

customer care solutions

from Nuance



white paper ::

Automated Password Reset Security Overview

table of contents

introduction	3
about nuance	3
physical security	4
application and network management	4
communication security	4
access control	5
data confidentiality and integrity	6
operating system baseline	6
intrusion detection systems	7
audit and logging	7
for more information	8

introduction

The Nuance Automated Password Reset (APR) Application is a complete, integrated hardware and software platform for voice security. Users are identified based on their unique voice signature (“voiceprint”); the authentication process and any subsequent conversation can be recorded and archived, and a searchable audit trail created. APR functions over any telephone. With APR, an organization will be able to:

- positively authenticate callers with biometric voice verification;
- automate interactions with speech recognition or touch-tone;
- record conversations;
- create a searchable audit trail of all interactions.

This document provides an overview of APR’s security features and recommended security practices for operating the server.

about nuance

Nuance is the leading provider of speech and imaging solutions for businesses and consumers around the world. Our 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 by calling directory assistance, getting account information, dictating patient records, telling a navigation system their destination, or digitally reproducing documents that can be shared and searched. Making each of those experiences productive and compelling is what Nuance is all about.

We comprise the world’s largest portfolio of speech and imaging products backed by the expertise of our professional services organization and a partner network that can create solutions for businesses and organizations around the globe. So whether it’s switching to speech to improve customer service or business productivity, or simplifying the way people work with documents, Nuance has the solution.

With the increasing threat of ID fraud, the ability to remotely verify a customer’s identity has never been more important. With APR, Nuance offers an important tool in the fight against ID fraud. The solution can also play in a key role in addressing compliance concerns. APR is being used today for telephone-based wire transfers, PIN/password resets and other critical customer and employee interactions.

Biometric voice verification is more secure and convenient than current telephone and computer verification methods. Every person has a unique vocal pattern, or “voiceprint”, that APR can use to verify identity. Unlike all other types of biometrics, voice does not require expensive scanners for verification – just a telephone.

Nuance has specialists in IT security, audio signal processing and interface design who work to ensure that the company’s solutions are both highly secure and user-friendly. Through strong R&D, the company is at the forefront of voice security technologies. For more information, please visit www.nuance.com/care

physical security

Good physical security of the APR is required in order to ensure strong information security.

It is recommended that the APR be deployed in an environment that meets the physical security requirements detailed in the enterprise security policy. As a rack mounted server system, the APR system is optimally located within a controlled access server room.

The following basic physical security precautions should be considered when locating and installing the APR server:

Physical Location

The APR should be located in a locked and secured room.

Access Control

Access to the APR location should be restricted to authorized personnel only. A control log should be used to record entry and exit from the space. The control log should be reviewed at periodic intervals.

Power

The APR should be protected from potential power loss/spikes with an uninterruptible power source (UPS).

application and network management

APR can be managed like any application server that resides on the enterprise network. Typically, a system administrator is assigned to undertake the duties of monitoring and managing system performance.

APR can be integrated into existing system management processes such as backup and recovery, OS patch control, and general system maintenance.

communication security

APR transmits and receives sensitive corporate data over the enterprise network to back-end identity management systems and databases. In order to protect this data, appropriate security controls must be in place for the physical network and data flows.

Communication transmission attacks can be categorized in two high-level domains:

- **Passive attacks** – an attacker monitors a communication flow.
- **Active attacks** – an attacker actively seeks out network and/or communication vulnerabilities for potential compromise.

In order to protect from these types of attacks, APR uses SSL (HTTPS) to cover corporate network connections. SSL is pre-configured at the time of installation of the APR system and includes the following measures:

- A fixed IP address assigned to the APR.
- A fixed DNS name pre-configured for the APR.
- A SSL certificate is requested and assigned for use with the APR.

access control

The APR access control model is based upon the principle of least privilege. APR protects resident data by controlling access to server data through group permissions, encrypting server files, and encrypting the onboard database.

The APR database provides application-level access control including password control to identify users. In this fashion, database users are permitted specific capabilities and subsequent control at greater or lesser levels of access granularity.

By assigning user IDs and passwords, the database administrator controls access to the database. By granting permissions to each user ID, the database administrator controls what tasks each user can carry out when connected. The APR system utilities and client connections are separated into specific user groups with varying levels of access and permissions.

The permission scheme is based on user IDs. When a user logs onto the database, he has access to all database objects that meet any of the following criteria:

- objects to which he received explicit permission.
- objects to which a group to which he belongs received explicit permission.

The user cannot access any database object that does not meet these criteria. In short, users can access only the objects to which they explicitly received access permissions.

The APR system administrator logon process is controlled through Windows authentication. The logon process is therefore standardized on the implementation of Active Directory access control. Access to the APR utilities is controlled through user name and password as configured and managed by the system administrator. The logon process is therefore also standardized on the implementation of Active Directory access control.

- **Administrator:** Administrator level access is required in order to make changes to the APR itself and also to the APR database.
- **General User:** The APR Clients consist of the utilities and telephony sessions generated as a result of the system receiving telephone calls. Access to APR system resources are strictly controlled and made available based upon the principle of least privilege.

The following user rights are pre-configured with APR.

- **Access this computer from the network**
Default: Administrators, Backup Operators, Everyone, Power Users, and Users
Recommended: Administrators, Authenticated Users

- **Allow log on locally**
Default: Administrators, Backup Operators, Power Users, and Users
Recommended: Administrators, Backup Operators, Power Users

- **Shut down the system**
Default: Backup Operators, Power Users, Administrators
Recommended: Administrators

data confidentiality and integrity

APR encrypts user voiceprints with a FIPS 140-2 approved cryptographic method. Federal Information Processing Standard 140-2 is the US Government standard that provides a benchmark for implementing cryptographic software. The Microsoft Windows 2003 default cryptographic services providers (CSPs) have completed FIPS-140-2 evaluation and these CSPs are employed within APR for encrypt/decrypt and hashing functions.

operating system baseline

Nuance ensures that APR security features will perform correctly and effectively by applying the Microsoft® Windows Server Common Criteria Security Template. One of the key tangible benefits of the Common Criteria Certification is that it provides guidance that simplifies the deployment and operations of Windows in a secure networked environment.

The Common Criteria (CC) is a repeatable methodology for documenting IT security requirements, documenting and validating product security capabilities, and promoting international cooperation in the area of IT security. The CC was established to replace the security criteria and processes used in various participating countries with a common criteria and process. This recognition has been formally established as the Mutual Recognition Agreement (MRA). The US participant in the MRA is the National Information Assurance Partnership (NIAP), a partnership between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

Use of Common Criteria “protection profiles” and “security targets” greatly aids the development of products or systems that have IT security functions. The rigor and repeatability of the Common Criteria methodology provides for thorough definition of user security needs.

APR ships with all applicable current OS and component patches. Nuance provides APR OS patches and system updates as a standard function of customer support.

intrusion detection systems

Nuance APR does not ship with a host-based IDS.

APR integration with IDS systems is described as follows:

- **Network Based IDS:** APR exists on the enterprise network as a typical application server. Depending on the variant of IDS, APR IP traffic will be identified and added to the IDS knowledge base of approved network communications.
- **Host Based IDS:** Should a host-based IDS be required for installation on the APR system, it is requested that the application software be provided to Nuance for testing prior to shipping of the APR system. This will allow Nuance to test the system with the IDS installed to verify there is no performance conflict or degradation of performance. Should performance issues be identified, these will be addressed and rectified by Nuance.

audit and logging

Audit logs are an important measure to identify and analyze suspicious activity.

APR can determine what transactions have occurred and who is responsible for each transaction. Each transaction is time-stamped and identified with the originator of the transaction. These auditing features are provided via three methods; Operating System Audit Logs, Database Audit Logs, and APR Transaction Audit Trail.

Auditing is a way of keeping track of the activity performed on the database. The record of activities stays in the database transaction log and includes the following:

- All login attempts (successful and failed), including the terminal ID;
- Accurate timestamps of all events (to a resolution of milliseconds)
- All permissions checks (successful and failed), including the object on which the permission was checked (if applicable)
- All actions that require DBA authority
- The transaction log

Since anyone with administrator access to the APR can alter or remove audit logs, it is strongly recommended that periodic archives of audit logs are automatically performed and saved to a different server, managed by different administrators. Windows 2000 and Window 2003 provide various audit logs through the "Event Viewer". Additionally, IIS provides configurable logging information with W3C Extended Log File Format. Regular examinations of the audit log are strongly recommended.

for more information

Contact us today to learn how Nuance can help your organization fight fraud and save money with cost effective, convenient and secure applications delivered on APR, the most comprehensive and readily deployable solution for voice verification.

Contact us at 1-866-968-2623 and say "sales department", by email eps.sales@nuance.com or visit our website: www.nuance.com/care

© 2008 Nuance. All Rights Reserved. Nuance is a registered trademark of Nuance. All other trademarks mentioned here are the property of their respective holders. WP05/08 NUCC100