VASCO
THE AUTHENTICATION COMPANY

IDENTIKEY
Authentication Server

IDENTIKEY® Authentication Server

Release Notes

3.12 R2

Intellectual Property

VASCO Software, documents and related materials ("Materials") made available on the Site contain proprietary and confidential information. All title, rights and interest in VASCO Software and Materials, updates and upgrades thereof, including software rights, copyrights, patent rights, trade secret rights, sui generis database rights, and all other intellectual and industrial property rights, vest exclusively in VASCO or its licensors. No VASCO Software or Materials published in this Site may be downloaded, copied, transferred, disclosed, reproduced, redistributed, or transmitted in any form or by any means, electronic, mechanical or otherwise, for any commercial or production purpose, except as otherwise marked or when expressly permitted by VASCO in writing.

Disclaimer

VASCO accepts no liability for the accuracy, completeness, or timeliness of Site content, or for the reliability of links to and content of external or third party websites.

VASCO shall have no liability under any circumstances for any loss, damage, or expense incurred by you, your company, or any third party arising from the use or inability to use VASCO Software or Materials, or any third party material available or downloadable from the Site. VASCO will not be liable in relation to any loss/damage caused by modification of these Legal Notices or Site content.

Reservation

VASCO reserves the right to modify these Notices and the content at any time. VASCO likewise reserves the right to withdraw or revoke consent or otherwise prohibit use of the VASCO Software or Materials if such use does not conform to the terms of any written agreement between VASCO and you, or other applicable terms that VASCO publishes from time to time.

Trademarks

VASCO®, VACMAN®, IDENTIKEY®, aXsGuard®, DIGIPASS®, CertiID®, CRONTO™, MYDIGIPASS.COM™, the MYDIGIPASS.COM MD Lock logo, the DP+ logo, the VASCO 'V' logo, and the CRONTO logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries.

VASCO reserves all rights to the trademarks, service marks and logos of VASCO and its subsidiaries.

Copyright

1. Introduction

Welcome to **IDENTIKEY Authentication Server 3.12 R2**!

This release replaces the IDENTIKEY Authentication Server 3.12 release. It includes all IDENTIKEY Authentication Server 3.12 features and fixes and provides additional functionality.

> **Note**
> Upgrading from IDENTIKEY Authentication Server 3.12 to this release is not supported.

IDENTIKEY Authentication Server is a server product designed to support the deployment, use, and administration of VASCO DIGIPASS technology. IDENTIKEY Authentication Server can be easily integrated with existing applications using a Software Development Kit (SDK).

IDENTIKEY Authentication Server supports the following primary functions:

- DIGIPASS one-time password authentication
- DIGIPASS signature validation
- Software DIGIPASS provisioning
- Administration and reporting
- Auditing

IDENTIKEY Authentication Server is designed to be easily usable with web applications, and also features an **Administration Web Interface**.

This document covers the following topics:

- New features and enhancements
- Fixes and other updates
- Known issues

For more information about configuring and using IDENTIKEY Authentication Server, refer to the respective documentation.

2. New Features and Enhancements

2.1. Maker–Checker Authorization

This version introduces support for maker–checker authorization. This process requires two different individuals to complete administrative commands, i.e. certain operations initiated by one administrator (**maker**) can only be executed after approval and authorization by another administrator (**checker**).

Currently, maker–checker authorization applies to the following operations:

- Creating a user
- Deleting a user
- Assigning a DIGIPASS authenticator
- Unassigning a DIGIPASS authenticator

The maker–checker authorization process is optional. By default, it is disabled.

2.2. New Client Component Type for DIGIPASS Gateway Clients

DIGIPASS Gateway is a new, pre-defined SOAP-based Client Component used for DIGIPASS Gateway clients in the context of Push Notification. Unlike other SOAP clients it does require a valid license key in the client component record. It does not require SOAP authentication to be enabled in the IDENTIKEY Authentication Server license.

IDENTIKEY Authentication Server supports DIGIPASS Gateway 4.0 and later.

2.3. New Authentication Method: IDENTIKEY Authentication Server Supports Push Notification for DIGIPASS App

IDENTIKEY Authentication Server now supports a new authentication method: Push Notification for DIGIPASS App via VASCO Notification Gateway. **Push Notification** is an out-of-band (OOB) authentication method that uses a push mode to enable the **DIGIPASS App** on a mobile device to authenticate a user. The user receives a notification prompt on the mobile device during the authentication process, and completes the authentication process by tapping on the device. Refer to the new DIGIPASS Push Notification - Getting Started Guide, available in the IDENTIKEY Authentication Server delivery package, for more detailed information. The Message Delivery Component (MDC) has been extended to support this new feature: the new **Push Notification message** delivery method has been added.

A new standard report has also been created in the context of this new feature. The **Canceled Authentication Trend** is a Trend Analysis Report and shows on a monthly basis a trend of push–notification-based authentications that were canceled or timed out. It is created as default report during installation and upgrade of IDENTIKEY Authentication Server.

You can use Push Notification as an alternative authentication mode for DIGIPASS Authentication for Windows Logon. The support of Push Notification for DIGIPASS Authentication for Windows Logon has been improved: you can configure IDENTIKEY Authentication Server to generate offline authentication data (OAD) during a successful Push Notification–authentication (for subsequent offline authentication using a one-time password (OTP)).

2.4. Limiting Multi-Device Licensing Provisioning Activations

This version of IDENTIKEY Authentication Server introduces a provisioning activation count for MDL activations per DIGIPASS license. This count limits the number of activations, when activating a DIGIPASS authenticator with the provisioning command. If the maximum number of activations has been reached, no further DIGIPASS instances can be created.

An administrator can reset the provisioning activation counter.

2.5. Deleting instances of a DIGIPASS authenticator compliant with Multi-Device Licensing

The administration of DIGIPASS authenticators has been extended: when unassigning a DIGIPASS license of a DIGIPASS authenticator compliant with Multi-Device Licensing, the pertaining DIGIPASS instance or instances are now also automatically deleted. This action is **not reversible**, i.e. the deleted instances cannot be recovered!

2.6. Supported Platforms, Data Management Systems, and Other Third-Party Products

IDENTIKEY Authentication Server 3.12 supports the following new platforms, systems, and third-party products:

VASCO Authentication Platform

VACMAN Controller version 3.17.0 has been integrated in IDENTIKEY Authentication Server 3.12.

Runtime Environment

The Web Administration Service and the IDENTIKEY User Websites require the following components to be installed:

- Oracle Java Runtime Environment (JRE) 8 Update 131

Web Servers (Administration Web Interface)

- Apache Tomcat 8.5.13

Virtualization Platforms

- VMWare ESXi 6.5

3. Fixes and Other Updates

Issue 71194: Support for Back-End Authentication with Push Notification

Description: When using Push Notification for user authentication and back-end authentication is set to **Always**, this setting is ignored. Authentication via Push Notification with back-end authentication only succeeds if back-end authentication is set to **None** or **If Needed**.

Affects: IDENTIKEY Authentication Server 3.12.0

Status:This issue has been fixed.

Issue 69912 (Support Case PS-176458): Incomplete List of RADIUS Support Limitations (Documentation)

Description: Virtual DIGIPASS OTP requests are not possible with CHAP or MSCHAP, which is not mentioned in the IDENTIKEY Authentication Server Administrator Guide.

Status: The documentation has been updated.

Issue 69834 (Support Case PS-177354): Unbind Device Information Is Missing (Documentation)

Description: The IDENTIKEY Authentication Server Administrator Guide does not provide information about unbinding a DIGIPASS for Mobile authenticator from a mobile device.

Status: The documentation has been updated.

Issue 69749: Vulnerability CVE-2016-8747 in Apache Tomcat

Description: Vulnerability CVE-2016-8747 allows remote attackers to obtain data that is unrelated to the current request.

Affects: IDENTIKEY Authentication Server 3.11.1

Status: This issue has been fixed. IDENTIKEY Authentication Server has been updated to use Apache Tomcat 8.5.13.

Issue 69749: Web Administration Service No Longer Requests a Client Certificate

Description: The Web Administration Service no longer requests a client certificate when connecting to IDENTIKEY Authentication Server.

Issue 69685 (Support Case PS-177669): Description of Max Days Between Authentications Is Incomplete (Documentation)

Description: The IDENTIKEY Authentication Server Administrator Reference and the Administration Web Interface Help do not contain information about setting **Max Days Between Authentications** to **0** in a policy.

Status: The documentation has been updated.

Issue 68773 (Support Case PS-176606): User Auto-Unlock Does Not Work Correctly for Primary Virtual DIGIPASS (Authentication)

Description: The user auto-unlock mechanism does not correctly support Primary Virtual DIGIPASS. This issue occurs if user accounts are set to support Primary Virtual DIGIPASS only. When such a user account is locked, and the user attempts to automatically unlock the account by requesting a one-time password (OTP) using the configured request method, the request for an OTP is considered an invalid authentication attempt. This effectively keeps the account locked for an additional lock duration and decreases the number of unlock attempts.

Affects: IDENTIKEY Authentication Server 3.9–3.11

Status: This issue has been fixed.

Issue 68565 (Support Cases PS-173999, PS-170431, PS-160073): No Multiline Support in MDC Email Message Templates (Web Administration Service)

Description: In previous versions, the Message Delivery Component (MDC) default message settings were configured per server using the **IDENTIKEY Authentication Server Configuration Utility**. Since IDENTIKEY Authentication Server 3.8 the MDC default message settings are configured on a solution-wide scope for all servers using **Web Administration Service**. During that change the support for multiple lines in email templates has been dropped.

Affects: IDENTIKEY Authentication Server 3.8–3.11

Status: This issue has been fixed. Multiple lines are supported again in MDC email templates for Virtual DIGIPASS, virtual signature, offline authentication data, and delayed activation notifications.

Issue 68453 (Support Case PS-176203): Inconsistency Between Ciphers and Enabled TLS Versions in Apache Tomcat

Description: TLS 1.0 and TLS 1.1 are enabled although only ciphers are available that require TLS 1.2.

Affects: IDENTIKEY Authentication Server 3.9–3.11

Status: This issue has been fixed. TLS 1.0 and TLS 1.1 are now disabled by default.

Issue 67345: Vulnerability CVE-2017-5638 in Apache Struts (Web Administration Service)

Description: Vulnerability CVE-2017-5638 allows remote attackers to execute arbitrary commands via a `#cmd=` string in a crafted Content-Type HTTP header.

Affects: IDENTIKEY Authentication Server 3.8–3.11

Status: This issue has been fixed.

Issue 67300 (Support Case PS-174825): Description of Limitation in Score- and CHAP-Based RADIUS Authentication Missing (Documentation)

Description: Score-based DIGIPASS applications do not support CHAP-based RADIUS authentications. IDENTIKEY Authentication Server documentation lacks a description of this limitation.

Affects: IDENTIKEY Authentication Server 3.4.x–3.11.x

Status: This issue has been fixed.

Issue 67158: Unsupported Settings Used in Default DIGIPASS Authentication for Windows Logon Policies

Description: The default policies provided for DP Windows Logon are configured to inherit the value for the Primary Virtual DIGIPASS Request Method policy setting from the parent policy, i.e. Base Policy. The effective setting is Password, which is invalid, because DP Windows Logon does not support the virtual DIGIPASS request mechanism and relies on another channel to retrieve a Virtual DIGIPASS, such as IDENTIKEY User Self-Management Website or IDENTIKEY Authentication Server Web Administration Service.

The following policies are affected:

- Windows Logon Online and Offline Auth – LDAP AD Back-End
- Windows Logon Online and Offline Auth – Windows Back-End
- Windows Logon Online Authentication – LDAP AD Back-End
- Windows Logon Online Authentication – Windows Back-End

Affects: IDENTIKEY Authentication Server 3.5–3.11.x

Status: This issue has been fixed. The affected default policies have been adapted to use the correct and supported policy setting.

Note that the existing default policies or any custom policies are not changed during an upgrade to this version. Adapt the affected default policies and any custom policies used for DP Windows Logon clients by setting the value for Primary Virtual DIGIPASS Request Method to None. If you are just using default policies you can also run the Restore Default Policy and Report Definitions Wizard (via the **Configuration Wizard**).

Issue 66776: Changes in IDENTIKEY Authentication Server not Effective in Database (IDENTIKEY Authentication Server)

Description: On installations of IDENTIKEY Authentication Server certain database changes are not saved.

Affects: IDENTIKEY Authentication Server 3.11

Status: This issue has been fixed.

Issue 66468 (Support Case PS-174389): Screen Shot in Installation Guide for Windows Shows Incorrect Upgrade Path (Documentation)

Description: In the description for configuring an ODBC deployment of IDENTIKEY Authentication Server after an upgrade the Installation Guide for Windows contains a screen shot with an incorrect upgrade path.

Affects: IDENTIKEY Authentication Server 3.11

Status: This issue has been fixed.

Issue 65997: getSecureChallenge and genRequest SOAP Commands Fail for Bluetooth DIGIPASS)

Description: The `getSecureChallenge` and `getSigningRequest` SOAP commands are failing for a user with a Bluetooth DIGIPASS.

Status: This issue has been fixed.

Issue 65991 (Support Case PS-173693): Provisioning Scenario Module Disabled By Default

Description: Since IDENTIKEY Authentication Server 3.9 the **Provisioning** scenario module does no longer require a license option and is available to all customers. When installing IDENTIKEY Authentication Server, the **Provisioning** scenario module is disabled by default. Furthermore, when loading a new server license file without the provisioning option enabled, the **Provisioning** scenario module is disabled. In both cases, the **Provisioning** scenario module must be (re-)enabled manually in the scenario configuration.

Affects: IDENTIKEY Authentication Server 3.9–3.11.0

Status: This issue has been fixed. The **Provisioning** scenario module is now enabled by default.

Issue 65882 (Support Case PS-173843): Decrypt DIGIPASS Information Message Entry Missing for Administrative Privileges (Documentation)

Description: An entry in the administrative privileges table for decrypt DIGIPASS information message in the IDENTIKEY Authentication Server Administrator Reference is missing.

Status: The documentation has been updated.

Issue 65742 : Set of Rules Determining Secure Channel too Restrictive for DIGIPASS Applications

Description: DIGIPASS applications have a strict set of rules when checking for Secure Channel support.

Affects: IDENTIKEY Authentication Server 3.11

Status: This issue has been fixed. The affected .dpx files (containing DIGIPASS with Secure Channel applications) need to be re-imported to make the fix effective.

Issue 61701: Unbounded Memory Build Up in SOAP Connections in IDENTIKEY Authentication Server

Description: An unbounded memory build up occurs when a SOAP connection is used for subsequent requests in IDENTIKEY Authentication Server during the lifetime of the connection.

Status: This issue has been fixed.

4. Known Issues

Issue 72079: DIGIPASS Control Parameters In Policy Cannot Be Modified (Web Administration Service)

Description: Changes to the DIGIPASS control parameters (specifically the synchronization windows settings) in a policy (via the DP Control Parameters tab in the Administration Web Interface) are actually not applied or saved when clicking SAVE.

Affects: Web Administration Service 3.12

Status: No fix available. To change the respective policy settings use Tcl Command-Line Administration instead.

Issue 59402: VASCO IDENTIKEY Authentication Server Service Fails to Start After Upgrade to IDENTIKEY Authentication Server 3.10

Description: When upgrading from IDENTIKEY Authentication Server 3.9 to IDENTIKEY Authentication Server 3.10, the VASCO IDENTIKEY Authentication Server service fails to start if automatic server discovery was incorrectly configured in IDENTIKEY Authentication Server 3.9. The following error messages are displayed in the Event Viewer:

```
class vasco::ConfigException: Error - 30 in function "DnsUpdate::configure (A service target must be given.)": The configuration is invalid
```

```
class vasco::Exception: Error - 30 in function "ConfigurationManager::configure (Configuration node "DNS-Update")": The configuration is invalid
```

Affects: IDENTIKEY Authentication Server 3.9.x

Status: When configuring IDENTIKEY Authentication Server 3.9 for automatic server discovery without providing a host name, the server appears to accept the empty Host Name field, and the VASCO IDENTIKEY Authentication Server service can be started. Although incorrect configuration of automatic server discovery does not affect authentication services or other server functionality, it leads to issues when upgrading to a more recent IDENTIKEY Authentication Server version.

Therefore, before upgrading to IDENTIKEY Authentication Server 3.10, you need to repair the automatic server discovery configuration in version 3.9, by specifying the host name in the Server Discovery section of the **Configuration Utility**.

Issue 58722: DIGIPASS for Mobile Timeshift No Longer Supported

Description: When the Timeshift feature of DIGIPASS for Mobile is used, it causes the offline data to become invalid. The option to set a timeshift for DIGIPASS for Mobile authenticators is no longer supported. This feature is outdated and has become obsolete because mobile devices are now correctly synchronized with IDENTIKEY Authentication Server at shorter intervals.

Affects: IDENTIKEY Authentication Server 3.6.x-3.10

Status: Do not use the DIGIPASS for Mobile Timeshift feature to avoid the offline data to become invalid.

Issue 58052: Recent Activity Query Permissions Are No Longer Granted If View Audit Information Privilege is Missing

Description: When upgrading to IDENTIKEY Authentication Server 3.8, all administrative users, who already possessed the View User and/or the View DIGIPASS administrative privilege, were additionally granted the View Recent User Activity and/or the View Recent DIGIPASS Activity privilege, respectively. This enabled the respective administrators to use new functionality introduced in IDENTIKEY Authentication Server 3.8, including the User Dashboard.

Affects: IDENTIKEY Authentication Server 3.8.x

Status: This behavior has been changed in IDENTIKEY Authentication Server 3.10. When upgrading to IDENTIKEY Authentication Server 3.10 or higher the View Recent User Activity and View Recent DIGIPASS Activity privileges are each granted only, if the respective user already possesses both the View User and View Audit Information privileges or the View DIGIPASS and View Audit Information privileges, respectively.

Issue 54398: Web Administration Service Cannot Be Displayed in Internet Explorer 10

Description: When trying to access the IDENTIKEY Authentication Server Web Administration Service with Internet Explorer version 10, the page cannot be displayed.

Affects: IDENTIKEY Authentication Server 3.9.x-3.10

Status: Third-party issue - install the Internet Explorer browser fix from Windows Update. Refer to https://technet.microsoft.com/library/security/MS14-066?f=255&MSPPError=-2147217396#ID0E5MAC for more information.

Issue 49355: Installing Web Administration Service with Ubuntu Software Center

Description: On Ubuntu Server 14.04 LTS, when installing Web Administration Service with the Ubuntu Software Center, the Apache Tomcat daemon is not started after the installation. This issue does not occur with other supported Ubuntu versions, or if Web Administration Service is installed via the command line.

Affects: IDENTIKEY Authentication Server 3.9 on Ubuntu Server 14.04 LTS

Status: Start the Apache Tomcat daemon manually after installing Web Administration Service using the Ubuntu Software Center, or install Web Administration Service via the command line.

Issue 48848: Upgrading Remote Administration Web Interface with Other Than Default Name (Upgrade)

Description: When an administrator manually changes the default name (i.e. the IP address) of a remote IDENTIKEY Authentication Server Administration Web Interface deployment, upgrading the Administration Web Interface fails because the Configuration Wizard searches for the IP address as the server name. The system

produces an error message.

Affects: IDENTIKEY Authentication Server 3.8.0 on Linux distributions.

Status: The administrator must delete the manually created entry; after the upgrade the IP address and key file must be again entered manually.

Issue 48452 (Support Case PS-144964): Multiple Authentication and Accounting Ports on IDENTIKEY Authentication Server (RADIUS Communicator)

Description: IDENTIKEY Authentication Server allows for the configuration of two RADIUS authentication ports and two RADIUS accounting ports. By default, one authentication and one accounting port is specified, the second ports can only be edited in the configuration file of IDENTIKEY Authentication Server , not directly in the Administration Web Interface.

Affects: IDENTIKEY Authentication Server 3.5.x - 3.8.x

Status: If a second authentication and/or a second accounting port for the RADIUS Communicator will be used, the port specifications need to be edited in the identikeyconfig.xml file.

Issue 47479: Upgrading Message Delivery Component (MDC) Stand-Alone Installation Fails (Upgrade)

Description: Existing installations where only Message Delivery Component (MDC) is installed cannot be successfully upgraded. Completing the Configuration Wizard fails with a "Generate SSL certificate failed" error message.

Affects: IDENTIKEY Authentication Server 3.6.x, 3.7.x

Status: No fix or workaround.

Issue 47459: New Global Server Settings Not Replicated After Upgrading an Environment with Individual ODBC Databases (Replication)

Description: When upgrading several IDENTIKEY Authentication Server instances in an advanced deployment environment using replication where each instance uses its own ODBC database, each instance creates new settings introduced with a new version in its own global server settings. The new global server settings apply to the particular instances, but **will NOT be replicated** to the other instances during or after the upgrade.

This affects for instance the Message Delivery Component (MDC) message settings migrated from the local to the global configuration settings during an upgrade to 3.8 (thus no change in replication behavior).

Affects: IDENTIKEY Authentication Server 3.8.x using replication with individual ODBC databases

Status: If you want to replicate new global configuration settings after an upgrade, you need to manually copy the database from the first upgraded IDENTIKEY Authentication Server instance to the other ones after upgrading each instance.

For more information, refer to the IDENTIKEY Authentication Server Administrator Guide, Section "Backup and Recovery" > "ODBC Recovery".

Issue 47318: Schema Not Added Completely when Database Collation is Case-Sensitive (ODBC Database Command-Line Utility)

Description: Adding the database schema when the database collation is case-sensitive fails with invalid column reference errors. This affects the ODBC Database Command-Line Utility `dpdbadmin` and any module relying on that utility.

Affects: IDENTIKEY Authentication Server 3.8.x

Status: No fix available.

Issue 47191 (Support Case PS-156982): IDENTIKEY Authentication Server Installation Fails (IDENTIKEY Authentication Server Installation with ODBC Data Store)

When attempting to install IDENTIKEY Authentication Server on a Windows Server 2008 R2, where the server name or any domain part of the host name starts with a number or a special character instead of a letter, the installation fails due to an error in the Java Runtime Environment keytool.

Affects: IDENTIKEY Authentication Server 3.6.x – 3.8.x

Status: The host name must be changed manually to avoid that the name or any domain part starts with a number.

Issue 46294 (Support Case PS-141029): SafeNet Hardware Security Module Mode Setup Causes Installation Failure (IDENTIKEY Authentication Server Installation)

Description: Deployments of IDENTIKEY Authentication Server with **SafeNet HSM** only support HSMs running in Normal mode. If the HSM is run in **High Availability** or **Workload Distribution** mode, the installation of IDENTIKEY Authentication Server fails.

Affects: IDENTIKEY Authentication Server 3.6.x, 3.8.x

Status: The SafeNet HSM must be run in **Normal** mode, i.e. `ET_PTKC_GENERAL_LIBRARY_MODE` must be set to **NORMAL**.

Issue 42477: IDENTIKEY Authentication Server SNMP Agent Persistent Data Storage (IDENTIKEY Authentication Server Linux Installation Script)

Description: The IDENTIKEY Authentication Server SNMP agent cannot store its persistent data (e.g. EngineBoots, EngineID), as the default persistent directory is not created by the installation script. By default, the SNMP Agent stores its persistent data in the /var/net-snmp directory.

Affects: IDENTIKEY Authentication Server setup on an Ubuntu Server 14.04 LTS, with the vasco-netsnmp package installed.

Status: A / var/net-snmp directory must be created and the **vasco-ias** user must have write access to this directory. If this directory does not exist and/or the **vasco-ias** user does not have write access to it, the EngineID and related information used by the IDENTIKEY Authentication Server SNMP agent will not be persistent. This may result in issues on the machine that receives SNMP TRAPv3 traps from IDENTIKEY Authentication Server.

Issue 42427: Warning of Missing nCipher Group not Included in Install Script (IDENTIKEY Authentication Server Linux Installation Script)

Description: In previous versions of IDENTIKEY Authentication Server, the install.sh script for Linux installations issued a warning if the required nCipher group nfast was missing, notifying the user that IDENTIKEY Authentication Server needs to be a member of this group if the nCipher HSM (now: **Thales nShield** HSM) was to be used for cryptographic operations. In versions 3.6.0 and 3.6.1 of IDENTIKEY Authentication Server, this warning is no longer included in the install.sh script.

Affects: IDENTIKEY Authentication Server installed on Linux with **Thales nShield HSM**

Status: This will be fixed in a future release of IDENTIKEY Authentication Server.

Issue 41811: Failure to Uninstall vasco-netsnmp via uninstall.sh on Ubuntu (IDENTIKEY Authentication Server Setup)

Description: When running uninstall.sh on a Ubuntu server, vasco-netsnmp is not removed automatically, and the SNMP management component remains on the client machine. This issue occurs because the vasco-netsnmp Debian packages prerm script fails to include the removal of the /etc/init.d/vasco-netsnmp init script.

Affects: IDENTIKEY Authentication Server setup on a Ubuntu Server 14.04 LTS and Red Hat Enterprise Linux 6 64-bit

Status: To remove vasco-netsnmp and the SNMP management component completely from the client machine, run the /etc/init.d/vasco-netsnmp stop script and remove /etc/init.d/vasco-netsnmp manually before running uninstall.sh.

Issue 41616: Self-Signed Certificates Created By Microsoft Internet Information Services (IIS) Cannot Be Used (Message Delivery Component (MDC))

Description: When trying to configure email delivery with SSL/TLS using a self-signed certificate created using Microsoft Internet Information Services (IIS) and converted to PEM format using OpenSSL, Message Delivery Component (MDC) cannot recognize a valid self-signed certificate and displays an error message. This is caused by the OpenSSL library. In some circumstances, the OpenSSL application itself may display an "Unable to get local issuer certificate (20)" error message.

Affects: All platforms.

Status: No fix available. This is a compatibility issue between OpenSSL and Microsoft IIS. Do not use self-signed certificates generated using Microsoft IIS.

Issue 39791: Configuration Wizard Causes Segmentation Fault When Connecting to Oracle RAC Database

Description: When trying to connect to an existing Oracle database during an advanced installation, the console version of the IDENTIKEY Authentication Server **Configuration Wizard** terminates with a segmentation fault, if the embedded PostgreSQL database has been installed.

Affects: All Linux platforms with Oracle RAC database.

Status: No fix available. Do not install the embedded PostgreSQL database if you want to use an existing Oracle database.

Issue 25333: Undefined TEMP Path Not Supported

Description: A Windows installation will fail if the TEMP environmental variable is undefined or empty.

Affects: All Windows platforms.

Status: No fix available.