# IDENTIKEY® Authentication Server

## Release Notes

3.8

# 1. Introduction

Welcome to **IDENTIKEY Authentication Server 3.8**! 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

This chapter describes the different significant enhancements of IDENTIKEY Authentication Server 3.8.

## 2.1. User Dashboard

The **User Dashboard** of the IDENTIKEY Authentication Server Administration Web Interface allows administrators to easily manage, monitor, and troubleshoot DIGIPASS user accounts, providing the most important user settings and user-specific reporting features in one place.

The Administration Web Interface has been enhanced with the following **User Dashboard** functionalities:

- Administrators can view a summary of recent user or DIGIPASS operations and IDENTIKEY Authentication Server events, including authentication, signature, provisioning and administration actions. The list of recent user or DIGIPASS activities contains detailed information for each record, such as a description of the action, the category it belongs to, the time it was audited, used clients and DIGIPASS (in case of recent user activity), and provides additional troubleshooting information in case of failure.
- The **View Audit Message** page displays the details of an audit message for the user or DIGIPASS recent activity on a single page and provides access to all relevant audit message fields. The administrator can access the View Audit Message page by selecting the relevant audit message code displayed in the **Recent Activity** page. When an administrator accesses audit records through the recent activity commands, this administration action is recorded; all enabled auditing methods are used for this.
- Another feature of the new **User Dashboard** is the **Quick Report** button in the **Dashboard** tab. This button allows an administrator to quickly generate a report for that user. Once the report is generated, the **Summary** page of the **Run Report** wizard opens where the generated report can be opened or a different report configured to be run. By default, a Detailed Activity Summary report is generated.

## 2.2. Additions to Reporting and Audit Scenarios in the IDENTIKEY Authentication Server Configuration Utility

The scenarios in the IDENTIKEY Authentication Server **Configuration Utility** have been extended. In the **Reporting** and **Audit** scenarios, the new **Audit ODBC Settings** tab has been added which includes all configuration settings necessary to successfully connect to the database holding the auditing tables. Also, a new button to test the connection to the data source has been added, and the utility now also displays information about the control table that is used for the database.

## 2.3. Improvements to Audit Message Table Indexes

The index levels for the audit message table (**vdsAuditMsg**) have been revised to improve indexing performance.

The default index level for the audit message table is set to 1 for new installations. This is the recommended setting when using the User Dashboard and reporting. Note that when upgrading an existing IDENTIKEY Authentication Server installation the current index levels are not changed. So you need to set the index level for the audit message table using the `dpdbadmin` command-line tool manually:

```
dpdbadmin addindex –u <dbusername> –p <dbpassword> -d <dsn> -level <lvl>
```

After upgrading an existing IDENTIKEY Authentication Server installation, the User Dashboard (**Dashboard** and **Recent Activity** tabs) does not include historical auditing data for events, which happened prior to the upgrade.

## 2.4. Improvements and Corrections to Various Audit Messages

Some audit messages included incorrect message details, used incorrect field names or omitted curly braces "{ }" in input details, or omitted various output details. The respective audit messages were corrected, including F-001003, F-005005, F-005008, F-010001, S-001003, S-005005, and S-010001.

## 2.5. Global Configuration of Message Delivery Component (MDC) Message Settings

In previous versions, the Message Delivery Component (MDC) default message settings were configured per server in the server configuration file (identikeyconfig.xml). This has been changed; the default message settings are now configured on a solution-wide scope for all servers within an replicated environment. If you upgrade an existing installation, the current message settings are migrated from the server configuration file to the global server settings in the database. If you upgrade several IDENTIKEY Authentication Server instances within a replicated environment, each instance migrates its own message settings to its global server settings without replicating it to the other instances during the upgrade; this means that the global server configuration settings of each instance may differ from each other after an upgrade.

The **Administration Web Interface** displays a separate tab for every message type in the global server configuration where the message settings can be viewed and edited.

Required permissions for this are:

- View Back-End Settings
- Update Back-End Settings

It is no longer possible to configure those settings using the **IDENTIKEY Authentication Server Configuration Utility**.

## 2.6. Multi-Device Licensing and Activation Supported on Linux and All Supported Data Management Systems

As of version 3.8 the **Multi-Device Licensing and Activation** feature of IDENTIKEY Authentication Server is available for all supported Linux distributions and all supported data management systems.

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

> **Warning**
> As of version 3.8, IDENTIKEY Authentication Server **no longer** supports the following:
>
> - **Any** 32-bit server operating system
> - Windows Server 2003
> - IBM DB2

IDENTIKEY Authentication Server 3.8 supports the following new platforms, systems, and third-party products:

### Operating Systems for Client Components

- Windows 8 (64-bit x64)
- Windows 8.1 (64-bit x64)

### Operating Systems for Server Components

- CentOS 6.6 (64-bit x86_64)
- Red Hat 6.6 and 6.5
- Ubuntu Server 14.04.2 LTS (64-bit AMD64)

### Data Management Systems

- Microsoft SQL Server 2014

### Web Servers (Administration Web Interface)

- Apache Tomcat 8.0.21
- IBM WebSphere Application Server 8.5.5

The Administration Web Interface requires the following components to the be installed on the Web server machine:

- Oracle Java Runtime Environment (JRE) 8 Update 45

### Web Browsers (Administration Web Interface)

- Google Chrome 41

### LDAP Servers (Back-End authentication)

- Novell eDirectory 8.8 SP8

### Virtualization Platforms

- Citrix XenServer 6.2

### Hardware Security Modules

- SafeNet ProtectToolkit C 4.3

VASCO Authentication Platform

VACMAN Controller version 3.14.1.1 has been integrated in IDENTIKEY Authentication Server3.8.

### Crypto-Library

- OpenSSL 1.0.1m

# 3. Fixes and Other Updates

### Issue 46237 (Support Case PS-150949): Missing Information in Documentation (Administration Web Interface)

In the IDENTIKEY Authentication Server Installation Guides for Windows and Linux, information related to the mandatory settings in Internet Explorer for the Administration Web Interface were missing. The documents have been updated accordingly.

**Affects**: IDENTIKEY Authentication Server 3.6.x – 3.7.x

# 4. Known Issues

### Issue 48994: Target User ID and Target Domain Audit Fields Include Unresolved User ID and Domain Data (Auditing)

**Description**: When an administrative command is executed, the target user ID and target domain for that command is recorded in the auditing database using the same character casing as the respective command input attributes, regardless how these fields are stored in the IDENTIKEY Authentication Server database.

This means that if you execute administrative commands via the **Tcl Command-Line Administration** using different character casing the commands may complete successfully, but record different target user ID and target domain information in the auditing records. This may prevent those audit messages from being included in the recent user activity (**User Dashboard**).

**Affects**: IDENTIKEY Authentication Server 3.8.x

**Status**: No fix available. This does not affect Administration Web Interface.

### 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 47479: Upgrading Message Delivery Component (MDC) stand-alone installations 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 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 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 45830 (Support Case PS-152814): Upgrading IDENTIKEY Authentication Server version 3.5 to 3.6 Fails (IDENTIKEY Authentication Server Upgrade)

**Description**: IDENTIKEY Authentication Server version 3.5 is installed on Windows 2008 with ODBC as data store and PostgreSQL as database; a second domain is set, and the administrator account is set in the Master Domain. Also, the **Administration Program** policy in IDENTIKEY Authentication Server is customized according to the the domain settings. Under this conditions, when attempting to upgrade PostgreSQL the upgrade fails, and the PostgreSQL service no longer exists on the machine.

**Affects**: IDENTIKEY Authentication Server 3.5.x - 3.6.x

**Status**: Before initiating the upgrade process, re-set the **Administration Program** policy to standard settings.

### Issue 44416: Default Policy for Administration Logon Cannot Be Used in a Multi-Device Licensing Administration Scenario (IDENTIKEY Authentication Server Administration)

**Description**: For IDENTIKEY Authentication Server administration with Multi-Device Licensing and Activation (Two-Step Activation), the default administration policy Identikey Administration Logon is used and operational. Administration with this policy will not be functioning with IDENTIKEY Authentication Server version 3.8.x.

**Affects**: IDENTIKEY Authentication Server 3.7.x

**Status**: The policy Identikey Administration for Multi-Device Activation must be used, which will be enforced in IDENTIKEY Authentication Server version 3.8.0.

### 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 12.04

**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 40727: Oracle Driver Crash (IDENTIKEY Authentication Server Configuration Wizard)

**Description**: When configuring the Oracle database with the IDENTIKEY Authentication Server Configuration Wizard on Linux, the Oracle driver crashes. This crash happens in the libclntsh.so.11.1 function kpusattr within the Oracle driver when setting an attribute.

**Affects**: Oracle ODBC driver on supported Linux distributions

**Status**: No fix available. Use the console version of the IDENTIKEY Authentication Server Configuration Wizard instead.

### 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 11g database during an advanced installation, the **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.