

# FREQUENTLY ASKED QUESTIONS

COSEC

What  
When  
Which  
Where  
How  
Who  
Why



**Date:** 25<sup>th</sup> February 2015

**Version:** V1R1

**Author:** Nishit Gandhi

## Smart Identification

In COSEC Devices 9,600 Fingerprints can be stored. We have 10,000 users but we cannot store the fingerprints of all the users in Device. We will have to find a solution for this.



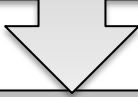
Let me find its solution in COSEC.



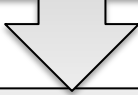
Great! COSEC is having solution to each and every problem. It has a feature called Smart Identification in which Fingerprints are stored in Smart Card itself.



Enable Smart Identification from COSEC Web Admin Module and set the General Additional Security Code



Enable Smart Identification in the respective Device as well



Enable Smart Identification while Enrolling User's Smart Card from COSEC Enroll Utility

Let me follow the  
above steps perfectly  
so that I can enable the  
Smart Identification  
Feature and utilize it.



Welcome System Admin - Google Chrome  
localhost/COSEC/Index.aspx  
MATRIX COSEC  
Right People in Right Place at Right Time

Admin

- System Accounts
- System Configuration
  - Global Policy**
  - Monitor Configuration
  - Rename Group
  - Enterprise Profile
  - Alert Message Configuration
  - Custom Message
  - Workstations
  - Component Status
  - Location Master
- System Utilities
- Views/Logs
- License Information

Global Policy

- Basic
- User
- Login
- Device**
- Access Control
- Time Attendance
- Roster
- Reports
- Visitor Management
- CWM
- Security

Auto Clear Alarm

Max Un-cleared Alarm 0

Sync Device Time With Server Time

Smart Identification

General Additional Security Code [.....] [.....]

Auto Add New Devices

Auto Assign New Device To Device Group

Device Group [ID] [Name] [↕]

Run PVR Door in Guide Mode

Welcome System Admin - Google Chrome  
localhost/COSEC/Index.aspx

**MATRIX** COSEC  
Right People in Right Place at Right Time

Devices

Device List  
Device Configuration  
Multi-Device Options  
Milestone Integration  
Masters  
Device Status  
Reports

Device Configuration

77  
Vega Controller-Device-77  
Vega Controller  
1/50000  
Active

Profile  
**Advanced**  
Features  
Others  
Cafeteria  
Special Functions  
Input Output  
Additional

Settings Timers

Generate Exit Switch Events   
Generate Invalid User Events   
Allow Exit When Door Lock   
Auto Relock   
Alarms   
Tamper Alarm   
Enable Additional Security  Configured  
Additional Security Code \*\*\*\*\*  
Re-Enter Code \*\*\*\*\*  
Warning: Changing this value can affect the SI function. **Default**  
Enable Smart Identification   
Access Level 8  
Access Mode Card  
Auto Acknowledge Alarm   
Alarm Auto Acknowledge Timer (Sec) 0

Set the Access Mode for this Device as required

Select Category: User Name: henl Search Clear Card Template Help Enable Logs

User ID	Name	Short Name	Enrolled Fingers	Enrolled Palms	Card 1	Card 2	Blood Group	Medical History	Personal Mobile
995	Henley	Henley	0	0	3530301964		NA		

Finger Enrollment Palm Enrollment Card Enrollment Capture Photo Signature Cafeteria

Reader Port: COM10 Card Type: MiFare Card Format: Default Format

Card Type: Card No.: Read Only Mode:

Enroll Verify Change Key

Personal Information

- User ID
- User Name
- Branch
- Department
- Designation

Finger Print Templates: No. of Templates: 0

Enroll as:  Card 1  Card 2

Enroll Abort

Smart Identification

- ASC GLOBAL
- FC Panel Lite-Device-8
- ID (Alpha-Numeric)
- PIN
- VIP
- Bypass Finger
- Validity Date
- Access Level

Emergency Contact

Blood Group

Medical History

Selected User Profile

User ID: 995  
Name: Henley

Browse

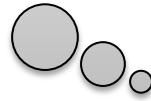
Enrolled Fingers: 0 Date of Joining  
Enrolled Palms: 0  
Department: Department-1  
Designation: Designation-1

Now After Enrolling the User from COSEC Enroll, without assigning the Device, Users are able to get access on it.





I will have to ensure that Enrollment has to be done from COSEC Enroll utility for those Users to whom Smart Identification is allowed.



For more information, contact  
Matrix Technical Training Team  
[Training@MatrixComSec.com](mailto:Training@MatrixComSec.com)

**Disclaimer:** The information contained in this e-mail and/or attachment may contain confidential or privileged information. Unauthorized use, disclosure or copying is strictly prohibited and may constitute unlawful act and can possibly attract legal action, civil and/or criminal. The contents of this message need not necessarily reflect or endorse the views of Matrix ComSec Pvt Ltd on any subject matter. Any action taken or omitted on this message is not entirely at your risk and the originator of this message nor does Matrix ComSec Pvt Ltd take any responsibility or liability towards the same. If you are not the intended recipient, please notify us immediately and permanently delete the message.