

VMS1000 Basic Information

Introduction

This contains the basic details for a VMS1000 system. Engineer training is an absolute must for the VMS 1000 system, particularly prior to the first installation.

System Documentation

It is critical that the integrator create and maintain a thorough record of the VMS system, without this support for the system is extremely difficult.

A typical system record would be an Excel sheet with at least the following information:

- IP address information of VMS1000 servers and clients. If ports are changed from defaults, then the ports also need to be logged.
- For cameras include IP addresses, MAC addresses, ports if not default, location, username, password.
- VMS1000 system camera number, title.

Default Passwords & IP Addresses

VMS1000 server	Redvision100
VMS1000 Admin	no password (blank)
VMS 1000 Server IP	DHCP

VMS1000 client PCs are shipped in the Dell default start up state, this is because each machine will need a specific user configuration to be set up before the VMS software can be installed.

VMS software is therefore not installed on clients but is included on every server in the path C:\Software\Digifort

The software can be copied to a USB stick and installed on each client.

When installing on client machines do not include the VMS1000 server application.

Admin and Surveillance Clients

All servers are shipped with the admin and surveillance software installed; both are programmed for local host 127.0.0.1

As soon as the server is allocated its IP address then the server details in the admin client need to be changed from the local host address to the servers allocated IP address. This is also true for the surveillance client.

Admin Password

Ensure that the admin password is changed before any programming is done. Changing the admin password after some features have been set up (such as master / slave) will stop working and cause confusion.

Always log the admin password as losing it will cause issues as written request is needed along with remote access to the server for it to be cleared.

Windows Firewalls

The servers are shipped with the Windows firewall turned off for all options. This is done to avoid connectivity issues which can occur due to the firewall being active. Once the system is working and tested then you can turn the firewalls on and allow the required ports through.

Normally only the server port is needed but all possible ports are listed below.

VMS1000 server	8600
VMS1000 API	8601
Https	443
VA Server	8610
LPR Server	8611
Mobile Camera Server	8650
Mobile Camera Streams	8652
Web Server	8000
RTSP Server	554

Anti-Virus Software

Antivirus software can play havoc with any VMS because there are so many uncommanded tasks taking place, particularly on client machines.

If anti-virus software is installed then it must allow all VMS1000 activities, many programs allow exceptions such as this.

Servers are shipped with Windows Defender disabled.

Technical Support

Basic technical support queries can be handled over the phone and email, for any in depth help a remote connection to the system is required.

Diagnosis via a remote connection allows any issues to be clearly seen and saves a huge amount of time and is a must.

Full pdf manuals are available and they contain clear and concise information regarding both server and client setup.