

# ACCESS CONTROL DESIGN GUIDE



## **Architecture Overview**

Netgenium access control has been designed from the ground up as a network solution.

The network is used as the platform for communication between the security end points (lock controllers and readers) and PolicyServer, the central management platform.

The solution is designed around the ALK370x-IP family of lock controllers, Wiegand card readers, ABR2502-IP biometric reader and PolicyServer.

The rest of this document looks at the key considerations for physical deployment and network topology when deploying Netgenium access control.

## Access Control At The Door

### Managing the Power Budget

Netgenium network devices are powered from PoE. The ALK3701-IP, ALK3702-IP and the ALK3704-IP lock controllers provide a 12Vdc supply for external hardware, including locking devices and Wiegand readers.

When designing a solution it is important to plan for the limitations of supply that the IEEE standards dictate.

#### IEEE802.3af Power

Both the ALK3701-IP and the ALK3702-IP are designed to be used with IEEE802.3af. This provides a maximum of 800mA@12Vdc for external hardware.

The exact power budget will vary depending upon cable run, type and condition of lock etc. However, a typical door using a magnetic lock and 2 Wiegand readers would use:-

1 x Mag Lock	500mA
2 x Wiegand Readers	220mA

### **Using High Power Locks with IEEE802.3af**

Certain lock mechanisms require more power than IEEE802.3af can supply. Shear locks for example require in excess of 1A in-rush current. If the total power requirement at the door exceeds the budget available, clean contacts are provided to enable an external power supply to be used.

### **IEEE802.3at Power**

The ALK3704-IP is capable of using IEEE802.3af and the high power IEEE802.3at Power over Ethernet, providing 1.6A@12Vdc usable power at the door.

## **Locating the Lock Controller**

The lock controller is designed to be located at the door being protected, so a network outlet is all that is required for power and connectivity.

Door furniture (lock, request to exit, card reader(s) etc.) are the connected to the controller according to the installation manual.

## **Double Leaf Doors**

Where double leaf doors need to be secured, two locking mechanisms will be required.

If the power budget for the door is too high for IEEE802.3af the options available are:-

1. Install ALK3702-IP and ALK3701-IP wired in Master/Slave mode (two network outlets required).
2. Install ALK3704-IP with IEEE802.3at power source.
3. Use an external Power Supply to drive the locks and use 'clean contacts' of the controller to switch the power.

## **Fitting The Emergency Break Glass**

The Emergency Break Glass is used to allow exit from an area via a secured door in the event of an emergency.

To comply with fire regulations there must be a mechanical method of breaking the electrical supply to a locking mechanism in the event of an emergency.

If you have fitted a fail-safe locking mechanism, for example a magnetic lock, to a door. The Emergency Break Glass provides the mechanical means of breaking the supply.

If an Emergency Break Glass is not required, you must fit the hard wired loop as per the installation manual.

## **Automatic Doors And Barriers**

Use the 'clean contacts' of the lock controller to trigger automatic doors, gates and barriers.

## Network Design

### Managing the Power Budget

Power over Ethernet switches and mid-span hubs allocate power according to the end devices PoE classification.

You need to be aware of the total load each switch or mid-span is going to be expected to handle in your design and ensure this falls within the capabilities of the equipment.

**Remember!! A 24 port PoE switch may not be able to supply full power to every switch port.**

Every Netgenium lock controller is classified as a Class 3 device. Therefore the network switch will allocate 15.4W of power from its overall power budget regardless of the actual power drawn from the port.

### Network Topology

There are no specific network design requirements necessary. The system will work perfectly well on a flat layer 2 network.

However, allocating a separate security VLAN for controllers is recommended. This provides the network administrator the ability to restrict access to the end devices at the network layer.

### WAN Links

The Netgenium solution to physical access control is a real time application. When a user swipes to gain access to a door, the authentication event is processed by PolicyServer. This process relies upon the request to and response from PolicyServer being transported in a timely fashion.

Because of the latency and unpredictable response introduced by the slower connections it is not desirable to use the corporate WAN to transport transactions between end devices and PolicyServer.

## Using Biometrics

### Managing the Power Budget

Power over Ethernet switches and mid-span hubs allocate power according to the end devices PoE classification.

You need to be aware of the total load each switch or mid-span is going to be expected to handle in your design and ensure this falls within the capabilities of the equipment.

**Remember!! A 24 port PoE switch may not be able to supply full power to every switch port.**

Every Netgenium lock controller is classified as a Class 3 device. Therefore the network switch will allocate 15.4W of power from its overall power budget regardless of the actual power drawn from the port.

### Network Topology

There are no specific network design requirements necessary. The system will work perfectly well on a flat layer 2 network.

However, allocating a separate security VLAN for controllers is recommended. This provides the network administrator the ability to restrict access to the end devices at the network layer.

### WAN Links

The Netgenium solution to physical access control is a real time application. When a user swipes to gain access to a door, the authentication event is processed by PolicyServer. This process relies upon the request to and response from PolicyServer being transported in a timely fashion.

Because of the latency and unpredictable response introduced by the slower connections it is not desirable to use the corporate WAN to transport transactions between end devices and PolicyServer.