



STAR Dealer Infrastructure Guidelines
Quick Reference Guide
2024

Contents

Introduction 2

 Overview 2

 Disclaimer 2

Hardware Recommendations 2

 Desktops, Laptops, and Tablets 2

Software Recommendations 3

 Operating Systems 3

 Internet Browsers 4

Network Configuration & Management 5

LAN Specifications 5

Wireless Networking Design 6

Dealership Mobility 7

Customer Access 7

Security 8

 Network Security 8

 Desktop Security 9

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

Desktops, Laptops, and Tablets

STAR recommendations for dealership desktop, laptop, and tablets have shifted away from broad hardware specifications. This is based primarily because of advancements in hardware processing power, the shift to cloud computing, and the ubiquity of mobility. STAR recommends hardware needs be determined on a use case scenario based on job function. When purchasing new devices, take the following factors into consideration:

- 1. Mobility:** Some functions within a dealership require mobility. Other job functions occur primarily at one physical location. Consider needs for mobility when purchasing a new device. Also remember that many mobile devices, such as tablets, run on specific software that may not be compatible with all needed hardware and software. Consider hardware and software requirements before deciding if a tablet, laptop, or desktop is the best choice for that job function.
- 2. Software Requirements:** Roles at the dealership will require interaction with different software. Software is often written for specific operating systems and internet browsers. Software applications may also require a minimum hardware specification. When purchasing a new device, understand the software the device will run, and the associated requirements needed to operate that software.
- 3. Hardware Accessory Requirements.** Dealerships often need specific accessories to perform a job function. Sales aids, service diagnostics, and other physical adaptors are needed for specific use cases. These accessories are often made with specific software and hardware specifications in mind. If the job function requires a specific accessory, check with the vendor for requirements before purchasing new equipment.

4. **OEM, DSP, and 3rd party requirements:** OEMs, Dealership Service Providers, and other 3rd party vendors often deploy specific dealership technologies. These technologies (hardware or software) may require specific specifications to operate efficiently. If a dealership device uses specific technologies, check with the technology provider.
5. **Reliability:** Device reliability needs to be considered when making hardware purchases. Some areas of the dealership, such as the service environment, are more prone to device failure. Some job functions are more limited by device downtime. When considering when and what to purchase, take into account the likelihood of device failure, and the impact a failure can have on that job function and dealership business operations.

Beyond use case recommendations, STAR can provide guidance on when to purchase new hardware, and what to purchase when that time comes. STAR provides guidance on “when to purchase new hardware” in the STAR Dealer Infrastructure Guideline in section 2.2.a. When determining what to purchase, STAR provides guidance on Consumer Grade vs Enterprise Grade hardware purchases in section 2.2.b. and a guide for Tablets and Mobile Devices in section 2.2.d.

STAR also provides guidance and specifications routers and switches to connect network hardware in section 2.2.c of the Dealer Infrastructure Guideline.

For more information on dealership hardware recommendations, including tablets, mobility, and hardware decommissioning & recycling 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, Microsoft has ended support for XP, Vista, and Windows7 operating systems. This includes critical security updates. STAR recommends dealerships do not use Windows XP, Vista, nor Windows 7.

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
Windows 11	24H2		
MAC OS X	14.2.1	Versions 11 (Big Sur) and below no longer supported.	Versions 11 (Big Sur) and below no longer supported.
IOS (for iPad and iPhone)	17		
Android	14		

**Latest updates/service pack as of January 2024*

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 2020*

Browser	Latest update or service pack*	Notes
Google Chrome	120	
Mozilla Firefox	121	
Internet Explorer	11	Internet Explorer was retired in June 2022. Microsoft Edge is the browser recommended by Microsoft.
Microsoft Edge	120	
Apple Safari	17	Not recommended for use on Microsoft Operating systems

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. <ul style="list-style-type: none"> - 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. <ul style="list-style-type: none"> - 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.

	<ul style="list-style-type: none"> - 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. Note: Check with OEM recommendations for compatibility guidance for OEM specific technologies.
Network standard	802.11ax or 802.11ac
Rogue Wireless Detection	<p>Scan, identify and remove any rogue wireless access points that may be on the dealership's network.</p> <ul style="list-style-type: none"> -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	<p>A fully-managed security device that continually monitors threats through Intrusion Detection system “IDS” and Intrusion Prevention System “IPS” and other mechanisms.</p> <p>The device should also have the following features:</p> <ul style="list-style-type: none"> • 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) <p>Because of the importance of the Firewall, and the fact it is often in the data path for most dealership traffic, STAR recommends a backup device in the case of failure. To limit downtime, dealers should consider a solution for automatic failover to the back up device in the case of a hardware failure.</p>
Network Segmentation	<p>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.</p>
Content Filtering	<p>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.</p>
SIEM	<p>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.</p>
Wireless Detection System	<p>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.</p> <ul style="list-style-type: none"> ○ 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: <ul style="list-style-type: none"> • 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 <u>days</u> , or less. At a minimum, dealerships should use “strong passwords” containing an 8-character minimum comprised of 3 of the following 4 requirements: <ol style="list-style-type: none"> 1) Uppercase 2) Lowercase 3) Numeric 4) Special characters.
Endpoint Detection and Response Platform	<ul style="list-style-type: none"> • A singular endpoint protection platform (EPP) and endpoint detection and response (EDR) solution should be deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts. Alerts from this service should be responded to immediately to mitigate risk and potential data loss. The service offering should provide cross-platform visibility into endpoint/server activities as well as: 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)