

HIGHLIGHTS

OneSpan Authentication Server is a comprehensive, centralized and flexible authentication platform designed to deliver complete authentication lifecycle management via a single, integrated system.

It offers secure and seamless access to a variety of corporate resources and (banking) applications, from SSL VPNs to cloud-based apps. It supports OneSpan's entire range of authentication solutions, and simplifies authentication management for both administrators and end users.

AUTHENTICATION SERVER

A software suite for banks and other businesses requiring secure access through proven, state-of-the-art server technology

OneSpan Authentication Server is a centralized authentication server offering strong authentication and validation of transaction signatures. It verifies authentication requests from individuals trying to access the corporate network or business applications.

The solution adds additional security measures to standard username/password logins across a wide range of servers and services. This stops unauthorized logins, even when passwords have been compromised. OneSpan Authentication Server is ideally suited for large and small enterprise network security implementations, application security and online banking security.

Strong, two factor authentication

The combination of OneSpan Authentication Server and Digipass® provides strong user authentication and greater security than static passwords, which expose the organization to data breaches. OneSpan Authentication Server provides a turnkey solution that can be rapidly implemented and operational.

User friendly transaction validation

OneSpan Authentication Server offers highly secure transaction signature validation for banks and financial institutions. Optional features include support for EMV-CAP and Hardware Security Module (HSM) to validate the signature in a secure and tamper-proof environment. By using the latest Cronto® technology, users can enjoy the best experience for their online banking by simply scanning a Color QR Code in order to log in or confirm a transaction.

Interoperability at the front-end

OneSpan Authentication Server uses a non-intrusive method of enabling Digipass authentication. It can be integrated using RADIUS, with Microsoft IIS-based applications such as Outlook Web Access, Citrix StoreFront or Microsoft RDWeb Access, or with any Internet application using SOAP. Additional modules are available for direct plug-in in various third party systems, such as Juniper SBR and Microsoft ADFS3.0/4.0.



OneSpan Authentication Server has an excellent high available design structure, an auto enrollment feature and is fully integrated with Windows Active Directory and Radius services. Together with the web based administrator interface, these features ensure that system administrators are able to work in a transparent and straightforward manner.”

Mohammed Abu-Nejim
Head of Data Networks for Qatargas



DATASHEET AUTHENTICATION SERVER

HIGHLIGHTS

- Can be used out of the box or integrated with existing infrastructure
- Designed to fit the needs of organizations of any size
- Easy to install, manage and support
- Easy to integrate in existing infrastructure
- Efficient tools for helpdesk staff
- Robust and easy expandable with users and applications
- Crono technology ensures an easy and convenient user experience
- Smooth migration, updates and maintenance

Wide Range of Supported Databases

OneSpan Authentication Server supports a wide range of ODBC compliant databases for data storage and ships standard with MariaDB. The Digipass related data can be stored with the users in the ODBC database and synced with Windows user information from the Active Directory.

Convenient web based user interface

All administration functions are available through a web based user interface, allowing remote administration and creating new opportunities for managed security services providers. End user support is efficient and easy to manage thanks to a dedicated overview of all functions that are required and used on a daily basis by helpdesk staff. An intuitive SelfManagement Website allows endusers to manage their software and hardware Digipass without Helpdesk intervention, thus freeing up admin resources.

Extensive auditing and reporting

The audit console monitors incoming and outgoing events on the OneSpan Authentication Server. Data gathered by the audit console provides critical details necessary to effectively manage a remote access environment. Extensive XML or HTML formatted reporting is provided for helpdesk troubleshooting, system- and security auditing, and accounting purposes.

Fits in any environment

OneSpan Authentication Server is available in the widest range of supported platforms: Windows Server, Ubuntu and RedHat distributions, VMware, Hyper-V and Citrix virtual environments, as well as dedicated appliance formats.



The integration went smoothly and quickly. OneSpan's Professional Services team and the technical team supported the integration well. In addition, the configuration with our NBF Direct online banking application was also done swiftly, thus allowing us to enhance two-factor authentication for our corporate banking customers in a quick and easy way. With this additional layer of security, we have made our customers even happier with NBF's services and level of customer engagement."

Nasar Siddiqui

Head of Electronic Channels for National Bank of Fujairah

FEATURES	
• Supports Digipass two-factor authentication, Cronto QR and transaction data validation	
• Supports EMV-CAP and Hardware Security Module (HSM)	
• Supports RADIUS and Microsoft IIS web server-based clients (Outlook Web Access, Citrix StoreFront, Remote Desktop Web Access)	
• Supports Office365 via ADFS3.0/4.0 and SBR	
• Supports Internet hosted applications via SOAP	
• Supports wireless protocols & the return of RADIUS attributes	
• Validation of Digipass Authentication for Windows Logon for locally connected users, in online and offline mode (W7, W8.1, W10)	
• Active Directory integration, ODBC database support	
• High availability through server replication and load balancing	
• End user Self-Management Website	
• Web-based administration GUI in a single browser window for all administrative functions	
• Dedicated dashboard page	
• Comprehensive audit system, with storage in a database or text file and an optional live audit viewer	
• Activity reporting with output in XML/HTML format	
• SNMP Monitoring	
• Available as Appliance or Virtual Appliance	

COMPLIANCE TO STANDARDS	
Radius	• RFC 2865 and RFC 2866
Wireless	• EAP, PEAP
Authentication	• Digipass OTP (challenge / response, response only) • Digipass Signature (transaction validation) • OATH (event based, time based) • EMV-CAP

SUPPORTED ENVIRONMENTS*	
Operating System (Windows version)	• Windows Server 2008 R2 with SP1 (64-bit) • Windows Server 2012 (64-bit), 2012 R2 (64-bit) • Windows Server 2012 Essentials (64-bit), 2012 R2 Essentials (64-bit) • Windows Server 2016
Operating System (Windows desktop)	• Windows 10 (Including Builds 1511 up to 1809) • Windows Server 2012, 2016
Operating System (Linux version)	• SUSE Linux Enterprise Server 12 (64-bit) • Ubuntu Server 14.04 LTS, 16.04 LTS (64-bit) • RedHat Enterprise Linux version 6.7, 7. x (64-bit) • CentOS 6.x, 7.x (64-bit)
Virtual Images	• VMWare ESXi Server version 5.5, 6.0, 6.5 • Citrix XenServer 6.2, 6.5SP1, 7.0 • Microsoft Hyper-V (WS2008 R2, WS2012, WS2012 R2; WS2016)
Supported Web servers	• Apache Tomcat version 8.5.37 • IBM WebSphere Application Server 8.5.5 Should include Java: JRE8, JSP2, JS2.4
Supported Web browsers	• Chrome 51, Firefox ESR45, Internet Explorer 11, Microsoft Edge 25
Data store (DBMS)	• Oracle 12c release 2 (64-bit, Linux, Windows) • Microsoft SQL Server 2016 with AlwaysOn Support, R2SP3, 2012SP2, 2016 (Windows) • MariaDB 10.2.16 (Linux, Windows)
Data store (Active Directory)	• Windows Server 2008R2SP1 AD • Windows Server 2012 AD, 2012 R2 AD, 2016 AD
LDAP Back End Authentication	• Windows Server 2008R2SP1 AD • Windows Server 2012 AD, 2012 R2 AD, 2016 AD • NetIQ eDirectory 8.8 SP8 • IBM Security Directory Server 6.3
HSM	• SafeNet ProtectServer Gold, Orange, Express • SafeNet ProtectServer External 2, Internal-Express 2 • Thales nShield Connect, Solo (on selected platforms)



OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.



Copyright © 2019 OneSpan North America Inc., all rights reserved. OneSpan™, Digipass® and Cronto® are registered or unregistered trademarks of OneSpan North America Inc. and/or OneSpan International GmbH in the U.S. and other countries. All other trademarks or trade names are the property of their respective owners. OneSpan reserves the right to make changes to specifications at any time and without notice. The information furnished by OneSpan in this document is believed to be accurate and reliable. However, OneSpan may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use. **Last Update January 2019.**

CONTACT US

For more information:

info@OneSpan.com

www.OneSpan.com