Nissan Group of North America

Nissan Dealer Network Infrastructure key performance indicators and best practices to ensure efficient network operations, standardization, technology adoption, and optimal customer experience.

This appendix to the STAR Dealer Infrastructure Guideline (DIG) serves as a comprehensive resource, providing additional information and resources to enhance your understanding and implementation of the guidelines.

CONTENTS

OVERVIEW

A dealership's network infrastructure consists of the hardware and software resources utilized to enable network connectivity, communication, operations, and management of the dealer's local area network (LAN). Network infrastructure provides the communication path and services between the dealership, service providers, Nissan technologies, and end customers. Proper selection, implementation, configuration, and network infrastructure management are critical to ensuring optimal customer experience, security, and operational efficiency.

This document provides guidance and best practices based on North America's high-performing Nissan and INFINITI dealerships. It is to be used as a reference and in conjunction with the STAR Dealer Infrastructure Guideline for detailed Nissan-specific recommendations and compatibility requirements.

Although this document is intended to provide guidance, tools, and assistance to dealerships, the dealership is responsible for network management and security. Dealer service providers, third parties, and Nissan North America cannot guarantee a secure dealer network, even if dealers follow the guidelines in this document.

HARDWARE

Most computer manufacturers offer two different grades of computers: consumer-grade hardware intended for home and personal use and enterprise-grade hardware intended for businesses. While the price of consumer-grade hardware may seem attractive for dealerships, the total cost of ownership is often greater due to the limited functionality, higher failure rates, and more complex support.

Nissan may recommend specific hardware platforms in certain areas, such as dealership service. In all other instances, Nissan recommends dealerships purchase enterprise-grade hardware. For more detail on enterprise vs. consumer-grade hardware, the differences, and reasons to choose enterprise-grade equipment, see section 2.2b of the STAR Dealer Infrastructure Guideline (DIG).

ADDITIONAL RESOURCES

For additional information on dealership hardware such as when to purchase, what to purchase, decommissioning & recycling of hardware, as well as guidance on mobility, see the STAR Dealer infrastructure Guideline, section 2.2.

Service Hardware

- Nissan CONSULT 3
- Nissan CONSULT 4
- Nissan INFINITI Diagnostic CONSULT Kit with VI3
- Panasonic Toughbook FZ-55

SOFTWARE

Operating Systems

- Windows 10
  - *Note: Windows 10 end of support is October 2025.*
- Windows 11
  - *Note: Utilize the latest service pack (23H2 or above).*

Internet Browsers

- Microsoft Edge (version 92+)
- Google Chrome (version 93+)

Service Software

- Nissan CONSULT III Plus Diagnostic Software (Version 235.10.00)
- Nissan CONSULT 4

LOCAL AREA NETWORK (LAN)

Bandwidth Requirements

Internet Technologies

Nissan recommends dealerships purchase business-grade internet services that include service level objectives (SLAs), enterprise support, and dedicated bandwidth. Nissan also recommends dealers use technologies such as QOS, traffic shaping, and network segmentation to ensure dealership resources in sales and service have enough dedicated bandwidth and are not affected by guest traffic, employee personal devices, or other IOT technologies.

Bandwidth Speeds and Availability

Nissan recommends that dealers dedicate over 5Mbps per sales and service endpoint. Dealers must plan to procure additional bandwidth to accommodate guests, administration, and other connected devices.

Backup Connection

Nissan recommends dealers have a backup internet service that uses a different provider and transport technology. This ensures that risks from vendor or physical network outages are better mitigated.

ADDITIONAL RESOURCES:

For additional information on Internet Technologies, planning for bandwidth and customer access recommendations see section 2.5 of the STAR Dealer IT Guides (DIG)

Network Configuration and Management

Recommendation	Specification
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	The dealership ISP should provide routable IP addressing. To ease support, dynamic addressing (DHCP) should be used for the dealer LAN.
Domain Name Services (DNS)	Use public DNS except when using Windows Active Directory. (In which case, having an internal DNS server is required.)
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 an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) and other mechanisms such as packet filtering, antivirus, and stateful packet inspection.

Wireless Networking

Wireless Coverage

Provide wireless network coverage so that the wireless signal strength averages -60dBm or better and has strong wireless coverage throughout the sales showroom, service drive, service shop/bays, customer lounge, service lot, and vehicle lot.

Access Point Placement

- Dedicate an Access Point (AP) to the following areas:
  - Service Lane
  - Service Shop/ Service Bays
  - Sales Show Room
  - Customer Waiting Area
  - Vehicle Lot
- Ensure a dedicated access point is within 65ft of Nissan Wireless Technologies.

Wireless Network Monitoring

Monitor and report on all connected devices, bandwidth utilization, signal strength, segmentation, and security activity.

Wireless Network Configuration

Recommendation	Specification
Network Segmentation	Dealers must ensure guest traffic, financial data, and the dealership network are segmented through VLANs or a separate Internet connection. Connections should be actively monitored for security events, bandwidth capacity, and configuration adherence. Nissan also recommends traffic shaping, QOS, or other mechanisms to ensure guest traffic does not interfere with dealership network operations or bandwidth capacity.
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.
Wireless Frequency and Channel Configuration	Utilize both 2.4 GHz and 5 GHz frequencies. To reduce conflict, access Points should be configured to the following channels: • For 2.4 GHz: Channels 1, 6, or 11 ONLY. • For 5 GHz: Channels 36-64, 100-140, or 149-165.
Authentication & Encryption	WPA2 with RADIUS authentication and AES Encryption. *Note*: Check OEM recommendations for compatibility guidance for OEM-specific technologies.
Network Standard	802.11ax or 802.11ac

SECURITY

Network Security

Firewall/ UTM

A fully managed security device that continually monitors threats through an Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and other mechanisms.

Security Management, Monitoring, and Response

Proactive, real-time event monitoring utilizing a SIEM service with 24x7x365 security event monitoring and response by a SOC 2-certified Managed Security Service Provider.

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 potentially harmful, inappropriate, or other non-business-related traffic.

Penetration Testing and Vulnerability Scanning

- Annual internal and external penetration testing of the dealer network is highly recommended.
- Perform continuous vulnerability scans of systems, infrastructure, and applications based on the current industry standards. Remediate security vulnerabilities in systems or other resources regularly based on criticality.

Endpoint Security

Patch Management

Perform patch management 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 required to be reset every 60 days or less and follow a standard "strong password" policy.

Multi-Factor Authentication (MFA)

Incorporate Multi-Factor Authentication (MFA) for all systems containing sensitive business and consumer data. MFA systems require users to use authentication factors from at least two of three different categories:

- Something the user "knows" (such as a password)
- Something the user "has" (such as a phone or key)
- Something the user "is" (such as a biometric indicator such as face or fingerprint scan)

Endpoint Detection and Response Platform

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 EDR Platform should also be able to assist with threat containment and remediation, activity reporting, and threat hunting.

APPENDIX A: ADDITIONAL SECURITY RESOURCES

Implementing Secure Systems

- Computer Security Resource Center National Institute for Standards and Technology (NIST) - http://csrc.nist.gov
- National Strategy to Secure Cyberspace, Department of Homeland Security - http://www.dhs.gov/files/publications/editorial_0329.shtm
- The SysAdmin, Audit, Network, Security (SANS) Institute the Twenty Most Critical Internet Security Vulnerabilities - www.sans.org/top20
- United States Computer Emergency Readiness Team (US-CERT) - www.us-cert.gov/resources.html
- Carnegie Mellon Software Engineering Institute CERT Coordination Center - www.cert.org
- Star Risk Assessment Questionnaire - https://www.starstandard.org/index.php/risk-assessment-questionnaire-2/

Security Policies

- Start DIG Section 2.6.a

Security Awareness Training

- STAR DIG Section 2.6.d

Identity And Access Management

- STAR DIG Section 2.6.b

Security Information Event Management

- Star DIG Section 2.6.f

Governance, risks, and compliance:

- PCI Security Standards: https://www.pcisecuritystandards.org
- Gramm-Leach-Bliley Act: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
- STAR DIG: Section 2.6

Email Security:

- Star DIG Section 2.6.h

Application Security

- Star DIG Section 2.6.i

APPENDIX B: NISSAN DEALER TECHNOLOGY INFRASTRUCTURE REQUIREMENTS

The following technologies are commonly deployed into Nissan Dealerships. Listed in the tables below are the bandwidth, Wi-Fi, and URLs required to operate these technologies. Dealers should ensure their network is configured to allow these technologies to operate as designed. This means deploying dual band wireless, whitelisting URLs, and providing enough bandwidth for each technology.

Hunter Equipment and Applications

Technology	Bandwidth Requirements	Wi-Fi Requirements	URL Whitelist
Hunter Alignment Machines	10+ MBps (total network)		• hunternetwork.com • www.hunter.com • www.getspecs.com • www.shopresults.net • www.webspecs.net • core.windows.net • hunternet.okta.com
Hunter Quick Check	10+ MBps (total network) 20+MBps (Total network for Quick Check Drive BDC feature)		• *.hunternetwork.com • www.hunter.com • www.getspecs.com • www.shopresults.net • www.webspecs.net • core.windows.net • hunternet.okta.com
Hunter Quick Tread Edge	10+ MBps (total network)		• *.hunternetwork.com • www.hunter.com • www.getspecs.com • www.shopresults.net • www.webspecs.net • core.windows.net • hunternet.okta.com
Hunter Road Force Tire Balancers	10+ MBps (total network)	2.4Ghz network (not compatible with 5Ghz)	• *.hunternetwork.com • www.hunter.com • www.getspecs.com • www.shopresults.net • www.webspecs.net • core.windows.net • hunternet.okta.com

Nissan Technologies and Applications

Technology	Bandwidth Requirements	Wi-Fi Requirements	URL Whitelist
ASIST	5+ Mbps per user		asist.na.nissancloud.com (port 22) asist.na.nissan.biz (port 22) http://www.asistfaq.com (port 80) https://www.asistfaq.com (port 443) https://b2bws.na.nissan.biz (port 443) https://esm.tweddletech.net (port 443) https://nissancms.tweddletech.net (port 443) http://nna.force.com https://nna.secure.force.com saml.jp.nissan.biz (CONSULT-III plus software usage) gdauth.jp.nissan.biz (CONSULT-III plus software usage) https://adtprod-us.dcs2.renault.com (CONSULT 4) https://gdauth.jp.nissan.biz (CONSULT 4) https://as.na.nissan.biz (CONSULT 4) xmscommandsvc.service-solutions.com (CONSULT 4) xmsReadinesschecksvc.service-solutions.com (CONSULT 4) xmspackage.service-solutions.com (CONSULT 4) https://asist-files.nnanet.com and *.nnanet.com port 8080 (ASIST WEB) https://asist-prod.auth.us-east- 1.amazoncognito.com https://appprodc3pcrashserviceapi.azurewebsit es.net/ (CONSULT CRASH TOOL)
Bomgar/ Tech Link	1.5. Mbps per user		https://techlink.nissan-ix.com/ https://nissan-usa.beyondtrustcloud.com/
CONSULT	5+ Mbps per user		asist.na.nissancloud.com (port 22) asist.na.nissan.biz (port 22) http://www.asistfaq.com (port 80) https://www.asistfaq.com (port 443) https://b2bws.na.nissan.biz (port 443) https://esm.tweddletech.net (port 443) https://nissancms.tweddletech.net (port 443) http://nna.force.com https://nna.secure.force.com saml.jp.nissan.biz (CONSULT-III plus software usage) gdauth.jp.nissan.biz (CONSULT-III plus software usage) https://adtprod-us.dcs2.renault.com (CONSULT 4) https://gdauth.jp.nissan.biz (CONSULT 4) https://as.na.nissan.biz (CONSULT 4) xmscommandsvc.service-solutions.com (CONSULT 4) xmsReadinesschecksvc.service-solutions.com (CONSULT 4) xmspackage.service-solutions.com (CONSULT 4) https://asist-files.nnanet.com and *.nnanet.com port 8080 (ASIST WEB) https://asist-prod.auth.us-east- 1.amazoncognito.com https://appprodc3pcrashserviceapi.azurewebsit es.net/ (CONSULT CRASH TOOL)
Tell Me More			https://vcat.nnanet.com/prweb/PRAuth/NissanOIDC
VCAT			https://vcat.nnanet.com/prweb/PRAuth/NissanOIDC

Nissan Certified NCAR Vendor Requirements

Technology	Bandwidth Requirements	Wi-Fi Requirements	Application & Email Filtering:
Dealerlogix			Application Filtering: menu.flathatsystems.com websocket.flathatsystems.com e-dealertire.com gateway.transit-pass.com faq.dealerlogix.com googletagmanager.com login.dotomi.com nissanna-prod.pegacloud.io Email Filtering: dealerlogix.com dealerlogixmail.com helpscout.net
DealerFX	Small Store (1 – 2 Advisors) 30 Mbps download by 20 Mbps upload Medium Store (3 – 5 Advisors) 40 Mbps download by 25 Mbps upload Large Store (6 – 9 Advisors) 50 Mbps download by 30 Mbps upload Big Stores (10+ Advisors) 70+ Mbps download by 40+ Mbps upload		dealer-fx.com dealer-fx.net dfx.one

CDK	100k per user or 1.65mbps for every 25 computers/mobile devices. Usage should not exceed 70%	1 GB Ethernet recommended; 100 MB fast Ethernet recommended. 5 GHz network recommended	
XTime Main App	See Bandwidth Requirements section (page 5)	Engage requires a dedicated wireless network (e.g. router and access points) with a dedicated internet connection to ensure sufficient wireless network access and communication with Xtime's servers. Wireless network coverage is required in all areas where the tablet is to be used. Intermittent coverage can prevent Engage tablet reception from communicating with Xtime servers causing the application to become inoperable. Wi-Fi coverage should be tested in all usage areas with an online wireless dashboard (see Wireless Networking Section on page 7) Engage tablet reception should be tested for proper operation in the areas with the weakest coverage to ensure proper operation.	50.31.36.212 159.183.210.37 159.183.210.42 159.183.210.60 159.183.210.66 192.254.112.93
XTime Engage App			xtime.app.coxautoinc.com http://*.xtime.com/ https://*.xtime.com/ http://s3.amazonaws.com/ https://s3.amazonaws.com/ http://xtime.s3.amazonaws.com/ https://xtime.s3.amazonaws.com/ https://unpkg.com https://xtchat1.aws.xtime.com

LenZ® Equipment and Applications

Technology	Bandwidth Requirements	Wi-Fi Requirements	URL Whitelist
LenZ®			See full list: https://support.realwear.com/knowledge/ip-port-url-allowlisting
TeamViewer (needed for LenZ®)	3MBps per user		https://licensing.svc.frontlineworker.com/app IP Address 13.69.62.84

Mahle AC Machines

Technology	Bandwidth Requirements	Wi-Fi Requirements	URL Whitelist
Mahle AC Machines		5Ghz network (not compatible with 2.4Ghz)	

Midtronics

Technology	Bandwidth Requirements	WiFi Requirements	URL Whitelist
Midtronics CPX-900		5Ghz network (not compatible with 2.4Ghz)	
Midtronics DCA-8000		5Ghz network (not compatible with 2.4Ghz)	
Midtronics DSS-5000		5Ghz network (not compatible with 2.4Ghz)	