VistaKey Quick Start Guide

1. Hook up all equipment. Set rotary dial on Vistakey for the access point number 1-15. [page 3-4]

2. Map VistaKey Zones to panel zones Up to 4 zones per Vistakey unit), [page 3-2]
Enter *93 Zone Programming, map DSM, RTE, GP and DSMB zones for each VistaKey module.

DSM Zone(door status monitor) suggest ZONE TYPE= 01 or 03. Set INPUT TYPE= 11.
This is your door contact. Note: If the door is opened after an access grant, the entry delay will not begin, therefore ZT04 will not go into delay.

DSMB (DSM Backup) Set ZT same as DSM, INPUT TYPE = 06(set access point #). (Option)
This zone is active only if the Vistakey looses power. The Control uses a standard on board Vplex SIM to monitor status for security.
***Note: you must remove power from the Vistakey module to enroll this zone.

RTE Zone(request to exit) Any zone type or not used. Set INPUT TYPE = 12. (Optional)
The RTE zone DOES NOT need to be mapped to a vista zone for the RTE to function. You would only do this if you did not have a RTE device and you wanted to use this zone as another GP zone.

GP Zone(general purpose) Any zone type or not used. Set INPUT TYPE = 13. (Optional)
This may be a tamper, low bat monitor for the power supply, or a regular protection zone.

3. Setup Access Point Programming options for each VistaKey module, [page 5-13] (Optional)
In the #93 Menu Mode: Most of the defaults should be fine except that the zones default to normally open, we will usually use normally closed contacts. You may also want to change other parameters such as door unlock time, access groups who may access this door. etc…
Note: This is where you decide which access groups will have access to this point. You may not desire all card holders to access all points.

4. Test system by using [code] + #78. Select option 2: (grant all cards) [page 3-2] (Optional)
To exit test mode, go into #78 again and select option 0.
View the event log to verify operation.

5. Set up access groups [page5-18] (optional)
By default, the access group definitions should be OK for a basic system. One thing to change might be “Armed restriction”. By default, any card will have access AND disarm the system. If you want to restrict this, assign the card to an access group with partition armed restriction and either don’t assign it to a user code, or assign it to a user code with access schedule limitations.

6. Enable Access Groups (card groups need to be "turned on"). [page 6-3]
The easiest way is to do [code] #77. Select option 77, select all 8 access groups. This enables all access groups for 24-hour access. You may also want to limit access groups by a time schedule in *Time Driven Events*. [page 5-2 through 5-9]

7. Add cards using installer or master code + #79, [page 6-5]
Each card must be assigned to an access group that was enabled in step 3 above.
Cards will automatically disarm the partition the DSM is assigned to upon grant with no additional programming(see step 5 notes). You may assign additional event actions to cards or assign them to a user code for reference in the event log and Central station reports or to restrict by schedules.

8. Test full system.