Aldridge IT Architecture for Business Optimization

Version 2018.1

Contents

Introduction

The Aldridge IT Architecture for Business Optimization ("IA", or "Architecture") is your reference to the IT products, tools, and subscription providers (collectively, "products") we use for all new technology implementations today. The Architecture applies to all technology purchases we make for you on your behalf, and it applies to you, in all the technology purchases you may make directly while engaged with us in an Aldridge Managed Services agreement.

Architecture evolves. In business and in IT, there's no circumstance where an initial plan can optimize everything for the long term. The dynamics of your organization change and grow over time, as does the landscape of available technologies and tools. It's important that we work together to keep your needs aligned to the present, appropriate technologies and tools. Over time, legacy IT investments and architectures that haven't kept pace; or that are beyond their intended operating lifecycle; can stifle innovation and increase your operating costs. We all want your organization's IT resources to be there, ready to work when you are. As importantly, we all want to work together to keep IT aligned with your organization, to bring discussions about current tools and evolving practices into our appropriate conversations together, and to stay mindful of opportunities to improve your organization's efficiency and return on IT investment.

From our experience across the many industries and organizations we work with, the Architecture represents the palette of IT tools we've determined are most-applicable and most-appropriate for most of our client organizations, including yours. The Architecture in turn represents what we've invested in our Managed Services to best provide, support, and maintain. Strong alignment to the Architecture contributes to strong delivery and a consistent experience for your organization with Aldridge Managed Services.

Taken separately or all together, the principles in this Architecture will help us develop future technology roadmaps together to manage IT costs and keep you ready for new opportunities.

Purpose

This Architecture exists so that:

1. All new IT purchases and subscriptions we introduce within your organization are made within the current version of the Architecture.
2. The Architecture identifies the products and subscriptions we've identified as most-appropriate for most organizations' IT environments.
3. For future planning, Aldridge can work with you to keep your organization's IT roadmap aligned to the current Architecture.

Alignment to Architecture for New Purchases and Subscriptions

When you're considering improvements or implementations within your organization's IT products and subscriptions, if this Architecture has applicable guidance for that category of IT, it's important to plan and operate within the Architecture.

IT is a large landscape, and there are often many brands and options to fulfill any particular need; the Architecture is your guide to the specific options we've identified to be the most-appropriate overall experience for your organization, and the options in which we've invested to provide you the best Managed Services experience. Just as you rely upon us to manage your organization's overall IT, rely upon us to follow your organization's needs in specifying the appropriate Architecture-guided solutions.

If there is a specific constraint within your organization that conflicts with the Architecture, let's discuss it and cooperatively understand the impacts and options.

If you have elements in your organization's IT that are not aligned to this current Architecture, we'll proactively work together to plan ahead to bring your IT into alignment with these best practices, prioritized and scheduled by the net impacts and benefits to your organization.

If you have categories of elements in your organization's IT that aren't represented within the Architecture, that doesn't necessarily mean those elements aren't supportable. Elements not represented in any category in the Architecture may be particularly specific to your organization or unique business needs, or may not yet be generally applicable to the majority of the client organizations we work with, and so haven't yet needed Architecture guidelines. Product categories not identified within the Architecture are typically supported in partnership with a specialist vendor you've engaged to administer that technology product.

Product End-of-Life (EOL)

Products no longer in the Architecture will continue to be supported by Aldridge Managed Services until the product is identified as "End of Life" (EOL). EOL dates are announced ahead of retirement by either Aldridge, the product manufacturer, or the product provider. An EOL date should be considered the date by which that product should certainly no longer be in active use within your organization's IT, and the date upon which the product manufacturer or Aldridge will no longer provide the same level of support.

During scheduled Business Reviews together, we'll help make you aware of upcoming End of Life dates for products in your organization's IT environment. It's important that we work together to proactively replace or eliminate products approaching EOL, to minimize the cost and operating risks EOL products represent to your organization.

Once you're aware that a product is beyond its EOL date, future Aldridge support for that product may be out of scope of your Managed Services agreement with Aldridge and separately billable. Until the product reaches its EOL date, we'll continue to support it within your Managed Services agreement.

Aldridge Responsibilities

Aldridge is responsible for notifying you during the initial sales process that this document exists, so you have an opportunity to review the Architecture, and understand its value, impacts, and benefits to your organization. The online link to the current, downloadable Architecture document becomes a part of the Service Order for new Managed Services business. It's our responsibility to notify you when a new version of the Architecture is published and available at the online link.

Client Responsibilities

It's your responsibility to attend all business reviews scheduled with Aldridge. The business review includes a discussion of End of Life or obsolete products within your IT environment. Aldridge will collaborate with you to design or recommend solutions for technologies that aren't aligned to the current Architecture.

It's our intention to always work with you to recommend and perform cost-effective, efficient, and non-interrupted transitions to current Architecture, but it's ultimately your responsibility to implement the optimized architecture. Not doing so may cause you to incur increased costs within your Managed Services agreement for Aldridge's support of your organization's out-of-scope technology.

Agreement

This IT Architecture agreement is part of an aggregate series of agreements which, combined together by reference, create one integrated contract (the "Agreement") between Aldridge ("we," or "us," including "our," and "Aldridge") and Client ("you," including "your," or "Client"). Each of Aldridge and Client may also be referred to as a Party and collectively as the Parties.

For any Quotes, Quotations, Proposals, Statements of Work, Sales Orders, or Service Order ("SO") agreements executed by you (individually and collectively, "Engagements"), this document and all the applicable documents listed in the tables immediately below ("Included Agreements") are legally integrated as if fully set forth as one Agreement.

Upon each Engagement renewal, this Agreement, but not the terms of any ongoing Engagement, will be superseded by the terms and conditions set forth in the then currently published version of the applicable Included Agreement available online as of the date on which your services are renewed (the "Renewal Terms"). If you do not agree to the Renewal Terms, you may decline to renew your services.

The Aggregate Set of Agreements between Client and Aldridge, the Included Agreements

Applicable Agreements Integrated into All Engagements	Available Online at
Master Services Agreement	http://aldridge.com/MSA
Services Guide Agreement	http://aldridge.com/SG
Service Level Agreement	http://aldridge.com/SLA
Standard Rates Agreement	http://aldridge.com/rates
Domain Name Registration and Renewal Agreement	http://aldridge.com/DNR
A current and submitted Client Information Form, available online	http://aldridge.com/info

Included Agreements Integrated into Specific Engagements, as Applicable	Available Online at
Monitoring Services Guide Agreement *(applies to Engagements which include Managed Services)*	http://aldridge.com/monitoring
Aldridge IT Architecture for Business Optimization *(applies to Engagements which include Managed Services)*	http://aldridge.com/architecture
Managed Backup and Continuity Services Agreement *(applies to Engagements which include Managed Backup and Continuity Services)*	http://aldridge.com/backupservice
Acceptable Use Policy Agreement *(applies to Engagements which include Aldridge Cloud Hosting or Connectivity Services)*	http://aldridge.com/AUP
Microsoft End User License Agreement *(applies to Engagements which include Aldridge Cloud Hosting Services)*	http://aldridge.com/EULA
Hosted VoIP Agreement *(applies to Engagements which include Hosted VoIP Services)*	http://aldridge.com/hosted_voip

Identity Management and Authentication

Overview

Today's IT is less defined by the physical place where you are presently working and more by your ability to access resources, services, and collaboration from wherever you are. Properly managing that access relies upon a consistent identity solution as part of your IT architecture – the pieces that work together to securely affirm you are who you say you are (authentication), and to then approve access to the resources for your work (authorization).

Well-implemented identity management contributes to your organization's overall security, by:

- limiting the number of separate usernames and passwords each individual needs to maintain;
- establishing central policies over password security and acceptable authentication;
- maintaining a central authority of credentials, reducing the likelihood that a former member of your organization has unintentional, lingering permissions to your resources; and by
- permitting holistic management of authentication activity across the organization.

Supported Options

Option	Recommended Usage
Hybrid Microsoft Active Directory (AD) + Microsoft Azure Active Directory (AAD)	Organizations operating traditional servers (either on-premise, or cloud) and using cloud services such as Microsoft Office 365. Enables policy management for Windows-based computers joined to the AD domain.
Cloud-only Microsoft Azure Active Directory (AAD)	Organizations that do not operate traditional servers, and only subscribe to Microsoft's cloud services. Does not include computer policy management.
On-Premise Microsoft Active Directory (AD), Microsoft Windows Server-based	Organizations that only operate traditional servers (either on-premise, or cloud), and are not subscribed to cloud services such as Microsoft Office 365. Enables policy management for Windows-based computers joined to the AD domain.

Optional Configurations

- Microsoft Azure Active Directory Multi-factor Authentication (Microsoft Azure AD Premium)
- Microsoft Azure Active Directory Adaptive Authentication (Microsoft Azure AD Premium)
- Microsoft Azure Active Directory Self-Service Password Reset (Microsoft Azure AD Premium)
- Microsoft Azure Active Directory Single Sign On (SSO) for Supported Cloud Applications
- LDAP-integrated Single Sign On (SSO) to Active Directory for compatible services
- RADIUS-integrated Single Sign On (SSO) to Active Directory for compatible services

Network Infrastructure

Overview

Your organization's network infrastructure defines the physical boundaries of your organization's IT.

The network infrastructure may include:

- each physical place of business where your organization regularly maintains offices or operates;
- the connection portion of the home networks of your remote staff that work from home with the support of your organization;
- connections to hosted, cloud-based networks and platform providers, tying your organization into IT resources for which you don't have to directly operate traditional, physical equipment; and
- tools permitting you and your staff to securely connect to your organization's IT network resources from anywhere they have appropriate Internet access.

Portions of your organization's network infrastructure are often referred to as:

- Local Area Network (LAN); the area(s) of your organization network that are private and physically or logically with your organization's exclusive control.
- Wide Area Network (WAN); the area(s) of your organization network that rely upon public or subscribed service connections, such as connections between offices you may have in two separate cities or secured connections you may maintain between your business offices and hosted, cloud-based networks.
- Wireless Local Area Network (WLAN); a subset of your organization's LAN which uses wireless radio technology, versus physical cables, to establish and maintain connections.

Internet Services

Performance Requirements

Service Feature	Recommendations
Downstream Bandwidth	Offices of <15 people: at least 15Mbps to 25Mbps for average workloads Offices of 15 to 75 people; at least 50Mbps to 100Mbps for average workloads Offices of 75 to 150 people; at least 100Mbps to 150Mbps for average workloads Offices of more than 150 people; at least 150Mbps for average workloads
Upstream Bandwidth	15Mbps, plus 10Mbps per 1TB of on-premise backup-protected storage, up to 100Mbps
Data Transfer Limits	We do not recommend the use of metered Internet connections for the main Internet services at your business offices or work sites.

IP (Internet Protocol) Address Requirements

- A static, routable public IPv4 address is required for the Internet connections of all regular business offices of your organization.
- A static, routable public IPv4 address is required for the Internet connections of remote staff who will be maintaining a secure (IPSEC) connection to the office network.
- The static, routable public IPv4 address allocated from your Internet Service Provider should be directly assignable to the Internet interface of the firewall equipment Aldridge will specify and maintain at your location.
- The smallest allocated public IPv4 subnet assignment from your Internet Service Provider should be a /30 subnet (subnet mask 255.255.255.252), which provides you one usable public IP for your office firewall, and one public IP maintained by your provider as the default gateway.
- If you are maintaining services at your business offices that are accessible from the Internet, the best practice for security and reliability is to allocate one additional static, routable public IPv4 address to each service. This may require you to maintain a /29, /28, or /27 subnet of usable IPv4 addresses (permitting 5, 13, or 29 usable IPv4 addresses, respectively) from your Internet Service Provider, at commensurate cost.

Provider Hand-Off / Customer Premise Equipment (CPE) Requirements

- From the customer premise equipment (CPE) your Internet Service Provider (ISP) requires that you operate at your place of business, your Internet Service Provider must provide a standard, wired Ethernet connection to your Internet service.
- The CPE must operate as a transparent bridge or router such that it does not alter or interfere with the Internet traffic or public IPv4 address usage of your organization.
- In general, Internet services requiring the use of PPPoE, NAT on CPE, or CIDR should be avoided as they often limit the types of services and networks you can operate at your offices and will impede our ability to monitor and maintain the resiliency of your organization's network. It may be necessary to use an alternative or more-expensive Internet service or Internet Service Provider to avoid these limitations.

Firewall Appliances

Firewall Appliances sit at the edge of your organization's office network usually managing and securing the connection between your organization's internal network equipment and your Internet service.

- A Cisco ASA Next Generation Firewall (NGFW) series appliance with FirePOWER network security services is required at each business office where your organization maintains an Internet connection.
- A Cisco ASA firewall may be required at each branch or individual home office that maintains a full-time network connection to your business offices via an Internet tunnel (IPSEC).
- Because of its critical role in the operation and security of your organization's Internet service, as part of providing protection and remediation for your network, we require transitioning most other firewall solutions to the current-generation Cisco ASA firewall series within 1 year.

Performance Requirements

Internet Bandwidth	Approved Equipment
Up to 100Mbps	Cisco ASA 5506X with FirePOWER (for offices of more than 5 people, or more than 2,000 sf) Cisco ASA 5506W-X with FirePOWER (for offices of up to 5 people and less than 2,000 sf)
Up to 250Mbps	Cisco ASA 5508X with FirePOWER
Up to 450Mbps	Cisco ASA 5516X with FirePOWER

Capability Requirements for All Firewall Appliances

- Active manufacturer hardware support and firmware subscription
- IPS (Intrusion Previous Services) support, for sites permitting direct Internet access
- AMP (Advanced Malware Protection) support, for sites permitting direct Internet access
- Web address / URL filtering support, for sites permitting direct Internet access
- SNMP (Simple Network Management Protocol) support
- SSH and HTTPS IP management support
- VLAN (Virtual Local Area Networking) support for at least 5 VLANs
- SSL VPN support (either software-client, browser-based, or with native client OS support)

Optional Configurations

- High availability (redundant firewall equipment), to help protect against the physical failure of one piece of firewall equipment.
- Secondary Internet connect support, to help protect against interruption of outbound Internet access should one of your office's Internet Service Providers experience an issue.

Network Switches

Network switches manage the physical connections between wired network equipment, computers, and other devices.

- Cisco SG250, SG350, or higher-series Cisco managed switches are required
- Alternate switches already in-service that meet the Capability Requirements, below, can be operated for their recommended useful life (typically 3 to 6 years), but the presence of the alternative equipment may impact the availability of some network services and impede our ability to efficiently monitor, administer, and troubleshoot your organization's network.

Capability Requirements for All Switches

- Active manufacturer hardware support and firmware subscription
- Gigabit Ethernet support (all ports)
- SSH and HTTPS IP management
- Full PoE (Power over Ethernet) capacity is recommended for all ports
- At least (2) 1Gbps+ SFP (Small Form-Factor Pluggable module) ports for switches with 16 ports or more; 10Gbps SFP recommended
- Switching capacity (backplane speed) of at least 20Gbps (10 port switches) or 100Gbps
- Stacking support
- SNMP (Simple Network Management Protocol) support
- VLAN (Virtual Local Area Networking) support for at least 64 VLANs
- QoS (Quality of Service) support
- STP (Spanning Tree Protocol) support
- Layer 3 (L3) features support is required for switches in Distribution or Core network roles

Wireless Access Points

Wireless Access Points permit nearby, compatible wireless devices to use radio networking (WiFi) to connect to portions of your organization's network.

- Cisco access points are required for most wireless service installations
- Alternate wireless equipment already in-service that meets the Capability Requirements, below, can be operated for its recommended useful life (typically 2 to 4 years), but the presence of the alternative equipment may impact the availability of some network services and impede our ability to efficiently monitor, administer, and troubleshoot your organization's network.

Capability Requirements for All Wireless Access Points

- Active manufacturer hardware support and firmware subscription
- Both 2.4GHz and 5.0GHz support
- 802.11a, b, g, n, and ac protocol performance support
- Gigabit wired Ethernet interface (1Gbps)
- Power over Ethernet (PoE) support
- SNMP (Simple Network Management Protocol) support
- SSH and HTTPS IP management
- WPA2, AES, EAP security support
- Standalone or Autonomous access point modes support
- Multiple SSID and VLAN support

Wireless Coverage Guidelines

The specific type and amount of equipment required for your location's best wireless network availability and performance will vary by the number of devices you wish to support, the types of activity your network will be used for, the size of the office space you wish to serve, the construction and materials of the building, competing local wireless signals, and more. The following recommendations are based on our experienced best practices for typical-office installations.

- Plan on (1) wireless access point per 1,500 sq ft of area you wish to serve (140 sq meters)
- Plan on dedicating additional wireless access points for high-density areas, such as classrooms or large meeting rooms
- For people performing typical document and collaboration tasks…
    - a Cisco 1832i-model wireless access point can typically accommodate up to 40 people
    - a Cisco 1852i-model wireless access point can typically accommodate up to 60 people
- Halve these estimates if people are using high-demand network applications
- Using the Cisco Aironet wireless products with Cisco Mobility Express, a dedicated wireless LAN controller appliance is typically not necessary for installations consisting of up to 30 wireless access points across up to 3 office sites. For installations requiring more than 30 access points, or more than 3 office sites, a wireless LAN controller appliance is recommended.

Network Routers

Network routers can be used for connecting Internet services into your premises, connecting voice or site-to-site networks between locations, and more.

- Cisco brand routers are required for most network router installations in cases where your organization's network design requires the presence of a router.
- Your Internet Service Provider (ISP) may provide an ISP-managed router as part of the Customer Premise Equipment (CPE) required to deliver Internet service to your organization. ISP-managed CPE routers located outside of the network firewall managed by Aldridge do not need to conform to these requirements.
- Alternate network routing equipment already in-service that meets the Capability Requirements, below, can be operated for its recommended useful life (typically 3 to 6 years), but the presence of the alternative equipment may impact the availability of some network services and impede our ability to efficiently monitor, administer, and troubleshoot your organization's network.

Capability Requirements for All Network Routers

- Active manufacturer hardware support and firmware subscription
- SNMP (Simple Network Management Protocol) support
- SSH and HTTPS IP management
- DES, 3DES, and AES IPSEC support
- At least (2) 1Gbps wired Ethernet ports
- At least (1) Enhanced High-Speed WAN Interface Card slot (EHWIC)

Client Virtual Private Networking (VPN)

Client VPN solutions permit your traveling and other out-of-office or working-at-home staff to securely access resources on your organization's network. Client VPN solutions establish a secure, authenticated, encrypted connection from your mobile staff's computer, using almost any Internet connection they presently have available to your organization's network.

- Cisco AnyConnect VPN will be used for all new Client VPN configurations requiring connectivity to your organization's office network.
- Microsoft Azure Point-to-Site VPN configuration is a supported solution if your organization does not operate an office network but does operate secured resources within a Microsoft Azure software-defined local area network.
- Alternate client VPN solutions already in-service that meet the Capability Requirements, below, can be operated until a Cisco ASA firewall appliance with VPN support is implemented for your office network, but the presence of the alternative solution may impact the availability of some network services and impede our ability to efficiently monitor, administer, and troubleshoot your organization's network.

Capability Requirements for All Client VPN Solutions

- Active manufacturer solution support
- Secure, encrypted authentication and traffic tunneling
- Support for both Microsoft Windows and Apple desktop operating system clients
- Support for both Android and Apple iOS clients
- Integrated identity authentication support (see Identity Management and Authentication)
- Multi-Factor Authentication support
- NAT-T (Network Address Translation Traversal) support
- Split Tunneling support

Personal Computer Equipment and Peripherals

Overview

Operating Lifecycle

We anticipate most personal computer equipment you purchase today will have a four-year useful life. After four years, whether through wear and tear or the benefit of technical advancements, most organizations find it's more cost-effective to replace aging equipment than to continue to support, repair, or operate within its performance constraints versus current options.

Manufacturer Configuration and Manufacturer Support

Aldridge supports the computer as a unit, not its individual components – the manufacturer warranties and supports the components, and we rely upon the manufacturer for parts replacement and proper operation and compatibility of the equipment. Because of this, Aldridge does not do custom computer builds or significant component changes or upgrades within personal computer equipment; the result would not be warrantied by the manufacturer.

We can do custom-specification computers for particular applications, business needs, and role demands. We work with manufacturers and the list of requirements to obtain a complete manufacturer-supported system proposal that meets or exceeds the requirements, ideally with manufacturer validation for the intended application or use.

In general, we recommend purchasing new personal computer equipment with a three-year manufacturer hardware warranty with on-site service. After three years, most of the cost of the initial equipment purchase has been depreciated, and while it may be feasible to continue to use the equipment to a fourth or fifth year, should a hardware issue occur or should the equipment require significant service or repairs, the cost of those services can be economically weighed versus the likely already-planned upcoming replacement of the equipment.

Local content is always at risk of loss

Knowledge and content that's kept exclusively on the local storage of any personal computer is always at risk of loss due to equipment theft, damage, failure, data deletion or corruption, or many other causes. We do not recommend nor support the storage of business information solely on any personal computer's local storage, and we cannot reliably recover or repair information that was kept in that manner.

While there are many ways to back up or copy data from a personal computer, that's very different from being relatively confident of being able to recover data from a particular point in time, with a reasonable amount of effort, if and when it is necessary to do so.

As supported alternatives, we recommend using a combination of:

- Cloud-hosted or server-based commercial e-mail solutions, where your primary mailbox and all personal content is kept on protected, central services, and cached to your local personal computer as needed.
- Cloud-hosted or server-based file storage, such as Microsoft SharePoint Online and Microsoft OneDrive for Business, where documents and collaboration content are stored primarily on protected, central resources, and optionally cached to your local personal computer as needed.
- Cloud-hosted or server-based applications and data sets, where you may be using an application locally but the application is interacting with data stored in a protected environment.

All of these solutions are intended to be:

- Automatic, requiring no user action to be regularly successful
- Consistent with the overall Architecture, leveraging the tools within the Architecture in ways they are best designed to be used
- Supportable, using the IT tools and expertise in which we continue to invest to keep you and your organization productive
- Independent of any particular physical equipment or venue
- Scalable, such that do not require customization or custom management to maintain

Security

Exclusive Organization Use

As a best practice, personal computer equipment regularly used to work with your organization, knowledge, and content should be used exclusively for that purpose. Public shared-use and family home computers used by multiple family members or a third party may become compromised and expose your organization to security risks.

A compromised mobile computer, brought into your office network, connected, and authenticated by an approved member of your organization may inadvertently introduce malicious software into your organization. A home computer, used by multiple members of a family but also sometimes used to connect to the office network via Virtual Private Networking (VPN), could provide a means for malicious software to reach your internal office network and resources.

For supportability, personal computer equipment managed and supported by Aldridge should be used exclusively for the purposes of the organization.

Drive Encryption

As a best practice, Aldridge recommends using BitLocker drive encryption on mobile computers using the Microsoft Windows 10 operating system, to help protect private organization information which may be locally-cached on the computer from the risk of theft.

Anti-malware Protection

Aldridge requires that the Aldridge suite of anti-virus and anti-malware software products be installed on each managed, supported personal computer. The Aldridge-managed suite of products may require removal or displacement of other anti-virus or anti-malware solutions. We all want your systems to be secure, reliable, supportable, well-performing, and ready to work when you are – in part, that's why you engage us for your IT outsourcing. It's important that we deploy the tools we've standardized upon, have invested development and expertise within, and are prepared to best use to support you and your organization.

Microsoft Windows-based Personal Computers

New computer purchases must meet or exceed these minimums.

- Manufacturer
  - HP, Microsoft, Lenovo, or Dell business-class machines recommended
- Operating System
  - Microsoft Windows 10 Professional, 64-bit
- Processor
  - Intel Core i5 minimum
- Memory
  - 8GB minimum
  - 16GB recommended
  - No aftermarket memory; OEM-only, covered by same manufacturer's warranty
- Storage
  - 256GB SSD minimum (solid state disk)
  - 512GB SSD recommended (solid state disk)
  - No aftermarket drives; OEM-only, covered by same manufacturer's warranty
- Display
  - At least two DisplayPort digital video outputs recommended
- Security
  - TPM hardware-enabled
  - UEFI enabled in BIOS
  - GPT operating system partition
- Peripheral Connections
  - USB 3 minimum
  - USB-C recommended
  - Bluetooth wireless required (mobile computers)
  - Built-in camera required (mobile computers)
- Network Connections
  - Desktop/Fixed Computers
    - Wired 1Gbps Ethernet minimum, with Wake-On-LAN support
  - Mobile/Portable Computers
    - 802.11n wireless minimum
    - 802.11ac wireless recommended
    - Wired 1Gbps Ethernet recommended, with Wake-On-LAN support
- Warranty
  - Manufacturer's 3 year on-site hardware warranty

Apple-based (“Mac”) Personal Computers

New computer purchases must meet or exceed these minimums.

- Manufacturer
  - Apple
- Operating System
  - macOS Mojave (version 10.14; released June 2018) or newer
- Processor
  - Intel Core i5 minimum
- Memory
  - 8GB minimum
  - 16GB recommended
  - No aftermarket memory; OEM-only, covered by same manufacturer's warranty
- Storage
  - 256GB SSD minimum (solid state disk)
  - 512GB SSD recommended (solid state disk)
  - No aftermarket drives; OEM-only, covered by same manufacturer's warranty
- Display
  - At least two DisplayPort, Thunderbolt, or USB-C digital video outputs recommended
- Security
  - FileVault-based drive encryption (mobile computers)
- Peripheral Connections
  - USB-C recommended
  - Bluetooth wireless required (mobile computers)
  - Built-in camera required (mobile computers)
- Network Connections
  - Desktop/Fixed Computers
    - Wired 1Gbps Ethernet minimum, with Wake-On-LAN support
  - Mobile/Portable Computers
    - 802.11n wireless minimum
    - 802.11ac wireless recommended
    - Wired 1Gbps Ethernet recommended, with Wake-On-LAN support
- Warranty
  - AppleCare+ for Mac 3 year on-site hardware warranty

Monitors and Displays

New purchases and existing monitors intended to be used with new or reallocated computer equipment must meet these minimum standards.

- Input
  - At least one digital input (DisplayPort, USB-C, DVI-I, or DVD-D)
- Display Attributes
  - At least 22” viewable area
  - At least 1680 x 1050 pixel resolution; 1920 x 1080 recommended (1080p)
- Ergonomics
  - Detachable adjustable base (height, tilt, pivot, swivel) recommended
  - Standard 10cm VESA mount compatibility recommended

Smartphones and Android/iOS Tablets

To be supportable, existing smartphones and Android/iOS-based tablets must meet the following specifications, as should all new purchases.

- Android-based (Google) Smartphones and Tablets
  - Operating upon a current or near-current Android OS released within the last 24 months
  - At least 16GB of device storage
  - Device encryption should be enabled

- iOS-based (Apple) Smartphones and Tablets
  - Operating upon a current or near-current iOS released within the last 24 months
  - At least 16GB of device storage
  - Device encryption should be enabled

Printers, Copiers, and Scanners

Copiers, Workgroup Printers, and Multifunction Devices

Supportable technical specifications for existing equipment and new purchases

- Engine
  - Color laser print engine recommended
  - Microsoft Windows Universal Driver support recommended
  - Microsoft Windows Server 2016-compatible driver required
  - Microsoft Windows Server 10-compatible driver required
  - Manufacturer native PCL6 driver recommended
- Connectivity
  - Wired gigabit (1Gbps) Ethernet networking recommended; 100Mbps minimum
  - Wireless 802.11n or 802.11ac network support recommended
  - HTTP web console
  - SNMP support
  - IPv4 printing support
  - IPv6 printing support recommended
- Scanning (if feature is present)
  - Scan-to-SMB Share support
  - Scan-to-SMTP (e-mail) support
    - TLS (Transport Layer Security) v1.2 encryption support
    - Microsoft Office 365 native compatibility
  - Scan-to-SharePoint Online support recommended
  - HTTPS web-console/local storage web-pickup recommended
  - LDAP address book support
- Fax Transmission (if feature is present)
  - IP-Fax (SIP/H.323) native sending support recommended
  - Analog POTS/RJ-11 telephone line sending is supportable

Personal Printers

- Engine
  - Microsoft Windows Universal Driver support recommended
  - Microsoft Windows Server 2016-compatible driver required
  - Microsoft Windows Server 10-compatible driver required
  - Manufacturer native PCL6 driver recommended
- Connectivity
  - USB-2 minimum; USB-3 recommended
  - Wireless 802.11n or 802.11ac network support recommended
  - Bluetooth support recommended
  - Wired 100Mbps Ethernet network connectivity recommended

Email Services

Microsoft Exchange Online

Part of the Microsoft Office 365 cloud services suite, Microsoft Exchange Online is our recommended and best-supported e-mail services solution for most organizations.

- Service Requirements
  - Active, maintained subscription to the Microsoft Exchange Online service
  - Aldridge global administrative access to your Microsoft Office 365 tenant, via either:
    - Designation of Aldridge as your Microsoft CSP (Cloud Solutions Provider)
    - Designation of Aldridge as a Partner of Record (POR)
- Client Requirements
  - As per current, published Microsoft Exchange Online guidance; in general:
    - A current Microsoft Outlook client application released within the last (3) years
    - A smartphone or mobile device with an operating system released within the last (2) years (we recommend the use of the Microsoft Outlook mobile app in lieu of the mobile device's basic manufacturer-provided e-mail client)
    - A current Internet web browser client released within the last (3) years
  - Local machine storage is recommended, sufficient to cache individual user mailboxes

Additional Supported Options

- Aldridge Managed Backup for Microsoft Office 365 Exchange Online
- Online Archiving
- Exchange Online Advanced Threat Protection (ATP)
- Litigation Hold and Retention
- Office Message Encryption (OME)
- Information Rights Management (IRM)
- Exclaimer E-Mail Signatures for Microsoft Office 365 Exchange Online

Microsoft Exchange Server

For organizations that require the specific customization capabilities of a traditional, individually-operated e-mail server, we support the Microsoft Exchange Server product on Microsoft Windows Server platforms.

- New deployments and upgrades: Microsoft Exchange Server 2016 or newer
- Present deployments:
    - Microsoft Exchange Server 2013 (end-of-life April 2023)
    - Microsoft Exchange Server 2010 (end-of-life January 2020)

Specifications will be based on Microsoft's best practices unless otherwise agreed.

Additional Supported Options

- Aldridge Email Protection Services (EPS) hosted e-mail antispam/antimalware service

- *See: Microsoft Windows Servers and Hypervisors*

File and Collaboration Services

Microsoft SharePoint Online

Part of the Microsoft Office 365 cloud services suite, Microsoft SharePoint Online is our recommended and best-supported cloud-based file services solution for most organizations.

- Service Requirements
  - Active, maintained subscription to the Microsoft SharePoint Online service
  - Aldridge global administrative access to your Microsoft Office 365 tenant, via either:
    - Designation of Aldridge as your Microsoft CSP (Cloud Solutions Provider)
    - Designation of Aldridge as a Partner of Record (POR)
- Client Requirements
  - As per current, published Microsoft SharePoint Online guidance; in general:
    - A current Internet web browser client released within the last (3) years
    - Microsoft Windows 10 Professional or Enterprise is recommended
    - Use of the Microsoft OneDrive synchronization client is recommended
    - A smartphone or mobile device with an operating system released within the last (2) years (for mobile Microsoft Office suite and content access)
  - Local machine storage is recommended, sufficient to cache individuals' often-used files

Additional Supported Options

- Aldridge Managed Backup for Microsoft Office 365 SharePoint Online

Microsoft Windows Server

For organizations with content, applications, or storage requirements that aren't appropriate for Microsoft SharePoint Online, we support the file storage and sharing features of Microsoft Windows Server.

- *See: Microsoft Windows Servers and Hypervisors*

Database Services

Microsoft SQL Server

Deployed as an on-premise resource or a cloud-hosted application, we're able to provide platform support for the Microsoft SQL Server database product.

- Supported Versions
  - New deployments and upgrades: Microsoft SQL Server 2016 or newer
  - Present deployments:
    - Microsoft SQL Server 2014 SP2 (end-of-life July 2024)
    - Microsoft SQL Server 2012 SP4 (end-of-life July 2022)
    - Microsoft SQL Server 2008 R2 SP3 (end-of-life July 2019)
    - Microsoft SQL Server 2008 SP4 (end-of-life July 2019)
- Typical Minimum Platform Requirements
  - Specifications will be based on anticipated load, scale, and processing goals
  - (1) CPU allocated
  - 8GB memory allocated (24GB recommended)
  - 100GB operating system volume
  - Dedicated SQL data volume recommended
  - Dedicated SQL logs volume recommended
  - Dedicated SQL backups volume recommended
- Deployment
  - Specifications will be based on Microsoft's best practices unless otherwise agreed
  - Simple Recovery Mode recommended
  - SQL + Active Directory integrated authentication recommended

The Microsoft SQL Server product must operate upon a supported Microsoft Windows Server platform.

- *See: Microsoft Windows Servers and Hypervisors*

Remote Desktop Services

Microsoft Windows Server

For organizations needing to have multiple users remotely access a desktop computing environment published from within your office network, we recommend the licensed Remote Desktop Services feature of the Microsoft Windows Server 2016 operating system.

- New deployments and upgrades: Microsoft Windows Server 2016 or newer
- Present deployments: as per Microsoft Windows Server supported versions
    - Note that Microsoft Remote Desktop Services implementations based on versions of Microsoft Windows Server prior to 2012 R2 use the prior generation of remote desktop graphics optimization and may experience significant performance issues displaying complex images and large graphics.
    - Note that Microsoft Remote Desktop Services implementations based on versions of Microsoft Windows Server prior to 2012 R2 use driver-based remote printer support, versus driver abstraction and print stream redirection; Remote Desktop Services users on platforms prior to 2012 R2 may experience significant printer reliability, performance, and compatibility issues.

Specification and deployment will be based on Microsoft's best practices unless otherwise agreed.

- *See: Microsoft Windows Servers and Hypervisors*

Citrix Virtual Desktops, Citrix Virtual Apps

Recommended for environments needing a larger scale or more-robust feature set than the native Microsoft Windows Server Remote Desktop Services offers, we support the addition of the Citrix Virtual Desktops (formerly Citrix XenDesktop) and Citrix Virtual Apps (formerly Citrix XenApp) products.

- New deployments and upgrades: Citrix Virtual Apps, Citrix Virtual Desktops v1808 or newer
- Present deployments:
    - Citrix XenApp, XenDesktop 7.x
    - Citrix XenApp, XenDesktop 6.x for Server 2008 R2 (end of life January 2020)
    - Citrix XenApp, XenDesktop 5.x (end of life January 2020)

Specification and deployment will be based on Microsoft's and Citrix's best practices unless otherwise agreed.

- *See: Microsoft Windows Servers and Hypervisors*

Productivity Applications and Services

Application Suites

- Recommended: Microsoft Office (via Microsoft Office 365 services subscription)
- Supported:
    - Microsoft Office 2016 (end-of-life October 2025) or newer
    - Microsoft Office 2013 (end-of-life April 2023)
    - Microsoft Office 2010 (end-of-life October 2020)
- Note that older Microsoft Office suites, while still supported by the manufacturer, are generally no longer receiving security updates and product fixes, and are increasingly incompatible with current Windows operating systems and other applications and services. While a given Microsoft Office version may still be supportable, it may not be compatible or sustainable with other elements of your broader IT environment.

Voice Services

- Recommended: Aldridge Hosted VoIP Services

Fax Services

- Recommended: eFax Corporate

On-Premise Servers and Storage Appliances

Physical Servers

Supportable technical specifications for new purchases.

- Brand
  - Recommended: HP
  - Supportable: Dell
- Memory (RAM)
  - 32GB minimum (appliances); 64GB recommended
- Storage
  - Dedicated RAID controller supporting at least RAID 0, 1, 10, 5, 6
  - RAID controller hot spare support recommended
  - At least 1GB of flash-memory RAID cache (FBWC)
  - Drive interface and media specified by intended use and performance
- Connectivity
  - Minimum (2) 1Gbps Ethernet wired connections
  - Wake on LAN support enabled
  - USB-3 or higher
- Management
  - Out-of-band management with IP KVM enabled (HP Advanced ILO, Dell DRAC)
  - Thermal monitoring and overheat protection
  - SNMP monitoring support
- Resiliency
  - Dual redundant power supplies recommended for most configurations
- Warranty
  - Manufacturer hardware warranty must be maintained for all server platforms
    - 24x7 4 hour onsite recommended for business-critical servers
    - 8x5 Next Business Day onsite acceptable for less-critical servers

Storage Area Network (SAN) Appliances

Supportable technical specifications for new purchases.

- Brand
  - Recommended: Quantum
  - Supportable: HP, Dell
- Controllers
  - Hot swappable dual redundant drive controllers
  - Cache mirroring
- Storage
  - Either:
    - Configurable RAID support for RAID 1, 10, 5, 6, 50, 60
    - or managed redundancy and dynamic performance tuning by load type
  - Hot swappable drives
- Feature Sets Supported
  - VMware certified for use with ESX
  - Microsoft certified for use with Microsoft Windows Server
  - SNMP monitoring support
  - HTTPS web console management
  - Replication support
  - Snapshotting support
  - Volume Copy support
- Connectivity
  - Minimum (4) 1Gbps wired Ethernet interfaces (2 per redundant controller)
  - (4) 10Gbps wired Ethernet interfaces recommended
  - iSCSI protocol support
- Resiliency
  - Hot swappable dual redundant power supplies, minimum
  - At least one hot spare drive maintained
- Warranty
  - Manufacturer hardware warranty must be maintained for all SAN platforms
    - 24x7 4 hour onsite recommended
    - 8x5 Next Business Day onsite acceptable

Network-Attached Storage (NAS) Appliances

Network-Attached Storage Appliances are appropriate for second-tier, archival storage. NAS appliances should generally not be used for primary business storage or critical business information. If you must use NAS within your organization and you're using an alternative solution, we'll work with you to plan transitioning to a supported solution.

- Supported: Aldridge Managed Network Attached Storage (NAS) with Cloud Backup and Restore

Microsoft Windows Servers and Hypervisors

Virtualization Hypervisors

- Recommended
  - VMware ESX 6.7 (on-premise installations) or newer
    - ESXi (no-license-cost edition) for single-host and unclustered environments
    - ESX Essentials Plus for environments with 2 to 3 clustered hypervisor hosts
    - ESX Standard for environments requiring vMotion online moves
  - Microsoft Azure cloud hosting (cloud installations)
- Supported
  - Microsoft Aldridge Cloud (cloud installations)
  - Microsoft Windows Server Hyper-V (on supported Windows Server versions)
  - VMware ESXi 6.5 (end-of-life November 2021)
  - VMware ESXi 6.0 (end-of-life March 2020)

Microsoft Windows Server

- Supported Versions
  - New deployments and upgrades: Microsoft Windows Server 2016 or newer
  - Present deployments:
    - Microsoft Windows Server 2012 R2 (end-of-life October 2023)
    - Microsoft Windows Server 2012 (end-of-life October 2023)
    - Microsoft Windows Server 2008 R2 (end-of-life January 2020)
    - Microsoft Windows Server 2008 (end-of-life January 2020)
- Typical Minimum Platform Requirements
  - (1) CPU allocated
  - 4GB memory allocated (16GB recommended)
  - 100GB operating system volume
  - Separate, dedicated applications and data volume(s)
- Deployment
  - Specifications will be based on Microsoft's best practices and guidance
  - Recommended deployment is as a virtual machine within a supported Hypervisor