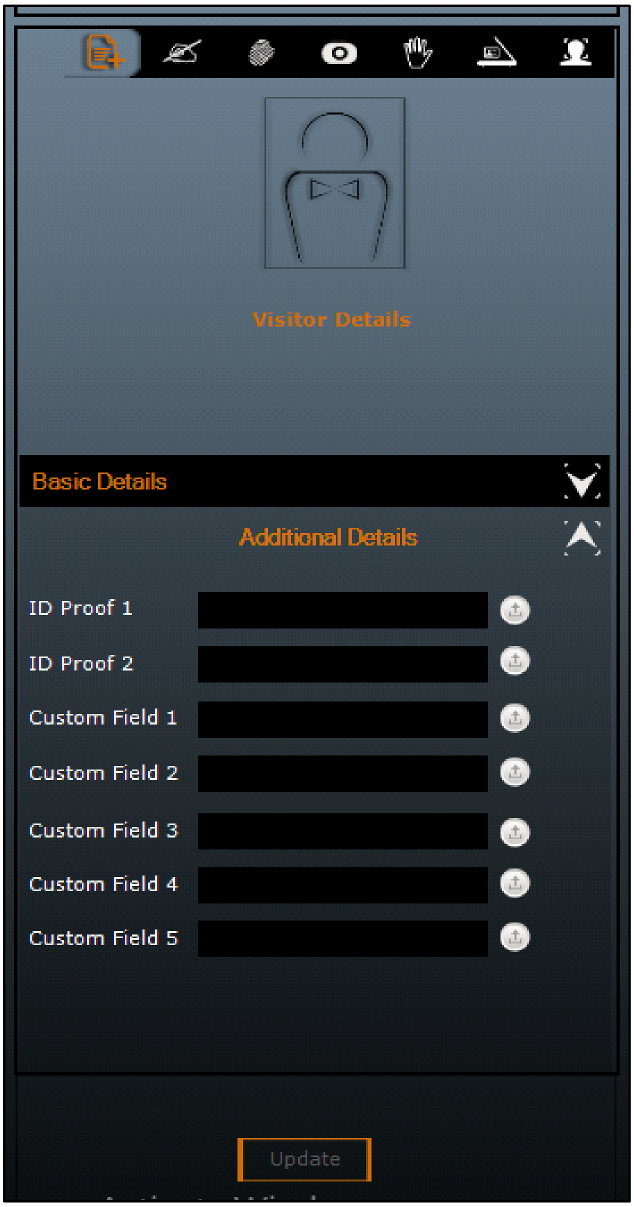
Gender ● NA ○ Male ○ Female

D.O.B. dd/MM/yyyy

Nationality

Additional Details

Update



Visitor Details

Basic Details

Additional Details

ID Proof 1

ID Proof 2

Custom Field 1

Custom Field 2

Custom Field 3

Custom Field 4

Custom Field 5

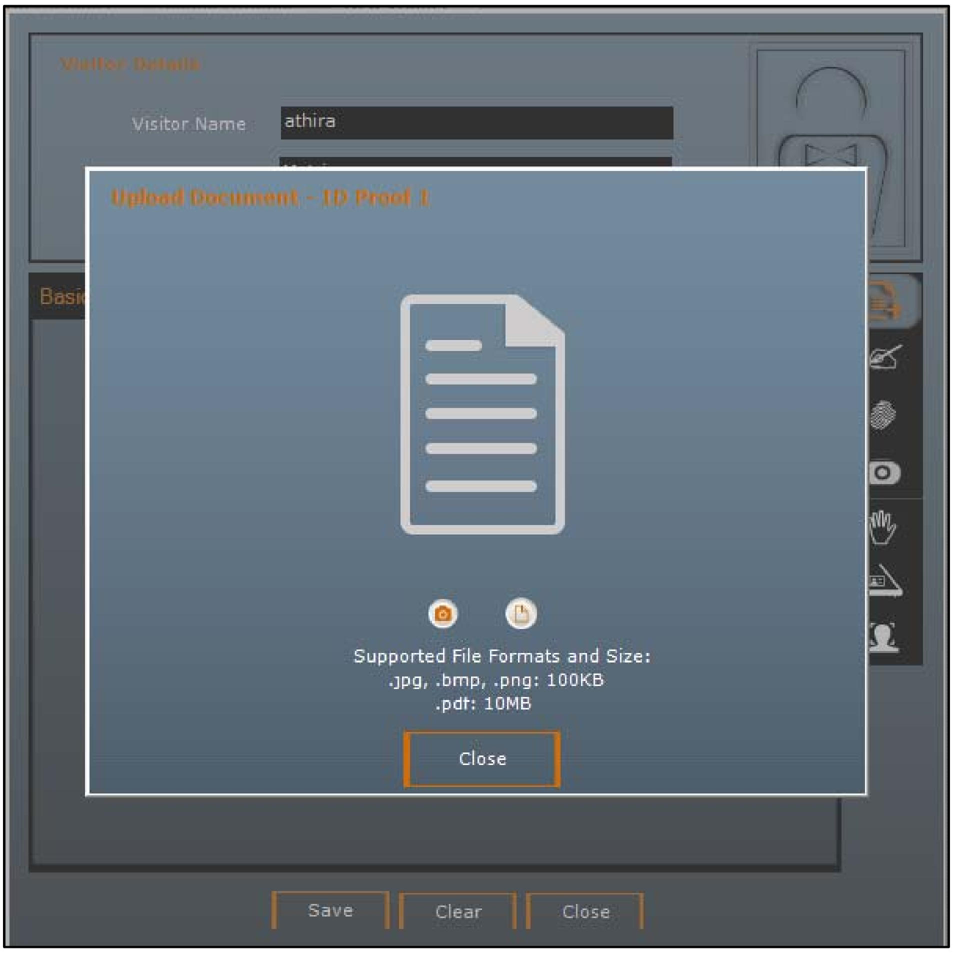
Update

Under Basic Details, enter the basic details of visitor like — Address, City, State, Country, PIN/ZIP Code, Email ID, Gender, Date of Birth and Nationality.

Under Additional Details, enter the necessary details of visitor. You will be required to upload documents for certain parameters.

Custom Fields in Additional Details are visible only after they are configured by your System Administrator.

To upload any document, click **Upload** button. The **Upload Document** pop-up appears as shown below:



Visitor Name: athira

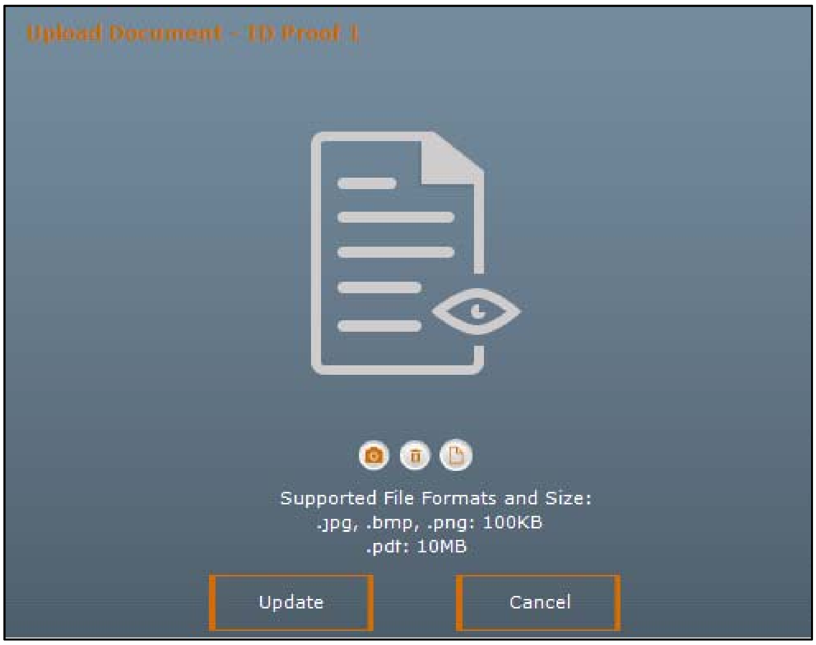
Supported File Formats and Size:
.jpg, .bmp, .png: 100KB
.pdf: 10MB

To upload the document, click the **Document** icon. Make sure the documents are as per the formats and size supported by the system.

You can even capture the image of the required document by clicking **Capture** and then upload it.

You will be able to delete the document/image you selected to upload by clicking **Delete** .

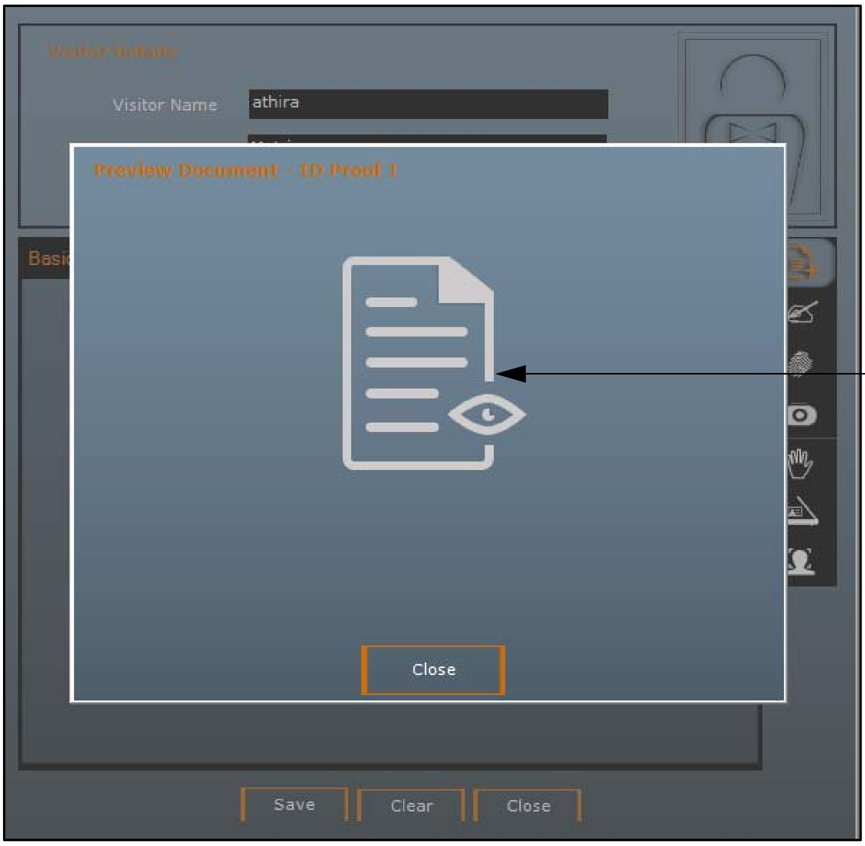
Click **Update.**



Upload Document - ID Proof 1

Supported File Formats and Size:
.jpg, .bmp, .png: 100KB
.pdf: 10MB

Once you upload the file, you can preview the uploaded file. To preview, click **Preview** button. **Preview Document** window appears where you can preview as well as download the uploaded document by clicking on the document icon shown below:



Visitor Details

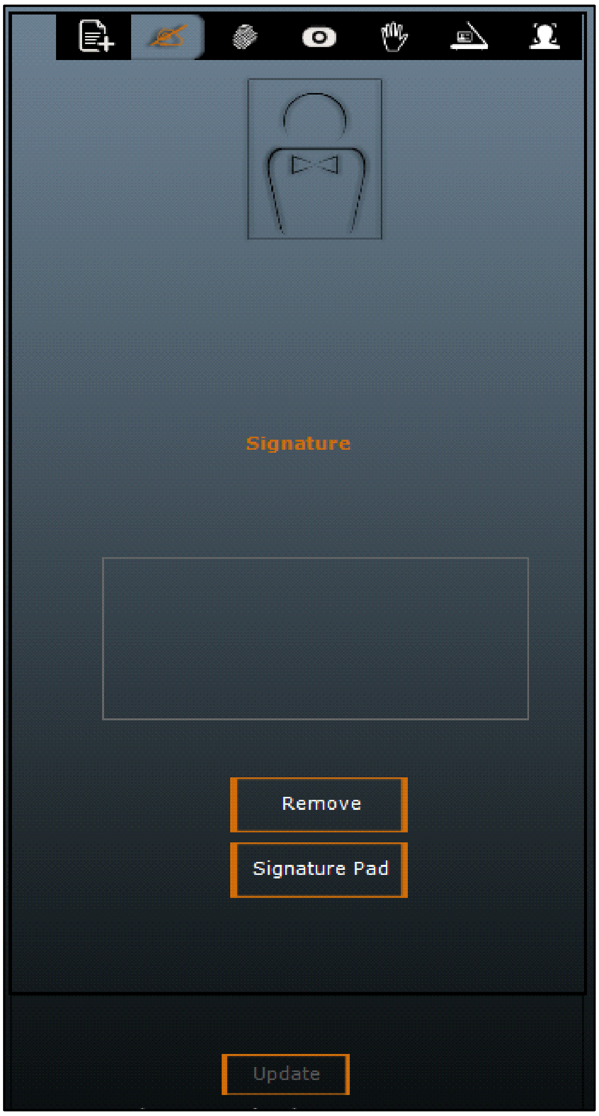
Visitor Name: athira

Preview Document - ID Proof 1

Click here to download the Uploaded document/image

Add Visitor Signature

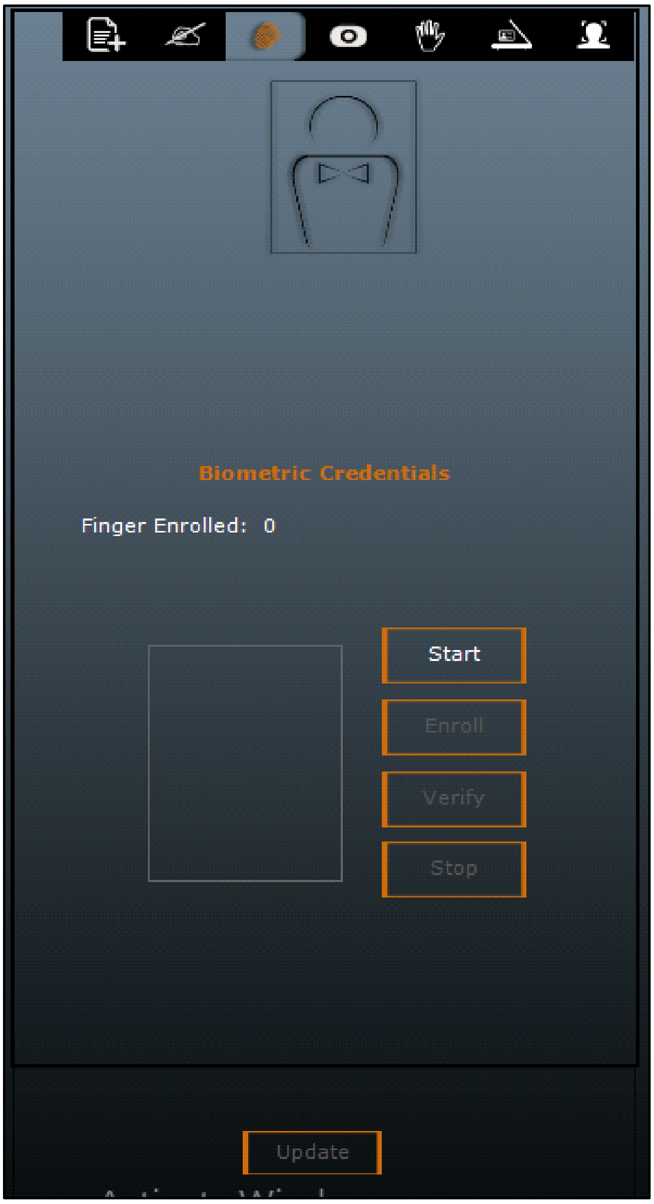
You can add the visitor’s signature here.



The process of adding the visitor’s signature is same as done in **New Visitors**. So refer *“Add Visitor Signature”* under New Visitors to know how to add the signature.

Enroll Visitor Finger

You can enroll visitor's finger here.

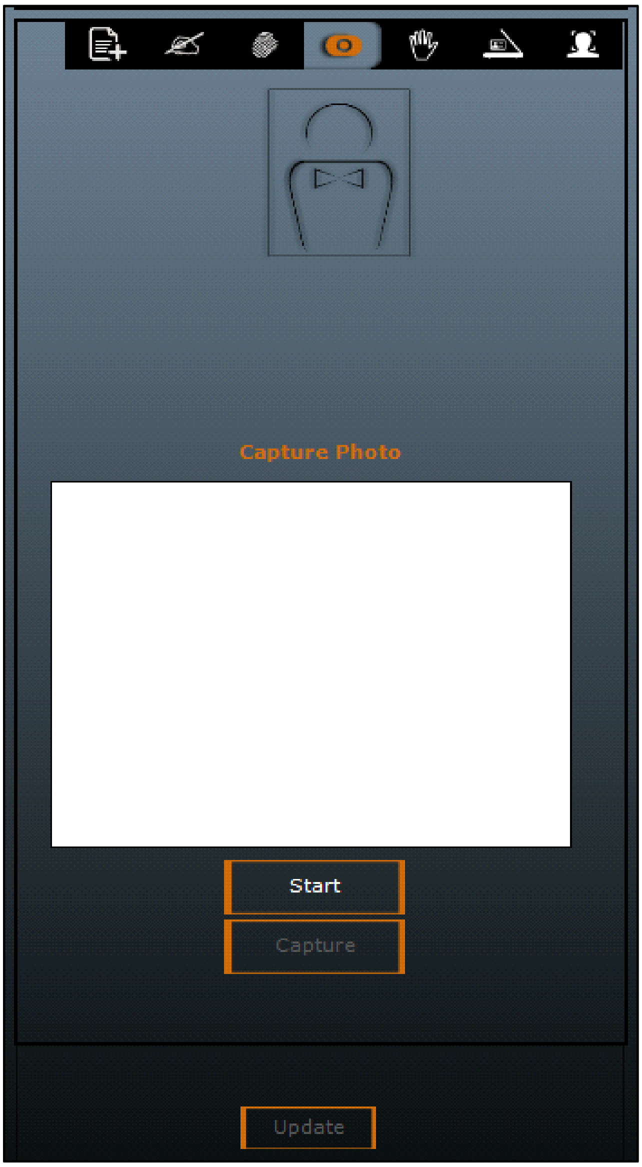


Finger Enrolled: 0

To know how to enroll the visitor's finger, refer *"Enroll Visitor Finger"* under New Visitors.

Capture Visitor Photo

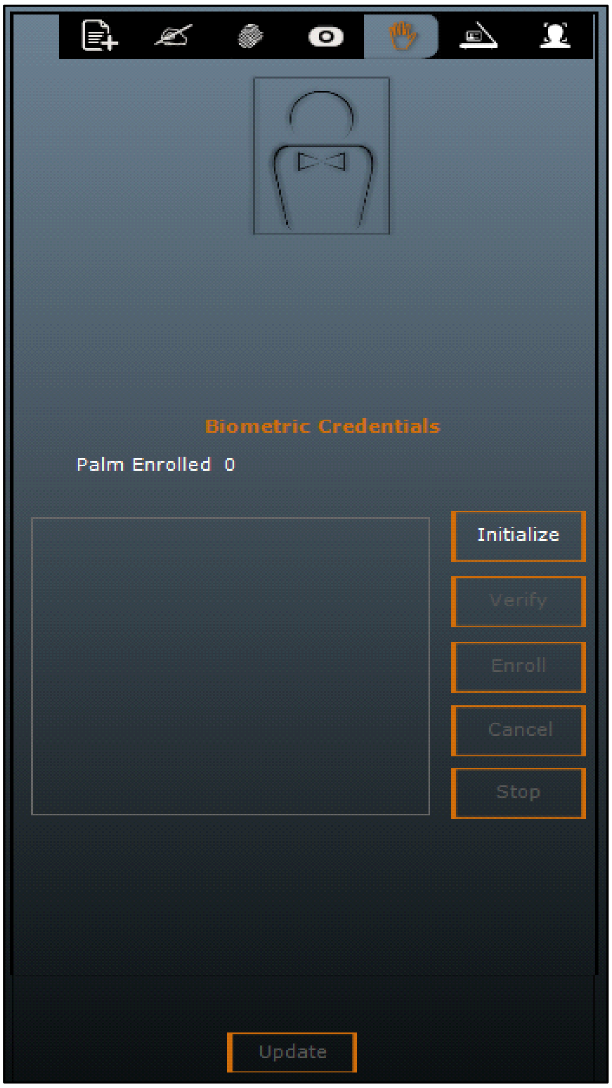
You can capture visitor's photo here.



To know how to capture a visitor's photo, refer *"Capture Visitor Photo"* under New Visitors.

Enroll Visitor Palm

You can enroll the visitor's palm here.



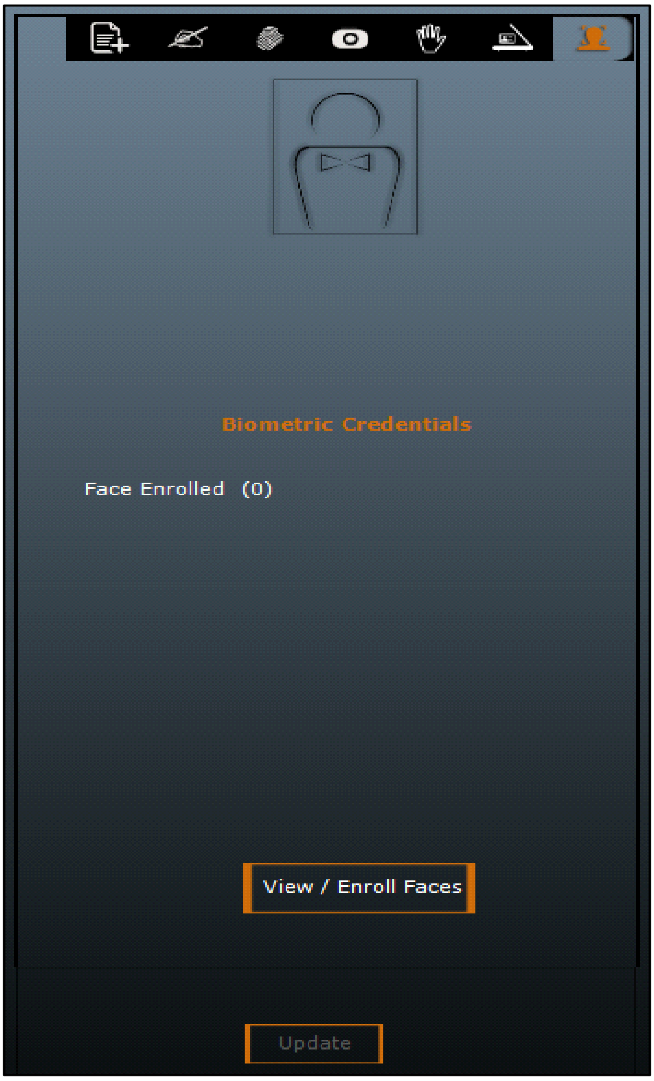
To know how to enroll the visitor's palm, refer *"Enroll Visitor Palm"* under New Visitors.

Read Visitor’s Information

When Samsotech Scanner / QR code Scanner is connected with VMS Utility then user Identity card (Driving License, PAN Card, Aadhar Card, Passport etc) can be scanned to get the information in VMS Utility. For more information, refer *“Read Visitor’s Information”.*

Enroll Visitor Face

You can enroll the visitor’s face from here.



Biometric Credentials

Face Enrolled (0)

To know how to enroll a visitor’s face, refer *“Enroll Visitor Face”* under New Visitors.

Registering Visitors

The COSEC VMS application enables you to register the visitor details before, or at the time of their arrival. There are 3 categories of visitors in the COSEC VMS application.

- First time visitor
- Frequent Visitor
- Pre-registered visitor

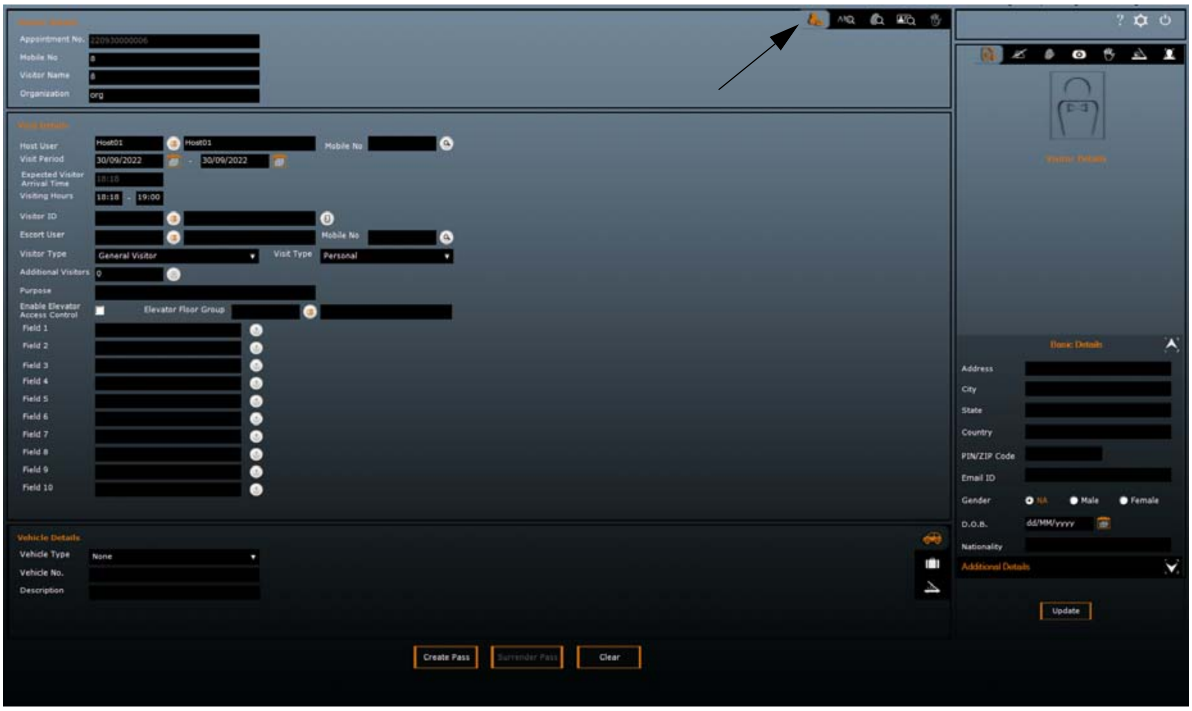
The operator needs to enter the details of the first time Visitor at the time of their arrival, while the other two categories already have their details in the visitor database.

The pre-registered visitors are either added from the COSEC Web application or the COSEC ESS application. Refer the COSEC system manual and the COSEC ESS manual for more details. Pre-registration involves the following:

- Providing basic information about the visitor and host.
- Providing additional information about the visitor.

Registering a First time Visitor

This involves cases of unplanned visits when the visitor is not pre-registered and is not a frequent visitor. In such cases, the registration is done directly from the VMS station when the visitor arrives. Click on the **New Visitor Mode** on the COSEC VMS home page as shown.

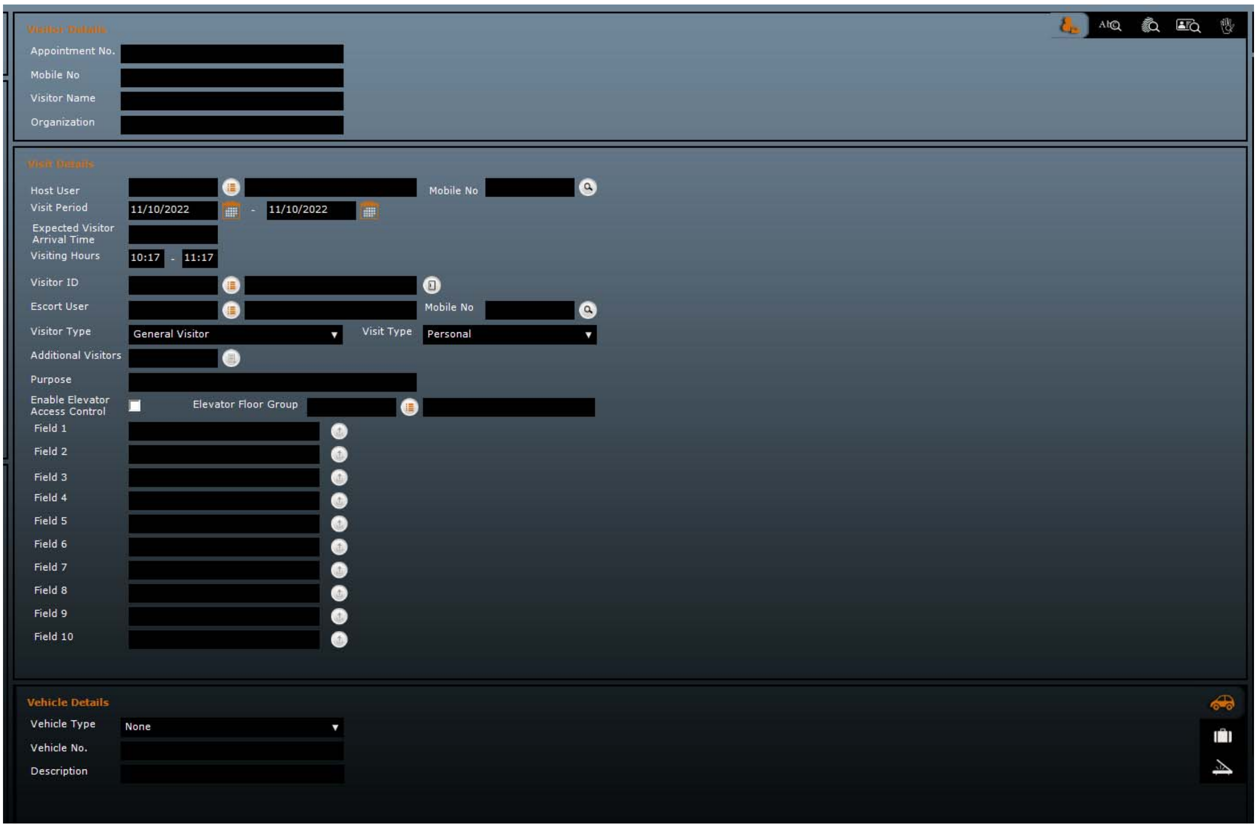


Appointment No. 220930000006
Mobile No 8
Visitor Name 8
Organization org
Host User Host01 Host01
Visit Period 30/09/2022 - 30/09/2022
Expected Visitor Arrival Time 18:18
Visiting Hours 18:18 - 19:00
Visitor Type General Visitor
Visit Type Personal
Additional Visitors 0
Enable Elevator Access Control ☐
Vehicle Type None
Gender ● NA ○ Male ○ Female
D.O.B. dd/MM/yyyy

When Samsotech Scanner is connected with VMS Utility then user Identity card (Driving License, PAN Card, Aadhar Card, Passport etc) can be scanned to get the information in VMS Utility.

Click on **Read Visitor's Information** icon. Then you can click on **Scan Card** or **Scan Chip** depending on the identity card to scan the visitor's information. After successful scanning the visitor's information will automatically appear in the Visitor Details fields based on the Reader Configuration done in COSEC Web > Visitor Management > Visit Components.

You can also enter the Visitor details manually as shown below.



Visit Period: 11/10/2022 - 11/10/2022
Visiting Hours: 10:17 - 11:17
Visitor Type: General Visitor
Visit Type: Personal
Vehicle Type: None

Enter the visitor details as explained below.

Visitor Details:

Field	Description
Visitor Name	Specify name of the Visitor. This is a mandatory field.
Organization	Specify the visitor’s organization name. This is a mandatory field.
Mobile No.	Specify the visitor’s cellphone number. This is a mandatory field.

Visit Details:

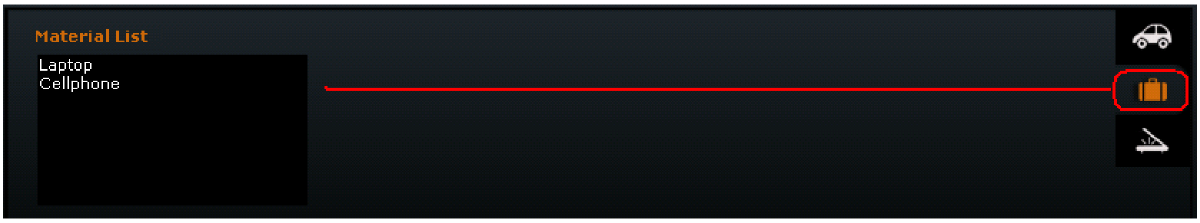
Field	Description
Host User	Click on the Picklist button and select the host from the User Master Picklist window.
Visit Period	The current date appears by default.
Expected Visitor Arrival Time	Enter the Visitors expected time of arrival.
Visiting Hours	The current time being the start time, the system by default specifies a one hour visit duration.

Field	Description
Visitor ID	Click on the Visitor ID picklist button and select the Visitor ID which is to be assigned to the visitor from the pop up window. Note: No Passes can be generated without Visitor ID (Visitor Profile) selection.
Escort User	In the event of the Escort rule being enabled on the PANEL DOORs, the user needs to specify an escort user whose credential is to be authenticated after the visitor credential. Click on the Picklist button and select the host from the User Master Picklist window. This feature has to be enabled at the COSEC PANEL200 as it is available only on the PANEL DOORs.
Visitor Type	Select from the options in the drop down list.
Visit Type	Select from the options in the drop down list.
Additional Visitors	Specify the number of additional visitors accompanying the visitor.
Purpose	Specify the purpose of the visit.
Enable Elevator Access Control	Assign Elevator Access Control to the visitors while creating Visitor Profile.
Elevator Floor Group	If Elevator Access Control is enabled, then this picklist will be enabled. If any Elevator Floor Group is selected from the picklist then access of that Floor Group should be provided to Visitor and Configuration for the same will be sent to all applicable devices. If no Elevator Floor Group is selected then access of all free floors will be provided to Visitor and Configuration for the same will be sent to device.
Visit Custom Fields (1-10)	Specify the information as per the format — Date or Time. Click on Upload button to upload any document. Click on Capture button to capture the image of required document and upload it.

Vehicle Details:

Field	Description
Vehicle Type	Select the vehicle type from the drop down list..
Vehicle Number	Specify the license plate number.
Description	Specify a description for the visitor vehicle.

Material List: Click on the Material List icon to specify the materials being carried by the visitor into the premises.



Material List

Laptop
Cellphone

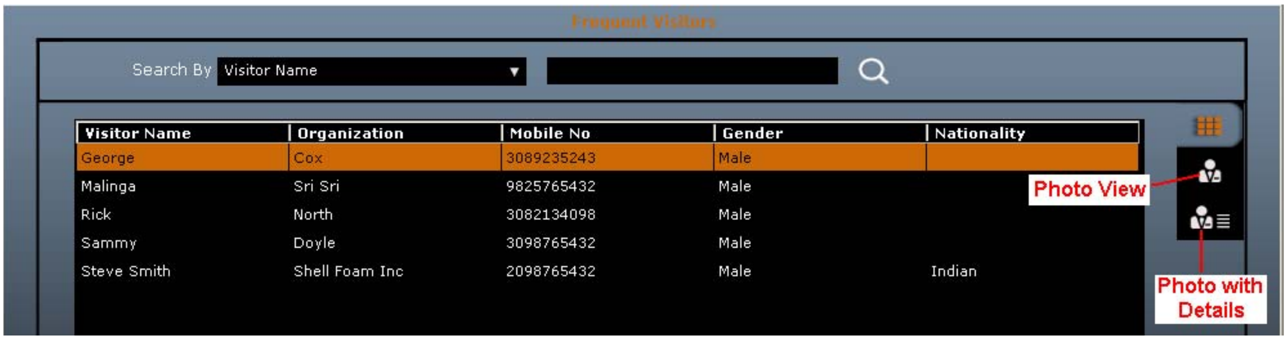
Visitor Document Scanning: Click on this icon and click on the Scan Documents button to scan the Visitor documents.

Click on the **Create Pass** button to complete the visitor check in process.

Registering a Frequent Visitor

Click on the Frequent Visitors link in the left pane of the COSEC VMS home page. The Frequent Visitors page pops up displaying the list of existing regular Visitors. The operator can filter the Visitors by Visitor Name, Organization, Mobile No., Gender and Nationality. The COSEC VMS application will load all the details of selected Visitor with photo and Fingerprint on the Visitor check in page.

The Frequent Visitor page also enables the user to select the Photo View or the Photo View with details as shown.



Frequent Visitors

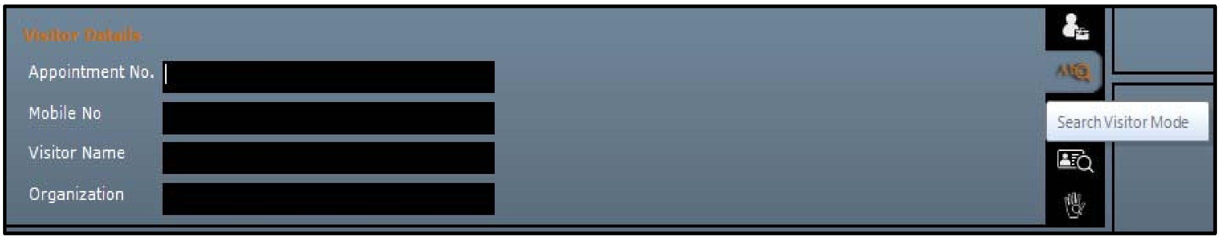
Search By Visitor Name

Visitor Name	Organization	Mobile No	Gender	Nationality
George	Cox	3089235243	Male	
Malinga	Sri Sri	9825765432	Male	
Rick	North	3082134098	Male	
Sammy	Doyle	3098765432	Male	
Steve Smith	Shell Foam Inc	2098765432	Male	Indian

Photo View

Photo with Details

The operator can also use the **Search Visitor mode** icon in the Visitor Details section to search for existing visitors. The COSEC VMS allows the operator to filter the search based on the Appointment No, Visitor Name, Organization or Mobile No. as shown.



Visitor Details

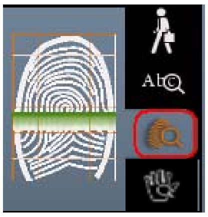
Appointment No.

Mobile No

Visitor Name

Organization

Similarly, the system can also search the visitor database by performing a fingerprint and palm match. Click on the **Search Visitor FP mode** and **Search Visitor Palm mode** icon to initiate the search process as shown.



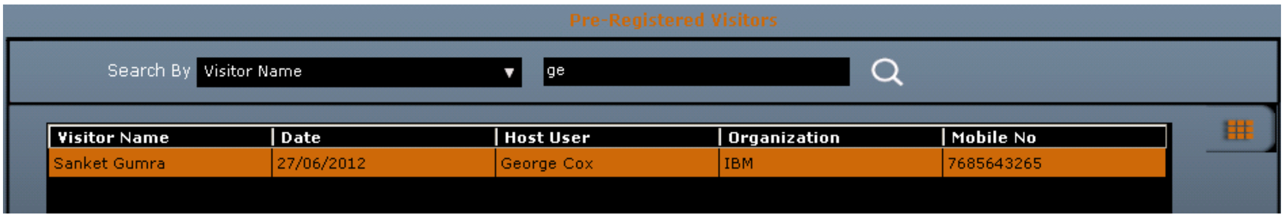
The Visitor needs to now place the previously registered finger on the fingerprint scanner.

Storing Visitor Information is necessary for Visitor Search feature to function properly. Palm search will be done locally only.

Registering a Pre-registered Visitor

Click on the **Pre - Registered Visitors** link in the left pane of the COSEC VMS home page. The Pre - Registered Visitors page pops up displaying the list of existing pre-registered Visitors. The user can filter the Visitors by Visitor

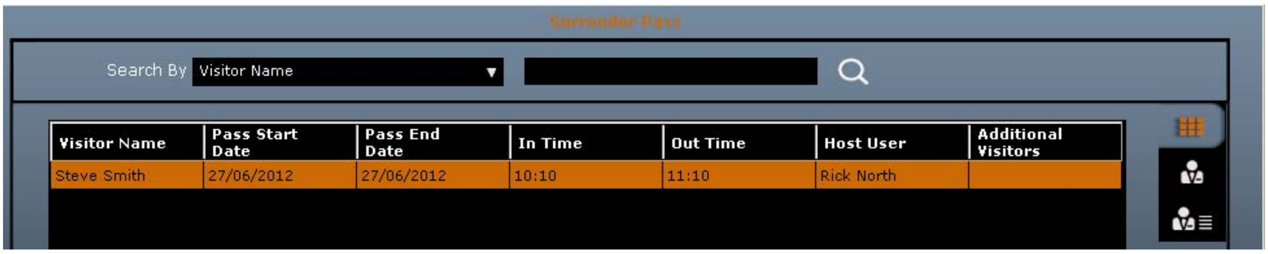
Name, Date, Host User, Organization and Mobile No.. The COSEC VMS application will load all the details of selected Visitor as entered by the administrator or host user at the time of pre-registration.



Visitor Name	Date	Host User	Organization	Mobile No
Sanket Gumra	27/06/2012	George Cox	IBM	7685643265

Visitor Signing out

The visitor must sign out while leaving the premises. Signing out a visitor ensures that the visitor has left the premises. The COSEC VMS has the Surrender Pass functionality to sign out visitors. Click on the Surrender Pass link in the left pane of the COSEC VMS home page.

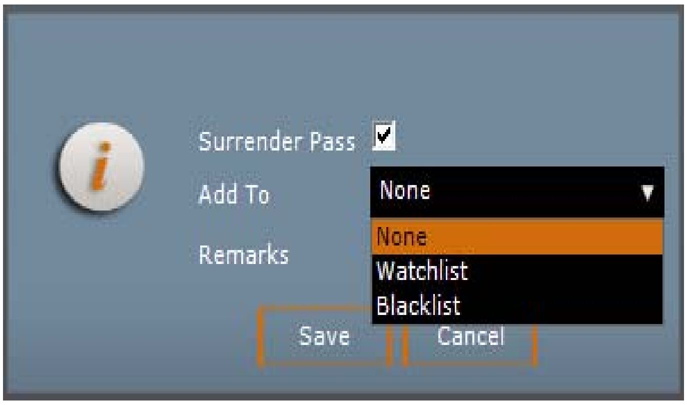


Surrender Pass

Search By: Visitor Name ▼

Visitor Name	Pass Start Date	Pass End Date	In Time	Out Time	Host User	Additional Visitors
Steve Smith	27/06/2012	27/06/2012	10:10	11:10	Rick North	

The list of check in visitors appears in the Surrender Pass window. The operator can filter the Visitors by Visitor Name, Pass Start Date, Pass End Date, In Time, Out Time, Host User, Type and Additional Visitors. Select the Visitor to be checked out from the list and click on the **Surrender Pass** option.



Surrender Pass ☑

Add To: None ▼

The above window also enables the operator to add a visitor to the **Watchlist/Blacklist.** Select the appropriate option from the dropdown list. Click **Save** in order to sign out the visitor.

This option can also be used to reprint a visitor pass in the event any error occurs while printing the pass at the time of visitor check in. Click on the Reprint button to print the visitor pass again. However, this option will not be available for visitors whose passes have expired due to overstay.

Once the Visitor pass is expired, the visitor ID will get free. And then the visitor ID can be assigned to the other visitor.

MATRIX

SECURITY SOLUTIONS

MATRIX COMSEC

Head Office:
394-GIDC, Makarpura, Vadodara - 390010, India.
Ph: (+91)18002587747
E-mail: Tech.Support@MatrixComSec.com

www.MatrixSecuSol.com