



customer care solutions

from Nuance



Nuance VocalPassword™ 8.2 :: Product Description



About Nuance VocalPassword™

Nuance is proud to present VocalPassword™ 8.2, the most secure, accurate, flexible, and easily deployed biometric speaker verification platform available in the market today. VocalPassword is an advanced biometric speaker verification system that verifies a speaker's identity based on voice samples acquired during interaction with voice, Web, or mobile applications. The release of VocalPassword 8.2 concludes over 12 years of intensive research and development efforts, as well as unparalleled experience in the deployment of voice biometrics technology and solutions worldwide with successful large-scale deployments in the financial, telecommunications, healthcare, enterprise, and government sectors. VocalPassword 8.2 delivers exceptional ease of integration and deployment, enabling customers to utilize the biometric power of voice to protect personal self-service applications and provide secure, efficient, and convenient access to contact centers and remote applications.



Key Features

- Text-dependent, text-independent, and text-prompted verification
- Liveness detection, utterance validation, and optional ASR functionality for knowledge-based verification
- Language-and accent-independent functionality
- Unsurpassed state-of-the-art accuracy
- Web service interfaces for quick, easy, and secure integration
- Integrated security and role-based authorization
- Multi tenancy, scalability, and multi-site high availability
- Web-based applications for stakeholders; security & fraud officers, technical support personnel, system administrators (domain experts) and customer service representatives
- A comprehensive set of tools and services that facilitate and expedite pilots and proof of concepts

Key Benefits

- Multi-factor security for voice, mobile Web applications, and transactions
- Improved efficiency via reduced agent handling time and increased automation
- Enhanced customer experience
- Effective risk management

Product Overview

VocalPassword is designed as a secure and scalable enterprise infrastructure that can support multiple applications and uses. The system's future proof multi-engine architecture concurrently runs Nuance's state-of-the-art language and accent-independent text-dependent, text-independent, and text-prompted speaker verification engines. These engines and additional algorithmic capabilities, such as utterance validation and liveness detection, allow for diversified verification and identification flows, meeting a range of security and customer experience requirements. VocalPassword's field-proven state-of-the art accuracy, advanced product security, and rich set of features, tools, and capabilities enable organizations to easily and successfully plan, install, integrate, roll out, and support small- and large-scale voice biometrics deployments.

Advanced Web-based applications provide stakeholders (i.e., security personnel, customer service representatives, system administrators, and domain experts) with easy access to tools and information, ensuring deployment success.

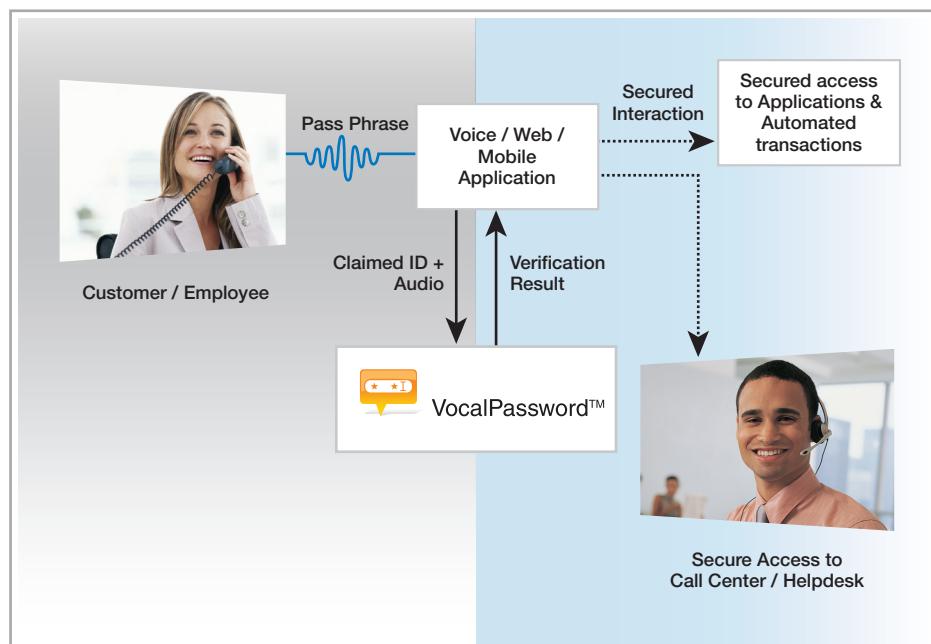
VocalPassword enhances operational security and the customer experience, while significantly reducing the costs and risks associated with remote authentication. VocalPassword has been rated as one of the world's leading biometric speaker verification technologies. VocalPassword was selected by leading financial services, telecom and security organizations, and IVR/voice platform vendors and system integrators worldwide as the speaker verification platform of choice. New features available in VocalPassword 8.2 ensure end-to-end security, meeting the most stringent IT security requirements.

BASIC FUNCTIONALITY

Text-dependent Speaker Verification

Using a passphrase to identify the speaker

- Enrollment – Enrollment is performed using three consecutive renderings of the selected passphrase. The passphrase can be in any language or accent and should contain at least 2 seconds of audio.
- Verification – VocalPassword verifies the speaker by comparing a single repetition of the enrolled passphrase to the voiceprint stored in the system's voiceprint repository. Several repetitions of the speaker's passphrase can be added and linked together to obtain a single score or decision.



- Identification – Speaker identification is carried out by comparing a single repetition of the speaker's passphrase to a list of voiceprints owned by the speaker or multiple speakers.

Text-independent - Speaker Verification

Using the speaker's voice alone

- Enrollment – Text-independent enrollment is performed using samples of the speaker's unconstrained voice. While a voiceprint can be trained using a few seconds of voice, additional voice samples will provide a more robust voiceprint.
- Verification – Text-independent verification is performed by comparing a speaker's voice sample (unconstrained speech) to a voiceprint stored in the system's voiceprint repository.
- Identification – Speaker identification is carried out by comparing the speaker's voice sample to a list of voiceprints or a predefined group.

Text-prompted Speaker Verification

Using a unique prompt, that is, a random subset of trained speech atoms (i.e., digits and words)

- Enrollment – Enrollment is performed using three samples of the speaker's voice repeated in predetermined utterances containing the designated speech atoms. The enrollment phrases (or sequences) are provided by the system and are defined using a preconfigured dictionary. In order to allow for language and accent independency, the target speech atoms (defined as seeds) are predefined in the system. No ASR engine is required.
- Verification – Text-prompted verification is performed using a phrase that contains a randomized subset of the speech atoms provided during enrollment. The speaker repeats the phrase, and the system verifies the speaker by comparing the speaker's voice sample to the voiceprint stored in the system's voiceprint repository. The verification phrase is provided by the system to the application in real time based on a predefined verification dictionary.
- Identification – The calling application generates the prompt as in the verification process. The speaker repeats the phrase, and the system verifies the speaker by comparing the speaker's voice to a list of voiceprints owned by the speaker or multiple speakers.

ADVANCED FUNCTIONALITY

Mitigating Recording Threats

The threat of fraudsters using voice recordings of legitimate speakers

- Liveness detection (Intra-session voice variation) – This unique and patented method significantly reduces recording threats. Following text-dependent verification, this method uses text-independent voice biometrics technology to compare the voice sample captured during the text-dependent verification process, with an additional sample captured by prompting the speaker to repeat a random or semi-random sentence. By combining the obtained biometric scores and validating that the speaker indeed repeated the requested utterance (using VocalPassword's Utterance Validation engine or ASR), a liveness detection score is extracted.
- Prompted passwords verification – Prompted verification requires the user to repeat a random phrase that is a subset of speech atoms (digits/words) trained during enrollment. Prompted verification provides protection against interception and playback attacks, as each session uses a different subset of the trained speech atoms.
- Playback detection – VocalPassword's patented playback detection algorithm runs as part of the verification process and identifies audio segments that unnaturally match audio segments that were previously used for verification/enrollment.

Detecting Known Fraudsters

Using watch-lists

- Fraudster detection – Nuance's award-winning fraudster detection capability allows the system to keep track of known fraudsters. In a common passphrase scenario (i.e., "My voice is my password"), this functionality analyzes enrollment/verification audio in real-time and alerts the application whenever a known fraudster is detected. Unique algorithms reduce the false alarm rate.

Enrollment Validation

Ensuring successful enrollment to achieve the best results

- Validating enrollment text – VocalPassword guarantees that the spoken phrase is the correct phrase using one of two options:
 - Utterance Validation. This is performed by VocalPassword using a proprietary algorithm. This algorithm is based on a background model that is trained as part of the system's setup (relevant when using common passphrase/s for enrollment/verification).
 - Automatic Speech Recognition. Using Nuance Recognizer (NR9/NR10) as an optional add-on, VocalPassword evaluates the audio captured and checks that it contains the required text.
- Enrollment consistency check – This algorithmic functionality validates that multiple enrollment utterances are consistent with one another in terms of their content and biometric features.
- Adaptation – By using new audio to update existing voice templates, VocalPassword allows each speaker to maintain an accurate voiceprint according to changing background noises and voice tones that shift with age.

Using VocalPassword for Knowledge-based Authentication

As an additional authentication layer

- Secret passphrases – VocalPassword can be used for Knowledge-Based Verification by enrolling text-dependent voiceprints that contain the answers to verification questions.
- ASR functionality – VocalPassword's ASR add-on can be used to validate the speaker's answers. This requires the relevant language model and grammar to be in place.

VocalPassword Flexibility

Customize VocalPassword to fit your needs

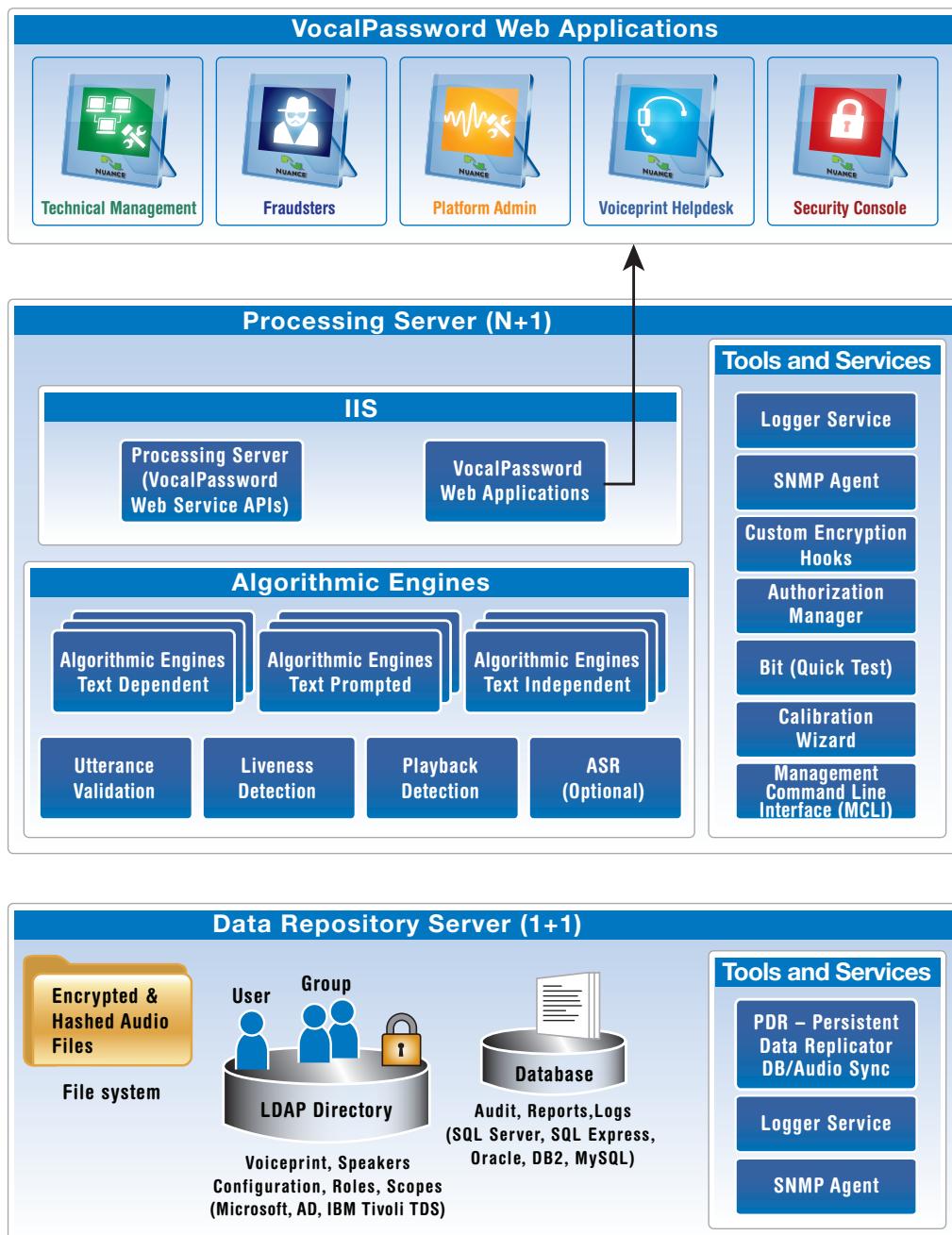
- Multiple configurations and calibrations – VocalPassword allows for use of multiple configurations and calibrations concurrently.
- Decision mechanisms – VocalPassword's built-in decision mechanisms may be overridden by ones designed by the customer through a custom plug in.
- Multiple voiceprints per speaker – VocalPassword allows for the enrolling of multiple voiceprints per speaker promoting security and language support.
- Audio formats – Besides built-in support for several standard telephony formats, any audio format can be supported through the audio format plug-in.

SYSTEM ARCHITECTURE

VocalPassword contains two components: the Processing Server and the Data Repository Server.

The Processing Server is the main processing unit of the VocalPassword system. It hosts the speaker verification engines, which perform algorithmic processing, control client services, and acquire audio through API calls. Multiple servers can optionally be used in a redundancy scheme for high availability purposes or in a load-balancing scheme for scalability. The Processing Server also hosts the Web applications used by system administrators, domain experts, helpdesk/contact center agents, etc.

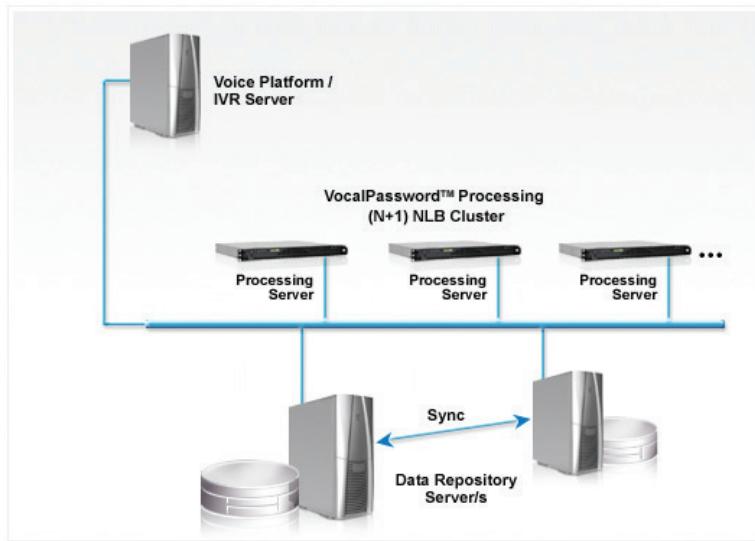
The Data Repository Server is responsible for storing the system and voiceprint data. It runs the system's database, LDAP Directory, and the file system (for audio recording storage). VocalPassword supports the use of two synchronized Data Repository Servers for high availability using a dedicated service (PDR – Nuance's data replicator).



DEPLOYMENT AND INTEGRATION

Scalability

VocalPassword scales up by utilizing multiple Processing Servers. The system's advanced Web service APIs enable client applications to work with any Processing Server. Scalability is achieved using standard load-balancing tools, such as Microsoft NLB clustering service and hardware-based network load-balancing solutions. Nuance VocalPassword 8.2 was tested for stability and response times under extreme load conditions.



High Availability

Nuance's products are designed to deliver constant, stable, and reliable service, securing customer-facing applications. Through the use of multiple Processing Servers and/or multiple Data Repository Servers, VocalPassword allows for a distributed architecture with no single point of failure, ensuring continuous service, 24/7. Configuration changes and voiceprint versioning mechanisms allow for system administration and upgrade with no disruption of service.

- Database cluster – VocalPassword's Data Repository Server can operate in a database cluster architecture (i.e., SQL Server cluster and Oracle RAC). This architecture is usually implemented at a single site and provides high availability by using at least two servers and highly reliable hardware and networks.
- Multiple data repositories – Each VocalPassword Processing Server can work with two Data Repository Servers (primary and secondary), optionally located in different sites. When the primary data repository is inaccessible, the Processing Server automatically switches to the secondary data repository in order to save the information. VocalPassword includes a real-time synchronization module that synchronizes two Data Repository Servers. Each Data Repository can be deployed on a cluster.

Multi-tenancy

VocalPassword 8.2's multi-tenancy capability allows for the logical partitioning of the entire system in a secure and effortless manner through the use of scopes. This allows for a clear-cut separation of the system's data, configuration, audit, roles, etc., within an organization, enabling a single enterprise to use VocalPassword for multiple/distinct applications in different business units. Multi-tenancy is ideal for a hosted solution, enabling a service provider to offer VocalPassword as a service for multiple enterprises. Regardless of which system tool is used or what API method is executed, any operation is performed in the context of a specific scope. Scopes are assigned to users/customers by the system security administrator.

VocalPassword Web Applications



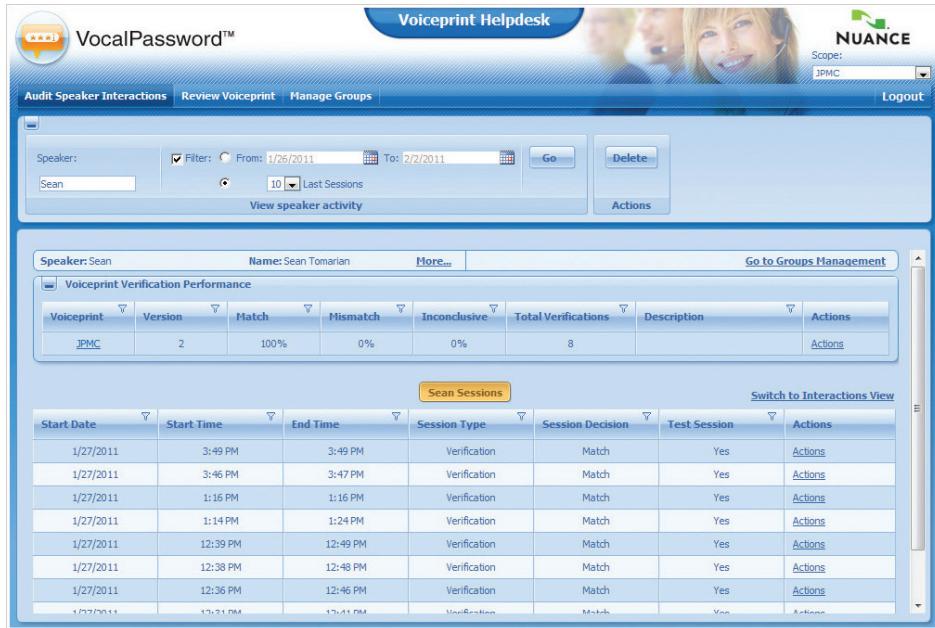
- VocalPassword's Platform Admin is a Web-based application that provides a variety of tools for properly setting up the system and its biometric functionality as well as managing speakers, voiceprints, and groups. Users can utilize this application to configure VocalPassword, perform queries and reports, and monitor system usage.



The screenshot shows the VocalPassword Platform Admin interface. On the left, a sidebar lists various engine components: Verification, Playback detection, Training, Text prompted, Text validation, Fraudsters detection, ASR, Liveness detection, Biometric decision, Enroll, Dictionary, and Audit. The main panel displays configuration settings for the 'Engine' section under three categories: Vox, Enrollment consistency, and Tones. Each category has a 'Main' tab with specific parameters like VoxVPThreshold (0.7), TextConsistencyThreshold (0), and IgnoreAudioAfterSilence (False).



- VocalPassword's Voiceprint Helpdesk provides a set of tools allowing for auditing and reviewing of a speaker's interactions with the system. Users can utilize Helpdesk functions to audit verification results and decisions, edit speaker information, delete a speaker, edit a voiceprint, and more.



The screenshot shows the VocalPassword Voiceprint Helpdesk interface. At the top, there are tabs for 'Audit Speaker Interactions', 'Review Voiceprint', and 'Manage Groups'. The main area shows a search bar for 'Speaker' (Sean) and date filters ('From: 1/26/2011' to 'To: 2/2/2011'). Below this is a table titled 'Voiceprint Verification Performance' for speaker Sean Tomarian, showing details like Version (2), Match (100%), and Inconclusive (0%). Further down, a table titled 'Sean Sessions' lists interactions from 1/27/2011 to 1/27/2011, including Start Date, Start Time, End Time, Session Type, Session Decision, Test Session, and Actions.



- VocalPassword's Technical Management is an application enabling technical personnel, who are in charge of the system's health, to monitor VocalPassword's system components' status, audit system-wide logs, schedule administrative tasks, such as audio purging, upload and view system licenses, and more.



- VocalPassword's Security Console is an application enabling security personnel to audit VocalPassword operations and analyze specific verification and identification processes. The application provides tools for managing fraudster's voiceprints and groups. In addition, Security Console collects and presents diversified security alerts.

Security Console

The VocalPassword Security Console Application enables security personnel to audit VocalPassword operation and analyze specific verification and identification processes. The application provides tools for managing fraudsters voiceprints and groups. In addition, the security console collects and presents diversified security alerts.

Authorization Manager

User Management

The VocalPassword Security Console Authorization Manager functionality allows managing all aspects of User Authorization. Authorization Manager is a general-purpose role-based security architecture for Windows. Using roles, the operating system can make determinations, such as whether a process is privileged to perform an action. VocalPassword utilizes Microsoft's Authorization Manager infrastructure to manage user authorization in the system.



- VocalPassword Fraudsters application supplies all the tools needed in order to perform real-time fraudster detection when identity theft is attempted. Use the application to manage fraudster and watchlist entities, analyze suspicious audio segments, and compare them to known fraudster voiceprints. An extensive reporting mechanism is available for audit purposes.

EVALUATION TOOLS

Evaluation Studio

- Evaluation Studio is a revolutionary product that addresses the need to professionally plan, test, and analyze voice biometrics systems and technologies. Nuance Evaluation Studio is used for benchmarking different vendor's products, evaluating, piloting and rolling out a selected product, or just researching voice biometrics technology and its underlying performance.

Experiment Results

Step	Description	Value
Step 1 - Overview	Overall Status	Success
Step 2 - Test Repository	Test Type	One-to-one
Step 3 - Calibration Repository	Calibration Type	One-to-one
Step 4 - Configuration	Configuration Type	One-to-one
Step 5 - Execution Plan	Execution Plan Type	One-to-one
Step 6 - Execution	Execution Status	Success
Step 7 - Result View	Result View Status	Success
Step 8 - Summary	Summary Status	Success

Experiment Media

File Name: TestAudioFile_1.wav

Error Rates Graph

Graph View | Details View

Legend: — False Accept Rate — False Reject Rate

Y-axis: Percentage (0-100)

X-axis: Time (00:00:00.000 - 00:00:30.000)

Data series: False Accept Rate (red line) starts at ~95% and drops to ~5%; False Reject Rate (green line) starts at ~5% and rises to ~95%.

- VocalPassword Fraudsters – Application supplies all the tools needed in order to perform real-time fraudster detection when identity theft is attempted. Use the application to manage fraudster and watchlist entities, analyze suspicious audio segments, and compare them to known fraudster voiceprints. An extensive reporting mechanism is available for audit purposes.

Technical Management Tools

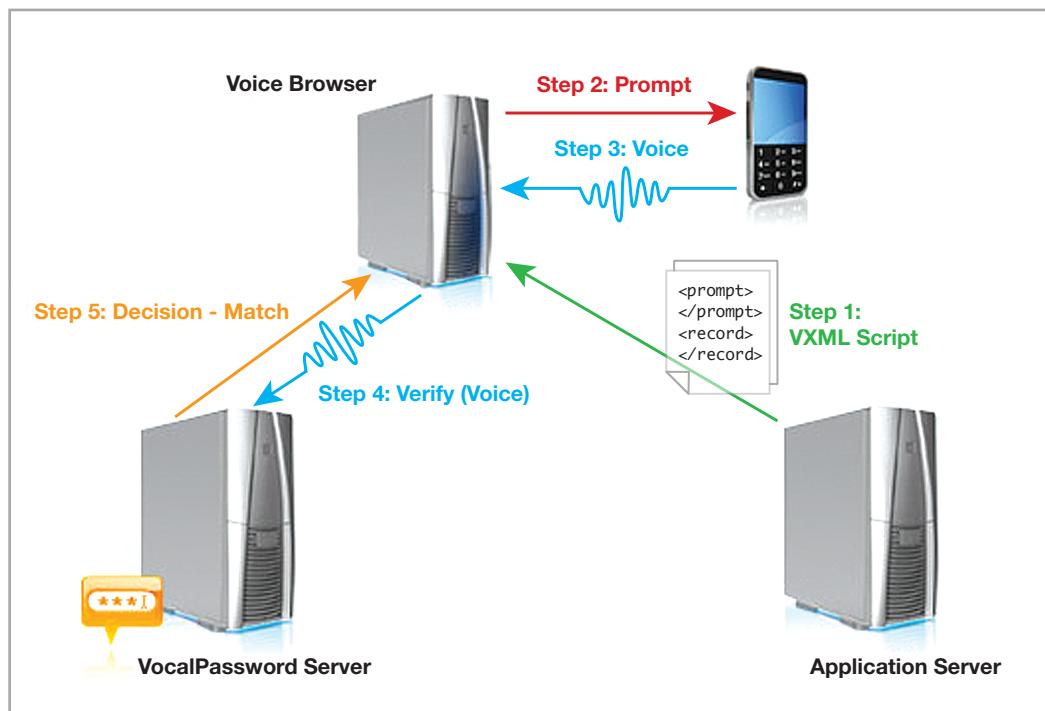
- QuickTest – QuickTest is a simple application that invokes a predefined BIT (built-in-test), which includes a set of operations, simulating a complete voiceprint's life cycle.
- SNMP Agent – Each Processing Server has an SNMP agent service that handles SNMP get/set requests and sends SNMP traps when important system events occur. VocalPassword monitoring can be easily added to standard SNMP-based consoles.
- MCLI (Management Command-Line Interface) – MCLI is an extensive set of command-line based tools for immediate or batch system administration.
- Calibration Wizard – Calibration Wizard is a Windows application allowing for system calibration using customer-supplied audio files. Calibration is required for optimizing system accuracy.
- Performance Counters – VocalPassword utilizes Windows Performance Counters. These counters provide information as to how well the VocalPassword system is performing. The counter data can help determine system bottlenecks and fine-tune application performance.”

Interfaces

VocalPassword 8.2 uses an enhanced, open, and flexible Web service API, ensuring smooth, platform-independent integration using any programming environment. The VocalPassword API is session aware, allowing users to associate multiple API calls with a single session and applying a session decision logic.

- VocalPassword Server API – VocalPassword's Server Web Service methods are used by client applications to perform operational functions, such as enrollment, verification, identification, and voiceprint administration. Enrollment and verification audio can be supplied to VocalPassword as part of an API call or provided as a URL to a previously recorded audio file. The API is fully compatible with VXML 2.0. Integration can be done directly from the VXML script, without passing through the application server.
- VocalPassword Manager API – VocalPassword Manager Web Service methods are used by the administration applications. The Manager API allows for system-level operations, such as changing configurations and uploading licenses.
- VocalPassword Explorer Extensions – VocalPassword Explorer Extensions enable users to send audio files to VocalPassword for processing in a straightforward manner. Available operations include Enrollment, Verification, and Identification. For example, a user can select three audio files containing a speaker's rendering of a passphrase from Windows Explorer, and create a voiceprint in VocalPassword by selecting the “Enroll” option under the VocalPassword item in the context menu. Alternatively, the user can select a folder containing hundreds of audio files and evaluate them against a stored voiceprint by initiating a “Verify” operation. Once an Explorer Extension operation is selected, a corresponding pop up message is displayed, prompting the user to enter required information. Operation status is reported back to the user as a message box in the Windows task bar. Verify and Identify operations generate a result file that can be processed by standard tools like Excel and Notepad.

- VocalPassword Platform Integration with Voice XML Platforms – VocalPassword has been successfully integrated with leading VoiceXML platforms using both VBScript and JavaScript. Integration with any VoiceXML platform can be easily accomplished using Nuance's sample code and VoiceXML scripts. VocalPassword natively supports calling its API using VXML data tag. Nuance is an active member of the VoiceXML SIV group and has contributed to the adoption of speaker verification functionality as part of VoiceXML 3.0.

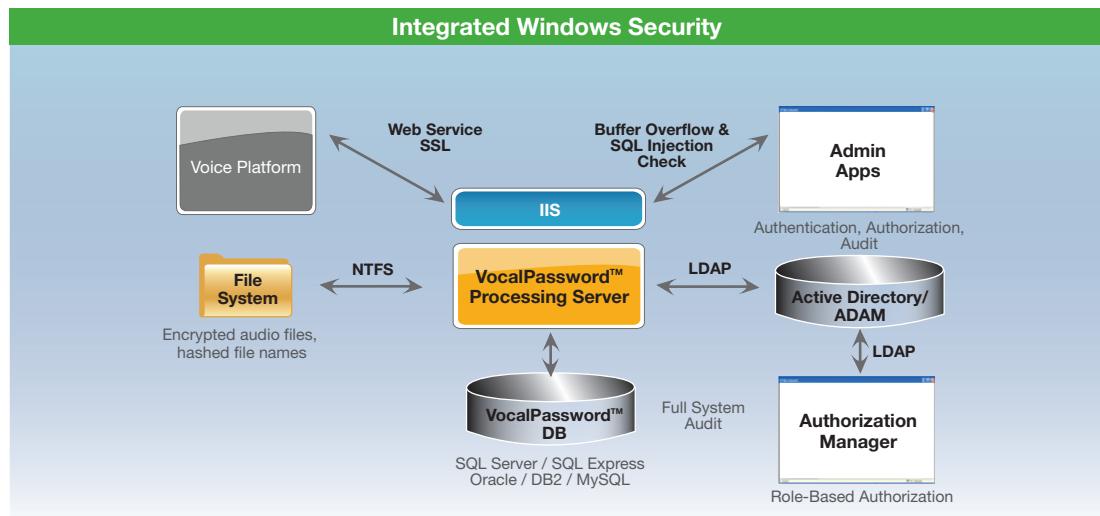


Security Features

VocalPassword's security design and features are based on the Common Criteria Protection Profile for biometric systems and has successfully passed third-party security audits performed by customers. VocalPassword 8.2 ensures data and system protection by implementing the following security measures:

- Role based authorization – Access to system applications, resources, and services is governed by roles which can be customized to meet specific security needs.
- Database access – Database access is protected by integrated Windows security or by using an encrypted username and password mechanism.
- PII & Audio Encryption – personally identifiable information and Audio encryption is supported with VocalPassword's built-in encryption mechanism, as well as with HSM (hardware security module) and custom encryption mechanisms.

- Voiceprint security – Voiceprints are stored in a proprietary format in the system's LDAP directory and cannot be reverse engineered. Voiceprint IDs are signed using a unique key and cannot be used outside the system or in other VocalPassword systems.
- Interface protection – Access to the system service (API) is controlled using IIS6 or IIS7 security supporting SSL encryption All authentication schemes are supported: Integrated, Basic, Digest, and Certificates.
- Audit and audit protection – A full audit trail is stored in the system's database. All voiceprint usage and manipulation records are available and stored securely in the system.
- Administration access control – Administration and configuration applications utilize integrated security.
- Input validation – Input validation serves as protection against SQL and LDAP injection, buffer overflow, and XSS attacks.



Quality Standard

VocalPassword is developed by Nuance Communications, under a quality system certified as complying with ISO 9001:2008 by the international Standards Institution.

Awards

VocalPassword – Best Implementation Awards



Speech Technology
Magazine 2010
Implementation Award
(Vodafone Turkey)



Speech Technology
Magazine 2008
Implementation Award
(Bell Canada)

System Requirements

Recommended Hardware

Processor	2 X Quad Core CPU
Memory	4GB
Storage	20GB

Software

Operating System	<ul style="list-style-type: none"> Windows 2003 – 32 bit Enterprise Edition & Standard Edition SP2 Windows 2008 R2 – 64 bit Enterprise Edition & Standard Edition SP2 Windows 7 – 64/32 bit Enterprise Edition & Professional Edition
Web Server	IIS6 and up
Database	SQL Server 2005 & 2008, SQL Express, Oracle 11g with RAC support, DB2 9.5, MySQL 5.5
Browser	Explorer 8.0 and up, Mozilla Firefox 3.5 and up
LDAP Server	ADAM, AD LDS, Active Directory, TDS (Tivoli Directory Server) 6.2

Selected Specification

Minimum VoicePrint Audio	2 seconds, 3 repetitions
Audio Format	8 bit Alaw, 8bit Ulaw, 8/16bit Linear, Custom (via CODEC plug-in)
VoicePrint Size	50K-100K
Management Protocol	SNMP V2
API	SOAP (XML/HTTP), HTTP (Get/Post)

about Nuance Communications, Inc.

Nuance Communications (NASDAQ: NUAN) is a leading provider of voice and language solutions for businesses and consumers around the world. Its technologies, applications and services make the user experience more compelling by transforming the way people interact with information and how they create, share and use documents. Every day, millions of users and thousands of businesses experience Nuance's proven applications and professional services. For more information, please visit www.nuance.com.

©2012 Nuance Communications, Inc. All rights reserved. Nuance, the Nuance logo, The experience speaks for itself, Verifier, VocalPassword, SpeakFreely, and Prodigy are trademarks and/or registered trademarks of Nuance Communications, Inc., and/or its subsidiaries in the United States and/or other countries. All other trademarks are the properties of their respective owners. DS 072312 NUCC1021