

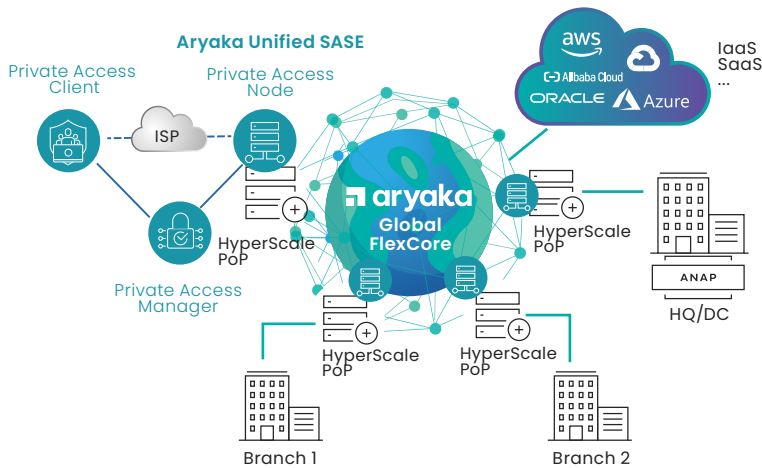
# Aryaka SmartSecure Private Access Datasheet



Private Access Datasheet

## Aryaka SmartSecure Private Access Overview

Aryaka's SmartSecure Private Access solution leverages the performance of Aryaka's global core network with its architectural cloud-first approach to provide the optimal solution for enterprises seeking a "best of both worlds" approach to remote worker connectivity: a solution that combines flexible utilization of deterministic, dedicated network resources to both branch as well as remote workers over a high performance network. This architecture always delivers on maximum performance - irrespective of traffic shifts between branch and remote worker traffic with consolidated visibility into network and application performance across enterprise core connectivity as well as VPN domains.



**HyperScale PoP**

Enable a Global Private Services Core with chaining of WAN, multi-cloud & Security

**ANAP Edge Services CPE**

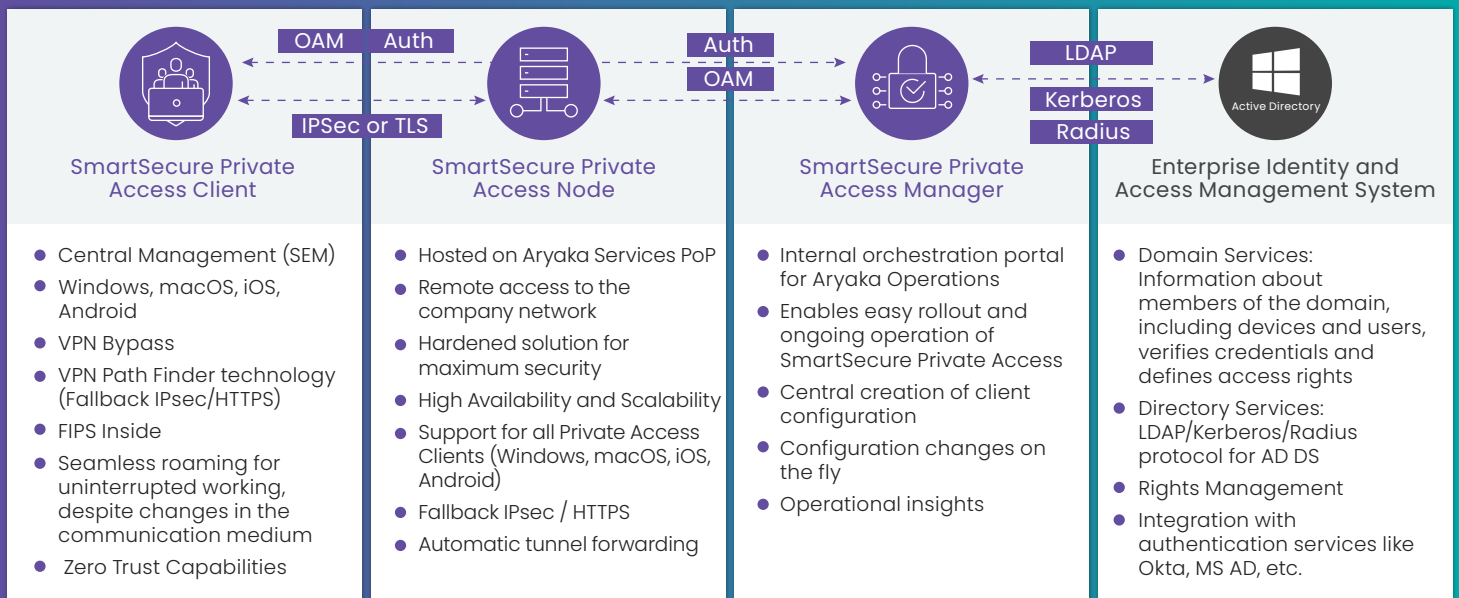
Connects enterprise offices to the Aryaka WAN Services Fabric - hosts VNFs (i.e. NGFW)

**SmartSecure Private Access Node**

Connects remote users to the Aryaka Private Access VPN as-a-Service and global private core for superior performance

Aryaka's Private Access solution is a highly flexible, fully managed virtual private network solution. It leverages Aryaka's global HyperScale PoPs architecture for unified connectivity and management for users anywhere to on-premise and cloud resources. Additionally, Aryaka Private Access users can leverage the full capabilities of Aryaka Unified SASE with the integration of our Next Generation Firewall/Secure Web Gateway (NGFW-SWG) for expanded web traffic and application inspection and security.

SmartSecure Private Access is based on the Enterprise VPN solution by NCP Engineering, a leading VPN provider.



# SmartSecure Private Access consists of the following architectural elements:



SmartSecure Private Access Client



SmartSecure Private Access Node



SmartSecure Private Access Manager

## SmartSecure Private Access Clients

The SmartSecure Private Access solution provides a centrally managed client suite for all major desktop or mobile operating system, including:

Windows

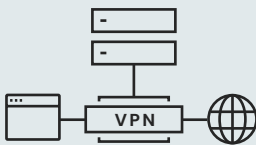
macOS

iOS

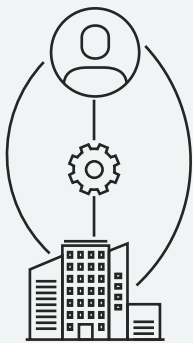
Android



Aryaka's SmartSecure Private Access Clients allow end user devices to select the closest Aryaka PoP for optimal, high-performance network access and reach it with the most effective tunneling protocol.



The SmartSecure Private Access Client ensures robust, unified endpoint compliance. It protects the integrity of the enterprise network by strict VPN access control, which first terminates on the nearest Aryaka SmartSecure Private Access Node and then proceeds to the appropriate private or public DC destination. Traffic travels over the Aryaka FlexCore, delivering the performance benefits of Aryaka's Layer 2 and Layer 3 core network. Zero Trust capabilities are also supported.



The SmartSecure Private Access Client is a communication software product for universal implementation in any remote access VPN environment. It allows remote workers to access applications and data transparently and securely, on-premise or in the cloud, from any location – just as if they were in the corporate office. Seamless roaming provides an optional secure, always-on connection to the corporate network, automatically selecting the fastest medium for access to the internet. When the access point or the IP address changes, Wi-Fi roaming, or IPsec roaming maintains the VPN connection. Even behind firewalls whose settings always block IPsec data connections, the Private Access Client ensures remote access is available by finding an unlocked path. The client supports domain logon using a credential service provider after establishing a VPN connection to the company network.



A bypass function in the Private Access Client allows the IT administrator to configure the client so that certain applications are exempted from the VPN and the data is sent over the internet even when split tunneling is disabled. This prevents applications such as video streaming from unnecessarily taxing the enterprise infrastructure.



All client configurations can be locked by the administrator, meaning that the user cannot change the locked configurations.



The Private Access Client is simple to install and simple to operate. A graphical, intuitive user interface provides information on all connection and security states. Moreover, detailed log information supports effective assistance from the help desk.

## SmartSecure Private Access Node

Aryaka's Private Access Clients connect to the Aryaka Private Access Node closest to them. Aryaka's Private Access Node are a virtual service hosted on Aryaka's global HyperScale PoPs, which provide a sub-30ms onramp to the Aryaka Core Network to 95% of knowledge workers around the planet. Aryaka's HyperScale PoPs host services that go beyond basic network connectivity: network and application acceleration, strict separation of customer-dedicated resources and secure traffic encryption, among others. Web and application security capabilities are also strengthened with the combination of Private Access and Aryaka NextGen Firewall and Secure Web Gateway.

After secure connections are established, the Secure Private Access Node function receives traffic from all the clients accessing it, and routes it across the high performance Global Aryaka FlexCore network to either the enterprise HQ/DC or to a SmartCloud service location that peers optimally given the user's location.

SmartSecure Private Access Node are based on a multi-tenant architecture and a hardened Linux operating system which is optimized for maximum security. Furthermore, the Aryaka HyperScale PoP architecture guarantees deterministic performance and high availability.

SmartSecure Private Access Node can handle a highly scalable number of connections to the company network via an IPsec VPN. The Private Access Clients users can be assigned the same private IP address from a pool assigned by the company each time they connect to the network. This makes remote administration much easier as each user can be identified by their IP address. If the IP address is assigned dynamically from a pool, it will be reserved for the user for a defined period (lease time). Dynamic DNS (DynDNS) ensures that the VPN Gateway is still reachable if the device is assigned a dynamic IP address.

## SmartSecure Private Access Manager





The SmartSecure Private Access Manager provides the configuration and management function for all components in the Aryaka Private Access solution. Together with the Private Access Node, it is also tasked with user authentication via communication with enterprises' existing IAM (Identity & Access Management) systems.

The SmartSecure's Private Access Manager allows Aryaka to provision and manage Private Access Clients and Private Access Node in the PoPs. It also establishes the connectivity with enterprises' over-arching IAM systems for the authentication of Private Access Clients. With this mechanism, the security status of mobile and stationary end devices is verified prior to the device gaining access to the corporate network. All parameters are defined centrally by Aryaka on behalf of the enterprise, and remote workers are granted access rights based on their compliance to them.

SmartSecure Private Access Manager is a key component in providing a VPN solution that is easy to establish and operate.

The Private Access Manager integrates with an enterprise's existing identity management (e.g. Microsoft Active Directory) and requests regular updates. As soon as a new employee is listed in this database, the Private Access Manager creates an individual configuration for this user, according to defined templates. If a former employee has been removed from the database, the Private Access Manager immediately blocks this VPN access. This eliminates the need to manually configure the computers of all mobile employees. The Private Access Manager also enables fast rollout of many users and software certificates.

## Private Access Manager provides the following functions:

 Client Configuration	Private Access Manager provides the configuration and management of all components for the Aryaka Private Access solution. This includes the Private Access Clients for Windows, macOS, iOS and Android. All relevant parameters are predefined and stored in templates.
 Automatic Update Process	The fully automatic update process allows the administrator to centrally provide all remote Private Access Clients with configuration and certificate updates. As soon as the client logs in to the corporate network, the system automatically updates the client. If malfunctions occur during the transmission, then the previously existing configuration remains unaffected.
 License Management (Used only by Aryaka Operators)	The licenses of all connected components are centrally stored in the PAM and managed by Aryaka for enterprise customers. The system transfers them into a license pool and automatically manages them according to specified guidelines. This license transfer might be used for: transfer into a configuration per remote client or gateway, returning the license to the license pool when an employee leaves a company, or triggering a prompt when no more licenses are available.
 System Monitor (Used by Aryaka Operators)	Aryaka can offer enterprises immediate insight into all important events within the SmartSecure Private Access solution. The administrator can use the system monitor as needed to call up status information in real-time, or to access previously saved data repositories for the remote access environment.

# SmartSecure Private Access Benefits



Dramatically improve global VPN performance by leveraging the Global Aryaka FlexCore



Improve end user experience and productivity with deterministic network behavior



Immediate visibility into network, application performance and user experience

## Technical Specifications

### SmartSecure Private Access Client

Universal, centrally administrable VPN Client Suite for Windows, macOS, iOS, Android

Operating Systems	Microsoft Windows, macOS, iOS, Android
Zero Trust Capabilities	<ul style="list-style-type: none"> <li>• Embedded L3/L4/Application Firewall</li> <li>• Least privileged access based on User-ID, device posture and network location with Zero Trust capabilities</li> <li>• Always-on user protection with network access only after user authentication</li> <li>• Zero-Touch Zero-Trust based on device certificates and authentication</li> <li>• Strict admission control policies enforcing device compliance with security policies with quarantine option</li> <li>• Integration with existing MFA (multifactor authentication) and OTP (one-time password) solutions</li> <li>• Next Gen Threat Prevention capabilities with Aryaka Unified SASE</li> </ul>
Security Features	The Enterprise Client supports all major IPsec standards in accordance with the RFCs
VPN Bypass	The VPN Bypass function allows the administrator to define applications which can communicate over the internet directly despite disabling split tunneling on the VPN connection. It is also possible to define which domains or target addresses can bypass the VPN tunnel
Virtual Private Networking	<ul style="list-style-type: none"> <li>• IPsec (Layer 3 Tunneling), IPsec proposals can be determined through the IPsec gateway (IKEv1/IKEv2, IPsec Phase 2)</li> <li>• Event log</li> <li>• Communication only in the tunnel</li> <li>• MTU size fragmentation and reassembly, DPD, NAT-Traversal (NAT-T); IPsec tunnel mode</li> </ul>
Encryption	<ul style="list-style-type: none"> <li>• Symmetric processes: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits</li> <li>• Dynamic processes for key exchange: RSA to 2048 bits; seamless rekeying (PFS)</li> <li>• Hash algorithms: SHA-1, SHA-256, SHA-384, SHA-512, MD5, DH group 1,2,5,14-21, 25-30</li> </ul>
Authentication Processes	<ul style="list-style-type: none"> <li>• IKE (Aggressive Mode and Main Mode, Quick Mode); XAUTH for extended user authentication</li> <li>• IKE configuration mode for dynamic assignment of a virtual address from the internal address pool (private IP)</li> <li>• PFS</li> <li>• PAP, CHAP, MS CHAP V.2</li> <li>• IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): Extended authentication relative to switches and access points (Layer 2)</li> <li>• Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready</li> </ul>

Networking Features	LAN Emulation: Ethernet adapter with NDIS interface, full WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network) support
Seamless roaming	If a communications medium error occurs, automatic switchover of VPN tunnel to another Internet communication medium (LAN/WWAN/3G/4G) without altering the IP address ensures that applications communicating over VPN tunnel are not disturbed and the session to the Private Access Node is not disconnected
VPN Path Finder	Fallback IPsec/ HTTPS (port 443) if port 500 (UDP encapsulation) is not possible
IP Address Allocation	DHCP (Dynamic Host Control Protocol), DNS: Dial-in to the central gateway with changing public IP addresses through IP address query via a DNS server
Communication Media	Internet, LAN, Wi-Fi, GSM (incl. HSCSD), GPRS, 3G, LTE, HSDPA, PSTN
Line Management	<ul style="list-style-type: none"> <li>• DPD with configurable time interval; Short Hold Mode</li> <li>• Wi-Fi roaming (handover)</li> <li>• Timeout (controlled by time and charges); Budget Manager</li> <li>• Connection Modes: automatic, manual, variable</li> </ul>
APN from SIM Card	APN (Access Point Name) defines the access point of a mobile data connection at a provider. If user changes provider, the system automatically uses APN data from SIM card to configure Secure Client
Data Compression	IPCOMP (lzs), deflate
Quality of Service	Prioritization of configured outgoing bandwidth in VPN tunnel (may vary with client OS)
Additional Features	UDP encapsulation, WISPr-support, IPsec-roaming , Wi-Fi roaming, Split Tunneling
Point-to-Point Protocols	PPP over ISDN, PPP over GSM, PPP over Ethernet;LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet Society RFCs and Drafts	<ul style="list-style-type: none"> <li>• RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation)</li> <li>• IP security architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP; RFC 7427: IKEv2-Authentication (Padding-method)</li> </ul>
Client Monitor Intuitive, Graphical User Interface	<ul style="list-style-type: none"> <li>• Multilingual (English, Spanish, French, German); intuitive operation</li> <li>• Configuration, connection management and monitoring, connection statistics, log-files, internet availability test, trace tool for error diagnosis</li> <li>• Display of connection status</li> <li>• Integrated support of Mobile Connect Cards, embedded</li> <li>• Client Monitor can be tailored to include company name or support information</li> <li>• Password protected configuration management and profile management, configuration parameter lock</li> </ul>

## SmartSecure Private Access Node

Remote access to the enterprise network leveraging Aryaka's global core network

### General

Aryaka HyperScale PoP locations

Aryaka has Service PoPs in over 40 worldwide locations, within <30ms of 95% of all knowledge workers world-wide.

Management	Aryaka Private Access Manager provides the provisioning and operations portal – enterprise administrators can gain immediate insights into their VPN deployment
High Availability	Aryaka HyperScale PoPs are built on a highly redundancy architecture and topology to ensure High Availability
Dynamic DNS (DynDNS)	Connection set up via Internet with dynamic IP addresses. Registration of each current IP address with an external Dynamic DNS provider. In this case the VPN tunnel is established via name assignment
DDNS	Connected VPN clients are registered with the domain name server via Dynamic DNS (DDNS), meaning that VPN clients with dynamic IPs can be reached via a (permanent) name
User Administration	Local user administration; OTP server; RADIUS; LDAP, Novell NDS, MS Active Directory Services
Statistics and Logging	Detailed statistics, logging functionality, sending SYSLOG messages
FIPS Inside	<p>The IPsec client integrates cryptographic algorithms based on the FIPS standard. The embedded cryptographic module, containing the corresponding algorithms has been validated as compliant to FIPS 140-2 (Certificate #1747)</p> <p>FIPS compliance will always be maintained when the following algorithms are used for set up and the encryption of a VPN connection:</p> <ul style="list-style-type: none"> <li>• Diffie Hellman-Group: Group 2 or higher (DH starting from a length of 1024 bits)</li> <li>• Hash algorithms: SHA1, SHA 256, SHA 384 or SHA 512 bits</li> <li>• Encryption algorithms: AES 128, 192 and 256 bits or Triple DES</li> </ul>
Client/User Authentication Processes	OTP token, user name and password (XAUTH)
<b>Connection Management</b>	
Line Management	Dead Peer Detection (DPD) with configurable time interval; Timeout (controlled by duration and charges)
Point-to-Point Protocols	LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Pool Address Management	Reservation of an IP address from a pool for a defined period of time (lease time)
<b>IPsec VPN</b>	
Virtual Private Networking	<ul style="list-style-type: none"> <li>• IPsec (Layer 3 tunneling), RFC-compliant</li> <li>• Automatic adjustment of MTU size, fragmentation and reassembly; DPD</li> <li>• NAT Traversal (NAT-T)</li> <li>• IPsec modes: Tunnel Mode, Transport Mode Seamless Rekeying; PFS</li> </ul>
Internet Society RFCs and Drafts	<ul style="list-style-type: none"> <li>• RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation),</li> <li>• IP Security Architecture, ESP, ISAKMP/Oakley, IKE, IKEv2 (incl. MOBIKE), IKEv2 Signature Authentication, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP, IKEv2 authentication compliant to RFC 7427 (padding process)</li> </ul>
Encryption	<ul style="list-style-type: none"> <li>• Symmetric processes: AES (CBC/CTR/GCM) 128, 192, 256 bits</li> <li>• Blowfish 128, 448 bits; Triple-DES 112, 168 bits; Dynamic processes for key exchange: RSA to 4096 bits; Diffie-Hellman Groups 1, 2, 5, 14-21, 25-30</li> <li>• Hash algorithms: SHA-1, SHA 256, SHA 384 or SHA 512</li> </ul>
VPN Path Finder	<ul style="list-style-type: none"> <li>• Fallback to HTTPS from IPsec (port 443) if neither port 500 nor UDP encapsulation are available</li> </ul>

Seamless roaming	The system can automatically transfer the VPN tunnel to a different communication medium (LAN / Wi-Fi / 3G / 4G) without changing the IP address to avoid interrupting communication via the VPN tunnel or disconnecting application sessions
Authentication Processes	<ul style="list-style-type: none"> <li>• IKEv1 (Aggressive and Main Mode), Quick Mode; XAUTH for extended user authentication</li> <li>• IKEv2, EAP-PAP / MD5 / MS-CHAP v2 / TLS</li> <li>• One-time passwords and challenge response systems</li> </ul>
IP Address Allocation	<ul style="list-style-type: none"> <li>• DHCP (Dynamic Host Control Protocol) over IPsec</li> <li>• DNS: Selection of the central gateway with dynamic public IP addresses by querying the IP address via a DNS server</li> <li>• IKE config mode for dynamic assignment of a virtual address to clients from the internal address range (private IP)</li> <li>• Different pools can be assigned depending on the connection medium (Client VPN IP)</li> </ul>
Data Compression	IPCOMP (Izs), Deflate

## SmartSecure Private Access Manager

Centrally Managed VPN as a Service with Fully Automatic Operation of a Remote Access VPN

Supported Functions	Automatic Update, Client Firewall Configuration, System Monitor
User Administration	LDAP, Novell NDS, MS Active Directory Services
Statistics and Logging	Detailed statistics, logging functionality, sending SYSLOG messages
Client/User Authentication Processes	OTP token, user name and password (XAUTH)
Supported RFCs and Drafts	<ul style="list-style-type: none"> <li>• RFC 2138 Remote Authentication Dial In User Service (RADIUS); RFC 2139 RADIUS Accounting; RFC 2433 Microso CHAP</li> <li>• RFC 2759 Microso CHAP V2</li> <li>• RFC 2548 Microso Vendor-specific RADIUS Attributes</li> <li>• RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP); RFC 2716 PPP EAP TLS Authentication Protocol</li> <li>• RFC 2246 TLS Protocol</li> <li>• RFC 2284 PPP Extensible Authentication Protocol (EAP); RFC 2716 Certificate Management Protocol</li> <li>• RFC 2511 Certificate Request Message Format</li> </ul>



+1.888.692.7925

info@aryaka.com

© COPYRIGHT 2015–2024 ARYAKA NETWORKS, INC. ALL RIGHTS RESERVED.

Aryaka is the leader and first to deliver Unified SASE as a Service, the only SASE solution designed and built to deliver performance, agility, simplicity and security without tradeoffs. Aryaka meets customers where they are on their unique SASE journeys, enabling them to seamlessly modernize, optimize and transform their networking and security environments. Aryaka's flexible delivery options empower enterprises to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for cloud-based software-defined networking and security services. For more on Aryaka, please visit [www.aryaka.com](http://www.aryaka.com).

About Aryaka