STAR Dealer Infrastructure Guidelines
Quick Reference Guide
2020

Contents

Introduction

Overview

This short reference document that is intended to be paired with the STAR Dealer Infrastructure Guidelines (DIG). Please refer to the STAR DIG for more information on any topic outlined in this reference guide.

Disclaimer

Any company name, application, website link, or technology reference mentioned in this document should not be considered an endorsement by the OEMs or by STAR unless that endorsement is expressly stated.

This document provides a basic specification or guideline for dealers to establish Internet communication. It is important to note that network infrastructure, dealer data, and system security is the dealership's responsibility. Third-party organizations such as service providers and partners may provide guidance and recommendations. Some organizations may provide software, hardware, or proprietary network elements to help streamline network operations. However, these applications, recommendations, or tools are not a substitute for network management.

Hardware Recommendations

Desktop PCs	
Component	**Specifications**
Processor	Intel Core i5 and above, or AMD equivalent
Memory (RAM)	4 GB or more
Hard Disk Drive	500 GB or more
CD/DVD Drive	CD/DVD combo, or external drive
Serial Port	1 (Optional USB adapter)
USB Ports	2 or more
Audio Adapter	16 bit
Audio Speaker	Optional
Display	1280x768 minimum resolution
Network Adapter	Wired: Gigabit (or greater) Ethernet Wireless: 802.11 n or ac
Warranty	3 year on site
Operating System	Windows Operating Systems are compatible with most dealership applications. Please see your OEM and technology partners when choosing an operating system.

Laptops	
Component	**Specifications**
Processor	Intel Core i5 and above, or AMD equivalent
Memory (RAM)	4 GB or More
Hard Disk Drive	320 GB or more
CD/ DVD Drive	CD/DVD combo, or external drive
USB Ports	2
Audio Speaker	Optional
Display	1280x768 minimum resolution
Network Adapter	Wired: Gigabit (or greater) Ethernet Wireless: 802.11 n or ac
Warranty	3 year on site
Operating System	Windows Operating Systems are compatible with most dealership applications. Please see your OEM and technology partners when choosing an operating system.

Routers & Switches	
Component	**Specifications**
Ethernet Standard Specification	IEEE 802.3 100baseT or 1000baseT
Redundancy	The connection of multiple switches together should use redundant links of the highest speed available, using STP or rSTP to ensure a loop-free topology.
Power Supply	Redundant power supplies are recommended to reduce downtime.
Speed	100 or 1000 Mbps
VLAN	Switches with VLAN and 802.1Q trunk technology should be used for routed networks with multiple subnets or VLANs.
Management Protocols	Managed devices should support industry remote management standards such as Simple Network Management Protocol (SNMP) and Remote Network Monitoring (RMON).
Wireless Switches	Wireless devices should be dual band and IEEE 802.11b/g/n compatible.

For more information on dealership hardware recommendations, please see section 2.2 of the STAR Dealer Infrastructure Guideline (DIG)

Software Recommendations

Operating Systems

Below is a list of the most common operating systems in the market today. Some applications are not compatible with specific operating systems. It is recommended that dealers check with their OEMs, DSPs, and other vendors to determine which operating systems to use. Please note, as of April of 2014, Microsoft ended support for XP operating systems. This includes critical security updates. STAR recommends dealerships do not use Windows XP.

Current Common Client Operating Systems	Latest update or service pack*	End of mainstream support	End of extended support
Windows XP	Service Pack 3	14-Apr-09	8-Apr-14
Windows Vista	Service Pack 2	10-Apr-12	11-Apr-17
Windows 7	Service Pack 1	13-Jan-15	14-Jan-20
Windows 8	Windows 8.1	9-Jan-18	10-Jan-23
Windows 10,	N/A	13-Oct-20	14-Oct-25
MAC OS X	10.9 (or higher supported) 10.11	Versions 10.8 (Mountain Lion) and below no longer supported.	Versions 10.8 (Mountain Lion) and below no longer supported.
IOS (for iPad and iPhone)	9.1		
Android	5		

Latest updates/service pack as of November 2015

Internet Browsers

Below is a list of the most common internet browsers in the market today. Some applications are not compatible with specific browsers. Other applications require specific browser settings, such as compatibility mode. It is recommended that dealers check with their OEMs, DSPs, and other vendors to determine which operating systems to use.

Latest updates/service pack as of January 2019

Browser	Latest update or service pack*	Notes
Google Chrome	71	
Mozilla Firefox	64	
Internet Explorer	11	
Apple Safari	12	Not recommended for use on Microsoft Operating systems
Opera	57	
Edge	18	

For more information on dealership software recommendations, please see section 2.3 of the STAR Dealer Infrastructure Guideline (DIG)

Network Configuration & Management

	LAN Specifications
Local Area Network	Gigabit Ethernet
Data Cabling	Existing data network cabling should be - at a minimum - TIA-568-A Category 5e standards. Category 6a should be used for new cabling. No horizontal cable runs should exceed 90 meters (295 feet). Fiber optic cable is highly recommended in place of data cable runs when the length exceeds 295 feet.
Equipment Location	LAN equipment should be housed in a wiring closet or communications room. All equipment should be mounted or secured to a rack or shelf.
IP Addressing	Dealership ISP should provide routable IP addressing. For the dealer LAN, dynamic addressing (DHCP) should be used to ease support.
Network Adapter	Gigabit Ethernet
Ethernet Switching	Gigabit Managed Switch. Label each interface and cable. This will save time when tracking back network cables for support or new installation.
Routers	Business-grade router. Routers should support Network Address Translation/Process Analytical Technology (NAT/PAT). Routers should also support dynamic routing using RIPv2, OSPF and BGP. - Change the device password at the time of installation and on an ongoing, regular basis. - Keep backup configuration on file in the case of a software failure or hardware replacement.
Firewall	A fully-managed security device that continually monitors threats through Intrusion Detection System “IDS” and Intrusion Prevention System “IPS” and other mechanisms such as packet filtering, antivirus, and stateful packet inspection. - Firewalls should support Network Address Translation/Process Analytical Technology (NAT/PAT). Firewalls should also support dynamic routing using RIPv2, OSPF and BGP. - Change the device password at the time of installation and on an ongoing, regular basis. - Keep backup configuration on file in the case of a software failure or hardware replacement. - For more information on firewalls and network security see section 2.6.
Domain Name Services (DNS)	Use public DNS except when using Windows Active Directory. (In which case, having an internal DNS server is required.)

Wireless Networking Design	
Recommendation	**Specification**
Wireless Hardware	Only enterprise-grade access points should be used. Enterprise grade access points are designed to provide roaming and other business class features (such as VLANs and/or multiple SSIDs) necessary to support the wireless devices for applications. Business grade wireless access points are also designed to accommodate a higher number of connections than consumer-grade hardware.
Network Segmentation	Dealerships must ensure guest traffic is segmented from the dealership network through VLANs or a separate internet connection.
SSIDs	Dealerships are recommended to use separate SSIDs for different business functions (i.e. sales, service, and administration). However, dealerships should not confuse SSIDs with network segmentation. SSIDs generally do not separate network traffic, but only provide a different way to join the network.
Coverage	Deploy wireless access points to ensure adequate coverage. Wireless tools can provide signal strength around the building. Be aware of structures or objects that can interfere with wireless coverage (electrical interference, radio frequency interference, or physical materials such as metals or concrete).
Authentication & Encryption	WPA2 with RADIUS authentication and AES Encryption
Network standard	802.11n or 802.11ac
Rogue Wireless Detection	Scan, identify and remove any rogue wireless access points that may be on the dealership's network. -A rogue wireless access point is defined as a wireless point of entry into the dealership's network that has not been authorized or secured by the dealer, IT management, and ownership. -All rogue wireless networks must be detected, found, and removed immediately. -STAR recommends the use of a managed wireless detection service that is continuously scanning the network for wireless threats.

Dealership Mobility	
Recommendations	**Specification**
Mobility within the dealership	Utilize a wireless mesh network to ensure end users can navigate around the location without losing connection or authenticating again.
Wireless controllers	A wireless LAN controller can be used in combination with the Lightweight Access Point Protocol (LWAPP) to manage lightweight access points across the dealership network. This will help to ensure adequate coverage, reliability, and network efficiency.

Customer Access	
Recommendations	**Specification**
Traffic Prioritization	Dealerships should utilize a firewall or other mechanism to limit guest bandwidth consumption. This will prevent guest access from interfering with business operations by consuming too much bandwidth.
Guest Authentication/ Terms of use	STAR recommends dealerships utilize a captive portal requiring guests to accept terms and conditions of use at the dealership. This can include content restrictions, bandwidth limitations, and usage agreements.
Internet Bandwidth	To ensure the dealership has enough bandwidth, a dealer must choose the right technology and speed. (See Section 2.5a and 2.5b in the STAR DIG for more information on technologies and internet bandwidth.) -STAR also recommends every dealership have a backup ISP connection from a different provider, using a different technology. -See section 2.5c for recommendations on internet backup connections.

For more information on network configuration and management, please see section 2.4 of the STAR Dealer Infrastructure Guideline (DIG)

Security

	Network Security
Firewall/ UTM	A fully-managed security device that continually monitors threats through Intrusion Detection system "IDS" and Intrusion Prevention System "IPS" and other mechanisms. The device should also have the following features: • Mechanisms such as packet filtering, antivirus, and stateful packet inspection. • Filter packets and protocols (e.g. IP, ICMP) • 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)
Network Segmentation	Payment Card information, customer information, dealership traffic, and customer traffic should be segmented via network segmentation (such as VLAN) or a different network (such as a dedicated circuit for guests) to ensure data security.
Content Filtering	Data loss can stem from employees surfing the web for non-business related activities. STAR recommends dealerships filter content on the network to remove potential harmful, inappropriate, or other non-business related traffic.
SIEM	Proactive, real-time event monitoring that utilizes a SIEM 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.
Wireless Detection System	Scan, identify, and remove any rogue wireless access points that may be on the retailer 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. ○ All rogue wireless networks must be detected, found, and removed immediately. ○ STAR recommends the use of a managed wireless detection service that is continuously scanning the network for wireless threats.
Penetration Testing and Vulnerability Scanning	Annual internal and external penetration testing of the dealer network is highly recommended. 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).

Recommendation	Desktop Security
PC Virus Monitoring	Enterprise-grade, antivirus 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 • Antivirus solution should include antivirus, anti-spyware, intrusion prevention, application control, spam control and rootkit detection
Patch Management	STAR recommends that patch management be performed on every PC to ensure each workstation has current Microsoft patches. Workstation Management should include remote monitoring of hardware/software failures, down servers, low disk space, excessive CPU usage and excessive memory usage.
Password Protection	Passwords should be set to expire every 60 days, or less. At a minimum, dealerships should use "strong passwords" containing an 8-character minimum comprised of 3 of the following 4 requirements: 1) Uppercase 2) Lowercase 3) Numeric 4) Special characters.

Endpoint Detection and Response	Enterprise-grade Endpoint Detection and Response service should be installed on all endpoints and critical servers. The service offering should provide cross-platform visibility into endpoint/server activities. The solution should be able to provide: • Threat Detection through static and behavioral AI engines and HIDS within the endpoint agent • Threat Containment and Remediation Guidance • Activity Reporting and Threat Hunting • Cross Platform visibility into process execution, network communications, file access, applications, DNS requests and encrypted web traffic

For more information on dealership security recommendations, please see section 2.6 of the STAR Dealer Infrastructure Guideline (DIG)