

IDENTIKEY
server

IDENTIKEY Server

Release Notes

Disclaimer of Warranties and Limitations of Liabilities

The Product is provided on an 'as is' basis, without any other warranties, or conditions, express or implied, including but not limited to warranties of merchantable quality, merchantability of fitness for a particular purpose, or those arising by law, statute, usage of trade or course of dealing. The entire risk as to the results and performance of the product is assumed by you. Neither we nor our dealers or suppliers shall have any liability to you or any other person or entity for any indirect, incidental, special or consequential damages whatsoever, including but not limited to loss of revenue or profit, lost or damaged data of other commercial or economic loss, even if we have been advised of the possibility of such damages or they are foreseeable; or for claims by a third party. Our maximum aggregate liability to you, and that of our dealers and suppliers shall not exceed the amount paid by you for the Product. The limitations in this section shall apply whether or not the alleged breach or default is a breach of a fundamental condition or term, or a fundamental breach. Some states/countries do not allow the exclusion or limitation or liability for consequential or incidental damages so the above limitation may not apply to you.

Copyright

Copyright © 2011 VASCO Data Security, Inc., VASCO Data Security International GmbH. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of VASCO Data Security Inc.

Trademarks


VASCO®, Vacman®, IDENTIKEY®, aXsGUARD®, DIGIPASS®, and ® are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries.

Table of Contents

1	Introduction.....	4
1.1	Main Application Versions.....	4
2	New Features and Enhancements.....	5
2.1	Exclusion option for administrator accounts.....	5
2.2	Temporary users.....	5
2.3	Thales nCipher support.....	5
2.4	Improved reporting performance.....	5
3	Fixes and Other Updates.....	6
3.1	Fixed a DUR issue on Windows Active Directory (support ref# 00036646).....	6
3.2	Base Policy no longer accepts Administrator accounts by default.....	6
3.3	Reporting from text file is no longer supported.....	6
3.4	Users can now control data point limits.....	6
4	Known Issues.....	7
4.1	Issues affecting Active Directory deployments.....	7
4.2	Issues affecting all deployments.....	7

1 Introduction

Welcome to the Release Notes for IDENTIKEY Server 3.4.

This document covers the following topics:

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

1.1 Main Application Versions

This release includes:

- ◆ IDENTIKEY Server 3.4.0.58
- ◆ Administration Web Interface 1.4.0.57

2 New Features and Enhancements

This chapter describes the different significant enhancements for the IDENTIKEY Server 3.4 release. For more information on each feature, refer to the [IDENTIKEY Server Administrator Guide](#) and [IDENTIKEY Server Product Guide](#).

2.1 Exclusion option for administrator accounts

This release features an option to prevent the usage of administrator accounts on authentication interfaces such as EMV-CAP authentication, signature validation, and provisioning. This option is configured via IDENTIKEY Server policy, and is useful in preventing attackers from locking administrator accounts via incorrect authentication attempts.

2.2 Temporary users

User accounts can now be configured to expire on a specified date and time. IDENTIKEY Server will automatically reject all authentication attempts via expired user accounts. In line with this new feature, the Administration Web Interface also provides reporting facilities for tracking user accounts that are expired or about to expire.

2.3 Thales nCipher support

With this release, IDENTIKEY Server now supports the following nCipher HSMs on 64-bit SUSE Linux 10:

- ◆ Thales nShield Connect
- ◆ Thales nShield Solo

2.4 Improved reporting performance

The Reporting scenario for this release has been further optimized, resulting in dramatic improvements to reporting performance. In addition, it is now possible to configure IDENTIKEY Server to adjust authentication performance by offsetting reporting performance, and vice-versa.

3 Fixes and Other Updates

This chapter enumerates major issues fixed in IDENTIKEY Server 3.4, along with notable changes to the way some features operate.

3.1 Fixed a DUR issue on Windows Active Directory (support ref# 00036646)

When IDENTIKEY Server was deployed with Active Directory storage, performing back-end authentication only (via group check) incorrectly updated the Active Directory attributes **vasco-ModifyTime** and **vasco-LastAuthTime**. This prevented the Dynamic User Registration feature from correctly creating new DIGIPASS users.

With IDENTIKEY Server 3.4, this issue is now resolved, and DUR works as expected.

3.2 Base Policy no longer accepts Administrator accounts by default

Administrator accounts can now be required, refused, or accepted for authentication via policy. For this, the default Base Policy was updated to only accept Administrator accounts on clients with the policy [Identikey Administration Logon](#).

3.3 Reporting from text file is no longer supported

In line with optimizing the Reporting scenario to improve reporting performance, creating reports directly from text file audit information is no longer supported. When upgrading to IDENTIKEY Server 3.4, IDENTIKEY Server will be reconfigured to create reports directly from database information.

To create reports from audit information stored on text file (i.e. when IDENTIKEY Server is configured to audit to text file), the audit information must first be imported to a database.

3.4 Users can now control data point limits

The reporting data point limit controls the maximum number of accepted data points. This limit is configured via the Report-Size-Limit parameter in the IDENTIKEY Server configuration file. Due to memory considerations, the default limit for the number of accepted data points is 100,000. If a report exceeds this limit, it will fail.

The recommended data point limit varies, depending on a system's available memory. With a data point limit of 100,000, a Detailed Authentication Report will only use around 300MB of memory, resulting in a report of approximately 2,500 pages.

Note that IDENTIKEY Server uses the third-party library Haru to generate PDF reports. Haru has an internal PDF size limit; increasing Report-Size-Limit increases the chances of reaching Haru's PDF size limit.

4 Known Issues

The following known issues exist in this release:

4.1 Issues affecting Active Directory deployments

The following issues only affect installations of IDENTIKEY Server 3.4 that use an Active Directory data store.

4.1.1 [12151 and 12152] Command-line DPX imports on Active Directory

At present, IDENTIKEY Server does not support importing DPX files via command line on Active Directory deployments. While the import process will succeed, any attempt to assign the DIGIPASS imported via this process will fail with the following error:

Error: -1: An unspecified error occurred (Failed to decrypt data using embedded crypto provider

This issue affects imports via the [dpximport.exe](#) tool and TCL. Because of this, users are advised to use the ADUCE interface to import DPX files in Active Directory instead.

4.1.2 [13236] Incorrect request handling on Windows member servers

When IDENTIKEY Server is installed on a Windows member server, it fails to write changes to the Active Directory data store with the following error:

Insufficient permission to perform action

To work around this, configure the IDENTIKEY Server service to run via domain service account.

4.2 Issues affecting all deployments

The following issues affect all installations of IDENTIKEY Server 3.4, regardless of data store.

4.2.1 [9619] Accepted Domain policy field

The **Accepted Domain** policy field does not restrict the domains with which users can log in. Do not use this attribute in implementing domain-based security policy.

4.2.2 [11865] Rescuing expired Administrator accounts

The Rescue Administrator feature cannot rescue expired Administrator accounts. As such, do not set an expiry date on the main Administrator account.

4.2.3 [12902] PDF reports filename extension

PDF reports are stored in the reports subdirectory of the IDENTIKEY Server installation with an incorrect XML filename extension.

4.2.4 [13903] Encrypted Attributes preventing bulk copying

When attempting to perform a Bulk User Attribute Copy with Encrypted Attributes enabled, the attempt will fail with an [invalid values](#) error. This is because IDENTIKEY Server will incorrectly use the masked value rather than the real value.

4.2.5 [13826] Migrating to IDENTIKEY Server 3.4 with Update existing records option

When using the [Data Migration Tool](#) to migrate to IDENTIKEY Server 3.4 from an older version of IDENTIKEY Server, enabling the Update existing records option will prevent Administrator user accounts from logging in. This is caused by changes to the Base Policy which relate to the updates described in [2.1 Exclusion option for administrator accounts](#) and [3.2 Base Policy no longer accepts Administrator accounts by default](#).

If this occurs, simply run the [Restore Default Policy and Report Definitions](#) wizard from the IDENTIKEY Server 3.4 [Configuration Wizard](#). Doing so will add the policy attributes necessary for Administrator user accounts to log in to IDENTIKEY Server 3.4.

4.2.6 [13985] Net-SNMP will not start after upgrade from IDENTIKEY Server 3.3 on Windows

After upgrading from IDENTIKEY Server 3.3 on Windows, Net-SNMP will no longer run. This is caused by the IDENTIKEY Server version change; as IDENTIKEY Server 3.4 is installed on a new directory, it can no longer communicate with Net-SNMP.

To work around this, manually uninstall Net-SNMP before upgrading from IDENTIKEY Server 3.3 to 3.4. Reinstall Net-SNMP as normal via the IDENTIKEY Server 3.4 upgrade process.

After upgrading to IDENTIKEY Server 3.4, you will still need to manually restart Net-SNMP.