ADAM Systems
Dealer Infrastructure Guidelines

2017

V17

Section 1: Guidelines Summary & Notes
Section 2: Dealer IT Guidelines

Section 1: Guidelines Summary & Notes

ADAM System has adopted these infrastructure guidelines for dealership's internal network environment to ensure optimal performance and reliability. These guidelines are designed to ensure a seamless and reliable end-user experience within the ADAM System's DMS. Following these guidelines should ensure a reliable, high quality end-user experience across all the dealership's software solutions.

The infrastructure guidelines are organized as follows:

- **Recommended** – the systems infrastructure components that will deliver performance and security while seeking to maximize the lifecycle of the investment. If you are looking to purchase new systems, please adhere to or exceed the specifications outlined in the "recommended" section.

- **Minimum** – the lowest acceptable systems infrastructure for conducting business with ADAM Systems

The recommended and minimum guidelines apply to Peer-to-Peer, Client / Server, Remote Desktop, and Xcelerate Cloud Platform deployments. Specific, detailed information appears in each section of the document.

Please Note the Following:

Dealerships utilizing dot matrix forms must **ONLY** use an Okidata Microline 321 Turbo or Okidata ML421.

ADAM Systems estimates the life cycle of a Server, Desktop PC, Laptop or Tablet PC on average is three (3) years.

The following applies to all ADAM System application deployments (Xcelerate Cloud Platform, Remote Desktop, Client / Server, Peer-to-Peer). It is important to note that ADAM System may integrate with other solutions that operate on unsupported hardware. Approved integrations between ADAM Systems and 3rd party solutions will function as designed.

Supported	Not Supported
Windows 10 Professional	Tablets running Android or Mac operating systems
Windows 8 or 8.1 Professional	Windows XP or XP Mode / Virtual PC
Windows 7 Professional	Any Home version of operating system
Window 2008 Server or Higher	Essentials versions of Windows Server

ADAM Systems highly encourages dealers to have a disaster recovery plan. Disasters range in severity and natural disaster threats vary from region to region. Each dealership should consider their own possible risk factors. We recommend the following be on every dealership's disaster recovery checklist:

- Secure data storage
- Regular nightly backups (local and offsite)
- Regular image backups of the application
- Regular image backups of the application server
- Computer viruses
- Security data breech / Data theft
- Fire
- Power failures (At a minimum, a UPS Battery Backup System should be deployed for your application server)
- Natural disasters (Flood, wildfire, hurricane, tornado, snowstorm, earthquake, electrical storms, pandemic, tsunami)

This is not a complete disaster recovery checklist. There are many factors to consider when developing a disaster recovery plan. It is important to remember that disaster recovery is not isolated to the realm of data. The whole idea of disaster recovery is business continuity, including personnel, vendors, clients, communication, sales, and data.

Section 2: Dealer IT Guidelines

DESKTOP PC/LAPTOP

DESKTOP PC/Laptop Recommended: **Guidelines for purchasing new hardware**	
System Memory (RAM)	8 GB or more
Hard Disk Drive	320 GB or more
CD / DVD Drive	CD/DVD Combo
Serial Port	May be required for peripheral compatibility
USB Ports	2 or more***
Network Adapter	1000Mbps Optional wireless WAN802.11g
Warranty	3 year onsite
Operating System	Windows 10 Professional, 32 bit or 64 bit
Printer	Networked Laser Printer

*** Note: For backup and support purposes, a dealership should purchase a USB drive to have on hand. The USB drive should be USB 2.0 or higher compliant flash drive with at least 12GB of free space.

The following provides what ADAM Systems considers the minimum requirements to run dealership applications. Do not reference the minimum specification when purchasing a new PC, but rather use it as a comparison for hardware being transitioned from one department to another.

Minimum: **Do Not Reference For New Hardware Purchase**	
System Memory (RAM)	4 GB
Hard Disk Drive	160 GB
CD / DVD Drive	CD / DVD Combo
Serial Port	1
USB Ports	2
Network Adapter	100 Mbps
Operating System	Windows 7 Professional SP1, 32 bit or 64 bit
Printer	Laser Printer

ADAM Systems does not support Windows XP Mode / Windows Virtual PC on Windows 7 Professional.

TABLET PC

Tablet PC Recommended: **Guidelines for purchasing new hardware**	
System Memory (RAM)	4 GB or more
Hard Disk Drive	320 GB or more
CD / DVD Drive	CD/DVD Combo
USB Ports	2 or more***
Audio Adapter	16 Bit
Audio Speaker	Recommended
Video	1024 x 768 resolution or greater, 32 bit color, 128 MB video memory
Network Adapter	Ethernet based 100Mbps

	Optional wireless WAN802.11g
Warranty	3 year onsite
Operating System	Windows 10 Professional, 32 bit or 64 bit

Notes:

- It is important to understand that your core ADAM DMS applications are not designed to be used with a touch interface and may not function properly using a touch device. Some 3rd party applications that integrate with your ADAM DMS are specifically developed to run on certain tablet devices, such as iPads. When these applications are deployed, any approved ADAM Systems integrations will communicate with those devices and applications for their intended use.
- Based on the evolving technology in the mobile space, the compatibility of certain programs may be limited to specific tablets and/or mobile device operating system version.

REMOTE DESKTOP SERVER

Server Requirements up to 25 users (over 25, please call ADAM Support) **Recommended:** **Guidelines for purchasing new hardware**	
Processor	Server Grade Processor
System Memory (RAM)	24 GB or more
Hard Disk Drive	4 – 8 500GB 10K HDDs (in pairs)
RAID Configuration	Raid 10 with RAID Controller
Hard Disk Configuration	Separate storage volume of at least 100GB is required for ADAM DMS suite
CD / DVD Drive	CD/DVD Combo
USB Ports	2 or more***
Network Adapter	1000Mbps or greater Network Speed Should be 1000Mbps
Warranty	3 year onsite
Operating System	Windows 2012 R2 Standard Edition****
Microsoft Server User CALs	CALs can be device or user
Microsoft Server Remote Desktop CALs	CALs can be device or user
UPS Battery Backup System	Recommended for server
Printer	Networked Laser Printers

**Note: Depending on the scope of use and number of users an additional processor may be required to optimize application performance

*** Note: For backup and support purposes, a dealership should purchase a USB drive to have on hand. The USB drive should be USB 2.0 or higher compliant flash drive with at least 12GB of free space.

**** Note: Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2, and Windows 2016 are the only ADAM supported server operating systems. If you have any questions regarding supported server operating systems, please call the ADAM Customer Care Team.

CLIENT / SERVER – SERVER

CLIENT / SERVER DEPLOYMENT IS NOT TO BE USED IN FRANCHISED DEALERSHIPS OR IN DEALERSHIPS WITH MORE THAN 5 USERS

Server Requirements up to 5 users (over 5 users requires Remote Desktop or Xcelerate Cloud Platform) **Recommended:** **Guidelines for purchasing new hardware**	
Processor	Server Grade Processor
System Memory (RAM)	8 GB or more
Hard Disk Drive	3 – 8 500GB 7.2 HDDs (minimum of 3)
RAID Configuration	Raid 5 with integrated RAID Controller
Hard Disk Configuration	Separate storage volume of at least 50GB is required for ADAM DMS suite
CD / DVD Drive	CD/DVD Combo
USB Ports	2 or more**
Network Adapter	1000Mbps Network Speed Should be 1000Mbps
Warranty	3 year onsite
Operating System	Windows 2012 R2 Standard Edition***
Microsoft Server User CALs	CALs can be device or user
Microsoft Server Remote Desktop CALs	Not required in Client / Server deployment
UPS Battery Backup System	Recommended for server
Printer	Networked Laser Printers

** Note: For backup and support purposes, a dealership should purchase a USB drive to have on hand. The USB drive should be USB 2.0 or higher compliant flash drive with at least 12GB of free space.

*** Note: Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2, and Windows 2016 are the only ADAM supported server operating systems. If you have any questions regarding supported server operating systems, please call the ADAM Customer Care Team.

RECOMMENDED PC SOFTWARE

Recommended:	
Word Processing	MS Office or Open Office
Spreadsheets	MS Office or Open Office
Presentation	MS Office or Open Office
Web Browser	Internet Explorer, version IE9 or higher (with current Service Pack) and the "compatibility view" enabled
Java	Current 32-bit version of Java J2SE™ Runtime Environment
Reader	Current version of Adobe Reader
System Recovery	Full Operating System Recovery Package, Ensure the PC manufacturer or reseller provides the necessary recovery software to restore the operating system in the event of a major software failure.
Desktop Anti-Virus	Enterprise Desktop Anti-virus solution that is updated automatically and managed through a centralized console.

LOCAL AREA NETWORK (LAN) CONFIGURATION

Local Area Network	Ethernet based 100/1000Mbps
Data Cabling	Category 5e
Equipment Location	LAN wiring should terminate, and equipment should be housed, in a wiring closet or communications room
IP Addressing	Dynamic addressing (DHCP) should be used to ease support
Network Adapter	100/1000Mbps
Traffic Switching	Managed switch
Routers	Business-grade router
Firewall	**Port 8010 should be open and forwarded to the application server for all ADAM Factory and API communications (IP range can be provided upon request).** Also reference network data security on page 10

MINIMUM INTERNET BANDWIDTH

DEALER NETWORK SIZE	GUIDELINE
SMALL (under 10 PCs)	**10.0 Mbps download (total bandwidth), 1.0 Mbps upload**
MEDIUM (11 - 24 PCs)	**20.0 Mbps download (total bandwidth), 3.0 Mbps upload**
LARGE (Over 25 PCs)	**40.0 Mbps download (total bandwidth), 5.0 Mbps upload**

Note: ADAM Systems recommends that dealerships also maintain on-demand backup Internet connectivity. ADAM Systems recommends a backup or failover circuit in the event your primary goes down or if you choose to balance your traffic over two connections to streamline efficiency. When considering a backup connection, it is wise to make sure it comes from not only a different provider, but from a different backbone, as well. As a possible solution, ADAM Systems recommends 3G or 4G wireless as a reliable secondary failover connection.

Internet Notes

- Inefficient bandwidth may result in unreliable or slow performance and may negatively affect ADAM DMS application's speed and functionality.
- Internet speed and performance can be greatly impacted by virus, spyware and malware malicious infiltrations.
- Bandwidth-dependent activities not related to dealer/ADAM Systems communications can greatly impact Internet performance as well. Examples of these activities are non-business Internet usage, i.e. video/audio downloads/uploads, gaming, file-sharing, etc.
- Factory communication requirements can also utilize significant amounts of bandwidth. Each dealer solution should consider the overall Internet utilization requirements for each area of the dealership. Additionally, dealers should develop Internet usage Guidelines for their employees that address non-dealership business Internet usage.

WIRELESS NETWORK

Note: When utilizing wireless networks, follow security Guidelines below. Wireless networks must be segmented from the dealership's wired LAN to protect customer data. **ADAM DMS applications should not use the wireless network.**

Recommended: **Guidelines for implementing new systems**	
Network Standard	WPA2 Enterprise, 802.11N with RADIUS authentication
Authentication & Encryption	WPA2 Enterprise, 802.11N with RADIUS authentication and AES Encryption
Coverage / Access Points	Wi-Fi should be accessible within the entire dealership footprint (including lot)

Minimum: **Lowest Acceptable Infrastructure for systems already in use at the dealership**	
Network Standard	WPA2 PSK Compliant
Authentication & Encryption	WPA2 Authentication w/ AES Encryption
Coverage / Access Points	Wi-Fi should be accessible within the entire dealership footprint (including customer lot)

Wireless Access Points:

Dealerships who choose to deploy wireless networks should use business grade access points only. Small Office/ Home Office equipment should not be deployed. All access points must adhere to the Guidelines specifications above.

Rogue Wireless Detection:

- Scan, identify, and remove any rogue wireless access points that may be on the dealerships network. A rogue wireless access point is defined as a wireless point of entry into the dealership network that has is not authorized, secured, or known about by dealer IT, management, and ownership. Any rogue wireless networks must be detected, found, and removed immediately.

SECURITY

PC Virus Monitoring

Enterprise-grade anti-virus products should be installed on all PCs and configured to automatically perform the following:

- Download and install most current virus signature updates
- Actively monitor for viruses
- Quarantine and eradicate infected files
- ADAM DMS applications and data directories should be excluded from any active real-time scans for performance reasons

Disaster or Attack Recovery

Essential dealership data should be backed up and verified regularly, using a backup utility or service that has the following capabilities:

- Offsite secured storage of media
- Regular daily backups
- ADAM Systems offers an optional offsite managed backup solution for your ADAM DMS data. Call for more information.

Data Network Security

Comply with all federal, state, local, and industry regulations for financial institutions, such as GLBA, PCI, etc.

Designate an employee (dealer direct possibly your PSC) to be in charge of security policies, procedures, and FTC required paperwork. The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions regularly perform a Risk Assessment to identify foreseeable risks.

Security Information and Event Management: Proactive, real-time event monitoring that utilizes a SIEM (Security Information and Event Management) service. SIEM needs to be able to collect data with capability to aggregate and correlate varying security data from the network in real-time. The SIEM service provider needs to be able to notify the network administrator in the case of a security event, as well as provide the proper documentation for compliance purposes. The ultimate purpose of a SIEM service is to aid in identifying or preventing an intrusion into your network. Immediate response to a breach can greatly reduce or prevent data loss.

Note: Reactive management software (i.e. Desktop firewall or antivirus) is not to be confused with a proactive SIEM service.

Data Network Security (continued)

Implement comprehensive security measures that include:

- Fully-managed security device that continually monitors threats through Intrusion Detection System "IDS" and Intrusion Prevention System "IPS" and other mechanisms. The fully-managed security device should include the functionality listed below.
    - Filter packets and protocols
    - Antivirus Scanning
    - Perform stateful inspection of connections
    - Perform proxy operations on selected applications
    - Report traffic allowed and denied by the security device on a regular basis (i.e. monthly)
- The security device should be able to filter packets based on the following characteristics:
    - *Protocol, e.g. IP, ICMP
    - Source and destination IP addresses
    - Source and destination ports
    - The appliance should perform real-time scanning of HTTP, SMTP, and FTP traffic for malware, spy ware, and other intrusions.
    - In addition, ADAM Systems recommends web filtering and monitoring websites visited to block inappropriate or entertainment orientated websites that are the most dangerous source for inadvertently downloading malicious programs.
- Timely, customized reporting on (IDS and IPS) activity
- Respond to all identified threats (form reporting) immediately.
- Protect each PC with unique passwords and a corporate anti-virus solution.
- ADAM Systems recommends annual internal and external penetration testing of the dealer network. A penetration test ("pen test") is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. A penetration test should be performed on any computer system that is to be deployed in a networked environment, in particular those with any Internet facing or exposed system. Penetration testing engagements can be performed externally (simulation of an attack from outside of your network, and exactly like having a hacking attempt launched from a foreign country), or it may be performed internally (from within your network to see what access and vulnerabilities exist).

For additional information on Network Security, please reference the following resources that provide industry laws, Standards, and recommendations:

PCI Security Standards: https://www.pcisecuritystandards.org
Gramm-Leach-Bliley Act: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
STAR Standard: http://www.starstandard.org/

A Dealership's Owner(s), not ADAM Systems, are ultimately responsible for determining their own network infrastructure, security, and network configuration.