DIGIPASS® Authentication for Remote Desktop Web Access
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

© 2012 VASCO Data Security International Inc. 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®, CertiID™, and the Vasco ‘V’ 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.

Date: 2012-02-23
# Table of Contents

1. Introduction .......................................................................................................................... 4  
   1.1 Main Application Versions ............................................................................................. 4  

2. New Features and Enhancements ......................................................................................... 5  
   2.1 Native Support of Internet Information Services (IIS) 7 (or Later) ....................... 5  
   2.2 Improved Configuration Workflow .............................................................................. 5  
   2.3 Improved Integration with IIS ...................................................................................... 5  

3. Fixes and Other Updates ...................................................................................................... 6  
   3.1 Deprecated Components and Features ...................................................................... 6  

4. Known Issues ...................................................................................................................... 7  
   4.1 Unknown Character Encoding .................................................................................... 7  

1 Introduction

Welcome to the Release Notes for DIGIPASS Authentication for Remote Desktop Web Access 3.4.0! This document describes new features and enhancements, as well as known issues.

1.1 Main Application Versions

This release includes:

- DIGIPASS Authentication for Remote Desktop Web Access 3.4.0
2 New Features and Enhancements

This chapter describes the different significant enhancements for the DIGIPASS Authentication for Remote Desktop Web Access 3.4 release.

2.1 Native Support of Internet Information Services (IIS) 7 (or Later)

With this release, DIGIPASS Authentication for Remote Desktop Web Access supports Internet Information Services (IIS) 7 or later.

2.2 Improved Configuration Workflow

Unlike with previous DIGIPASS Authentication Plug-In versions, restarting IIS is no longer required after you have made changes to the plug-in configuration.

2.3 Improved Integration with IIS

IIS Management Scripts and Tools is no longer needed to register the DIGIPASS Authentication Plug-In in IIS.
3  Fixes and Other Updates

This chapter enumerates major issues fixed in DIGIPASS Authentication for Remote Desktop Web Access 3.4, along with notable changes to the way some features operate.

3.1  Deprecated Components and Features

- The DIGIPASS Authentication Plug-In no longer supports VACMAN Middleware.
- With this release, the Flash challenge applet is no longer supported.
- With this release, Internet Information Services (IIS) 6 is no longer supported.
4 Known Issues

This chapter lists and describes known issues that exist in the DIGIPASS Authentication for Remote Desktop Web Access 3.4 release.

4.1 Unknown Character Encoding

If you specify character encoding (in the DIGIPASS Authentication Plug-In Configuration Center or the Settings.xml file) that is unknown to the product, an out-of-memory error will be reported in the plug-in’s trace file instead of the correct error message.