Matrix Technical Support Mailer – 46
Access Route using Smart Card

Dear Friends,

This technical mailer will throw the light upon newly added feature i.e. Access Route using Smart Cards. This feature is available from COSEC V05R04 versions and onwards.

This Access route functionality is available for Direct Doors (Version 2), Wireless Doors, PVR Doors and Panel Doors as well.

What is Access Route?

Sequence of devices defined in a route that an assigned user must follow in a particular order. On violation (of route), either user will be not be granted on succeeding devices (*Hard*) or if granted will give a message of rule being violated (*Soft*).

Why Access Route?

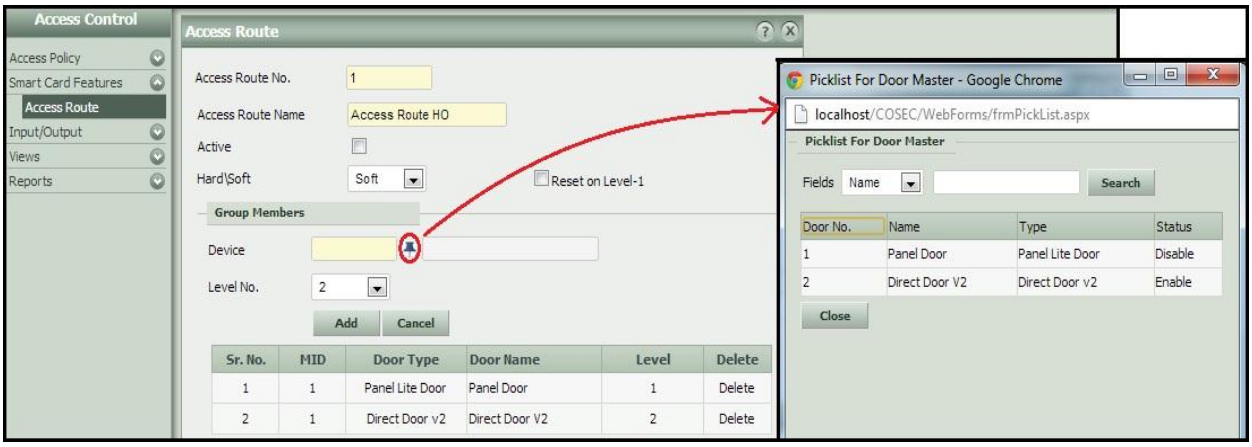
To protect the valuable assets of an organization, an administrator needs to keep an eye on every employees of that firm. This is not possible as man-power is always consumed and for Large Enterprises this is a non-practical task.

In such a scenario, if an employee tries to access certain premises where the entry for him/her is actually restricted, needs to show identity verification every time. Wrong Identity, Fraud IDs and Proxy entries are common things which can be failed to recognize. Here is the limitation.

This limitation can be overcome by the Access Route facility. Here, the Access Route allows the administrator to define an access policy which entails the user to access the COSEC Doors in the configured sequence. This restricts the users to stick to the specific Route where the entry is allowed and denying to every other device.

The COSEC system has the capability to define up to 75 Doors on a single route.

Go to Access Control → Smart Card Features → Access Route option in the left pane. The following Access Route window appears.

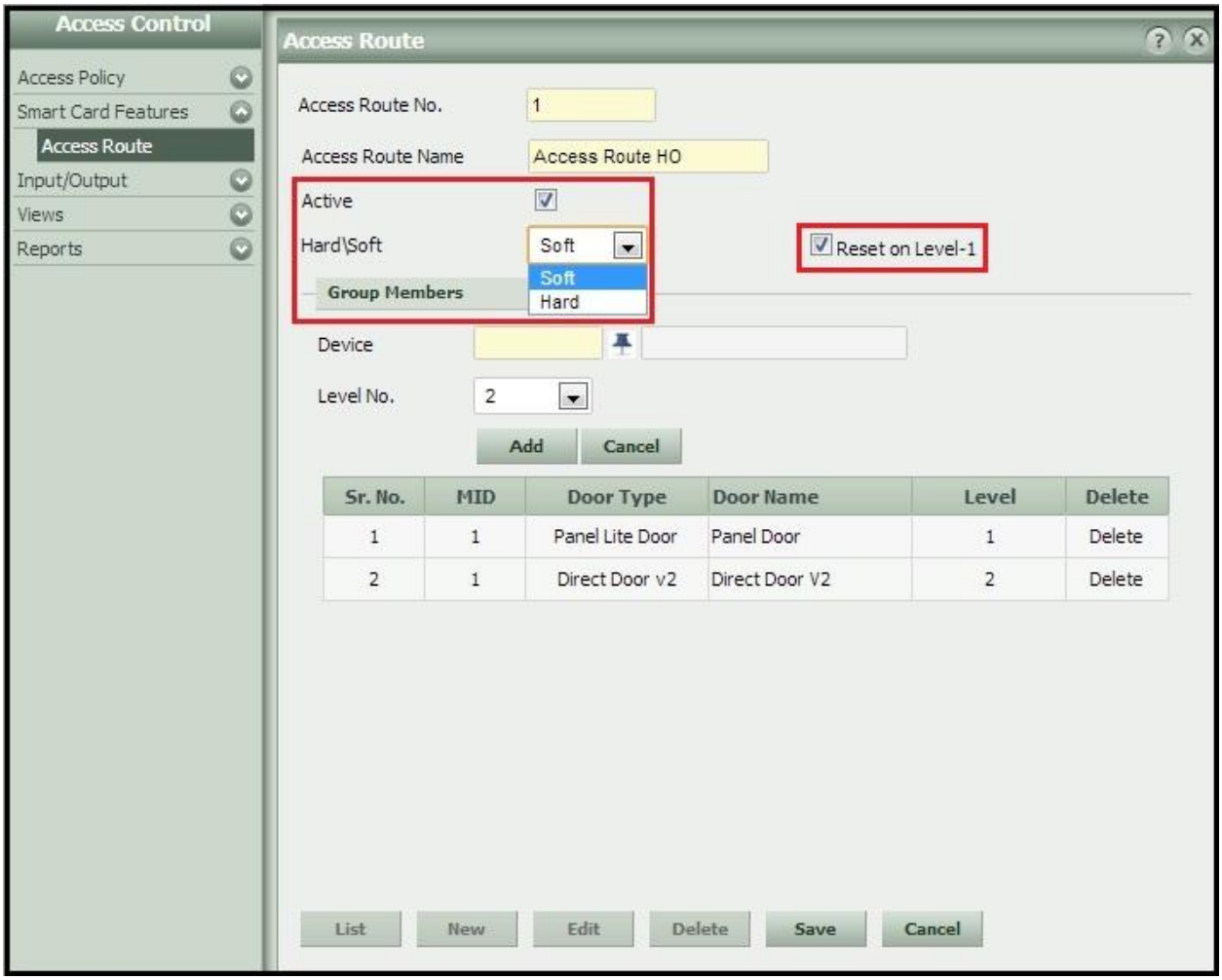


To define a new Access Route, click on Add New in the main Access Route window. The following window appears on your screen. The Access Route No. is system generated and cannot be edited by the user.

Specify a unique descriptive Access Route name and check the Active box to enable this functionality.

This functionality operates in two modes:
Hard: Access will be granted only if the access route is followed.
Soft: Access will be granted on any door on the access route with a access route violation message.

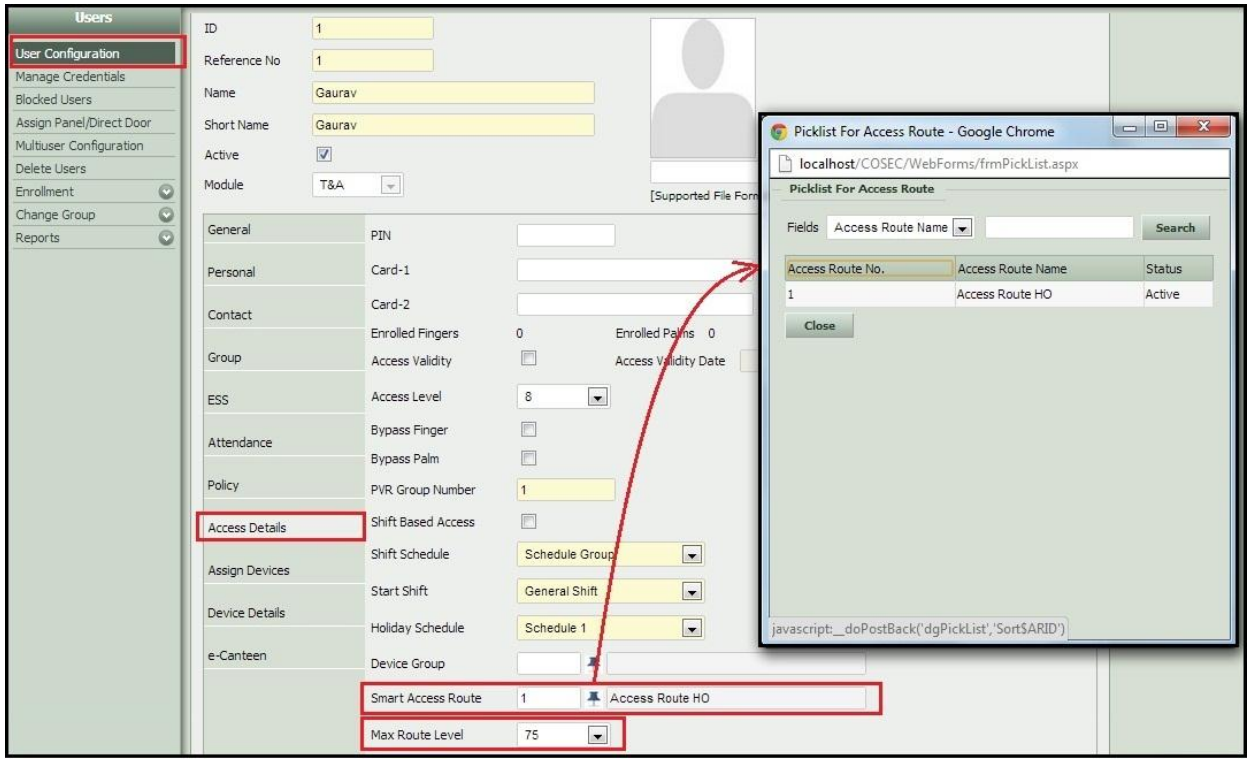
Reset on Level-1: In this case the Route will get reset if the Card is swapped again on device with Lowest Access Level.



In this case order has to be maintained for both entry as well as exit. Therefore it is necessary to have exit readers installed on all doors of the access route. Also, all the doors must have the Mifare reader as entry as well exit readers

Now user needs to define the Member Doors which would be part of the Access Route being defined. Click on the pick list button and select the appropriate Door from the pick list Pop-up window. Select the Level number for the Door from the pull down list. Multiple Doors can be assigned to a single level. However, the same door cannot be assigned to multiple levels.

The administrator can now assign the configured access routes to the users as explained below.



Go to Users → User Configuration → Access Details → Smart Access Route. Here, select the defined Smart Access Route to be assigned to the user. Also Select the Max Route Level for particular users to allow up to that access level.

Case Study:

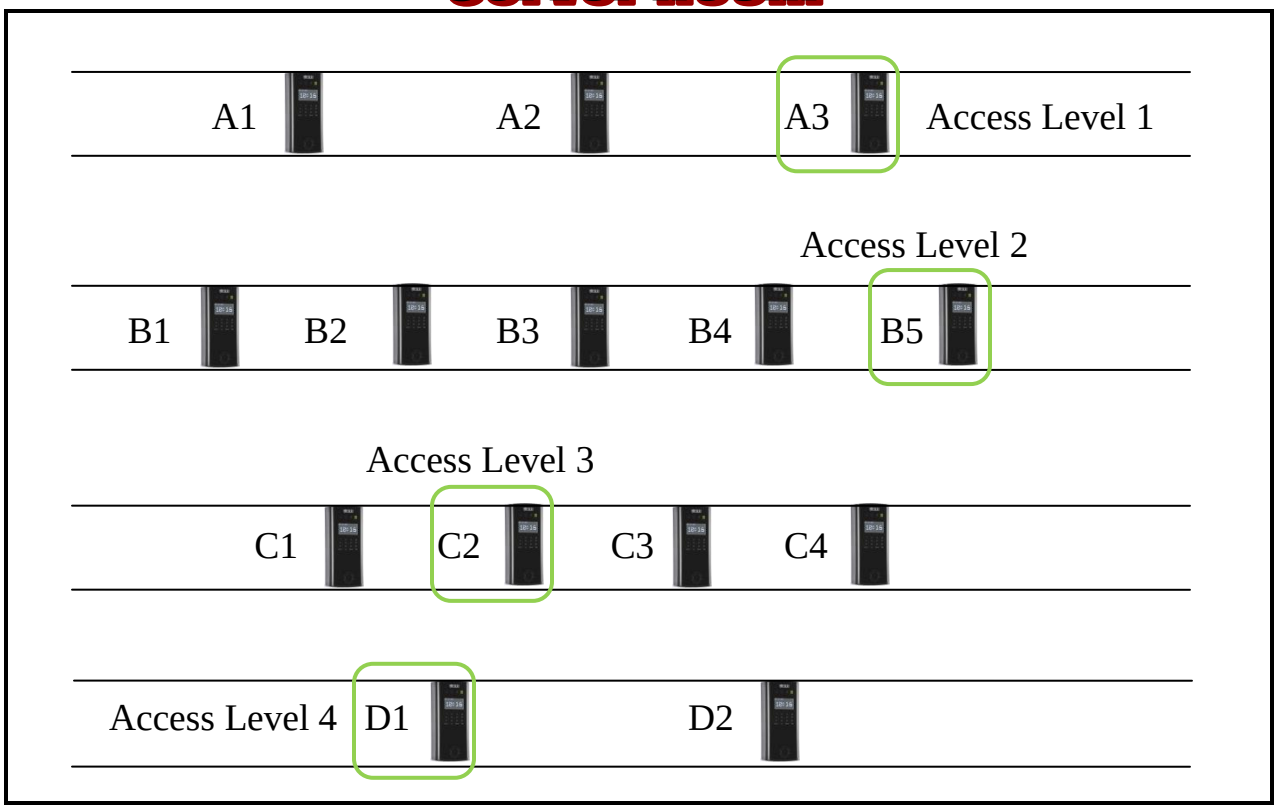
Let us consider the following scenario:

A1, A2, A3 – Ground Floor
B1, B2, B3, B4, B5 – First Floor
C1, C2, C3, C4 – Second Floor
D1, D2 – Third Floor

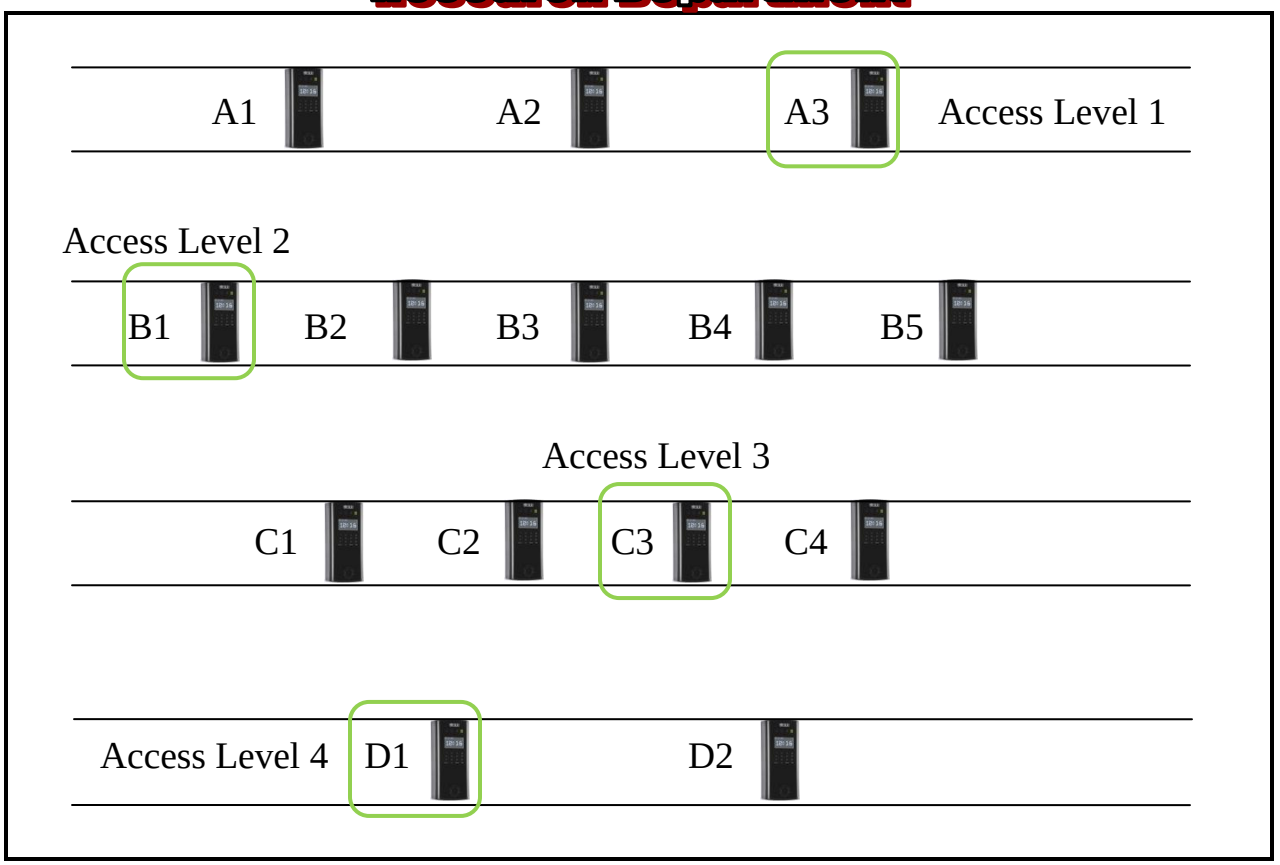
Server Room Route is defined in the order A3 → B5 → C2 → D1
Research Department Route is defined in the order A3 → B1 → C3 → D1

MATRIX
SECURITY SOLUTIONS

Server Room



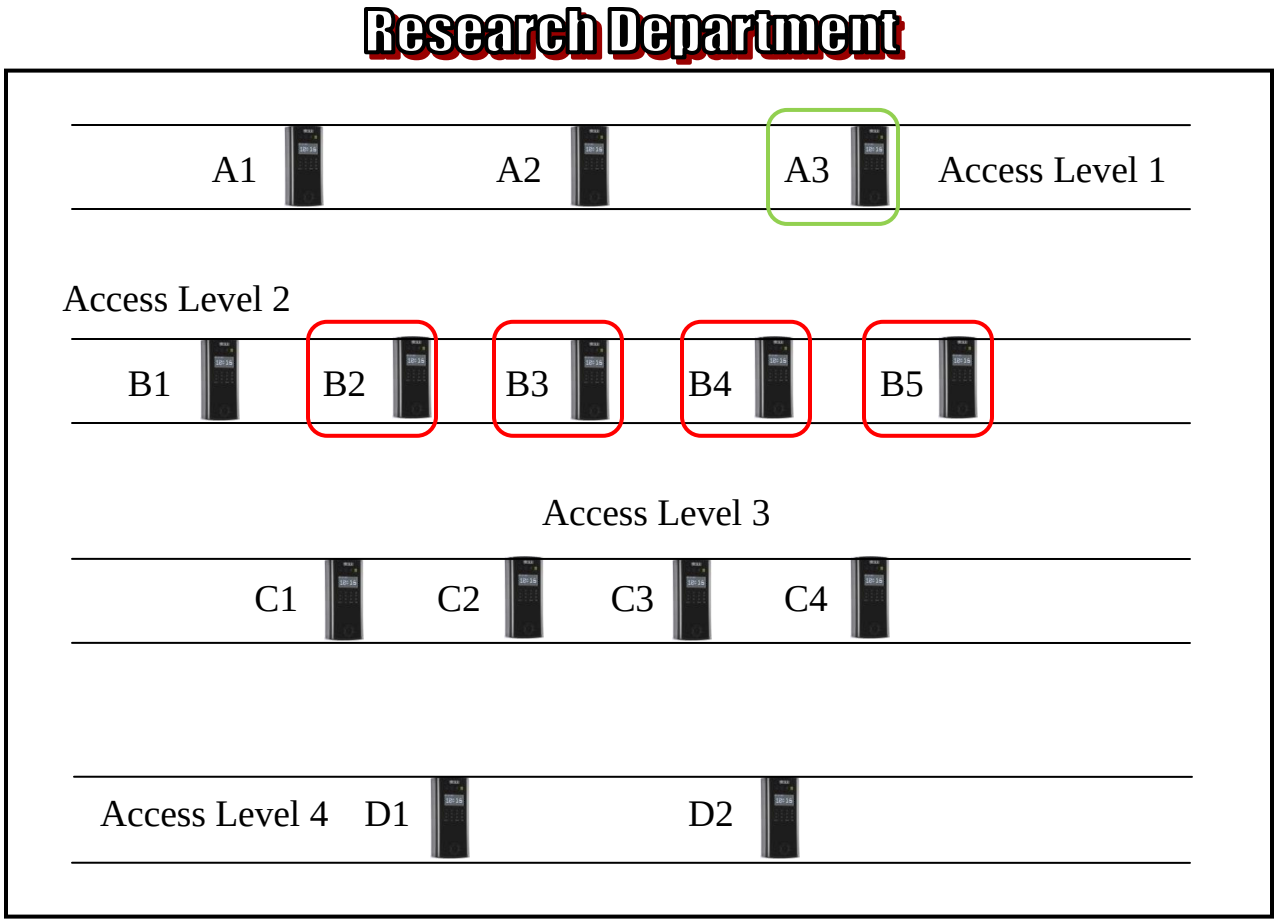
Research Department



The above are the two examples shown in the order from lowest access level to the higher level. To get pass through the particular route, users ought to follow the Access Routes Assigned to each one of them. In case of sequence break, the users will be denied to that particular device.

Note: Access Level to the devices can be assigned while defining the Access Route as explained above.

In Case of Access Route not being followed:



➔ It is shown above that once the access route is violated; the access won't be granted on that particular device.

➔ But this doesn't mean that Access Route details on the smart card will be erased. The former details will remain as it was. And the user will be allowed on coming back in the defined route.

Working:

Now when the access route is defined then route configurations will be sent to all the devices defined in the route along with Device ID and level of each device in route. Device in route will be having the information of all devices in the same route.

When a user shows his Smart Card on Door B5, it will read the last device id (Here A3 for respective routes 1 or 2) of device accessed by the user (Which is stored in the smart card).

Now the Access level read by the device, happens to be the Access Level greater than the Previous Level (In this case, Previous Access Level is Level 1 and the Next Access Level is Level 2, i.e. greater than previous one), the User will be allowed.

Note:

➔ *In case of Panel door if door is in degrade mode, user will get the access to that door by Facility Code written on the card but the ID of that device will not be updated to the card.*

➔ *If level checking/writing on the Smart Card is skipped, it will create conflicts for higher order doors as the level checking should be in sequence (i.e. from lower to higher). Thus user will not be allowed as the access route is violated.*

➔ *If the Panel door and the succeeding door are in the same level, the user will be allowed.*

Thanks & Regards,
Technical Support Team – Security Product
Matrix ComSec, Vadodara, India
E-mail: support@MatrixComsec.com