VASCO
THE AUTHENTICATION COMPANY

DIGIPASS
authentication

DIGIPASS® Authentication for Microsoft ADFS Release Notes

3.6

Disclaimer of Warranties and Limitations of Liabilities

Legal Notices

Trademarks

VASCO®, VACMAN®, IDENTIKEY®, aXsGuard®, DIGIPASS®, CertiID®, CRONTO™, CRONTOSIGN™, 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.

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.

Date: 2015-03-27

Table of Contents

1 Introduction

Welcome to the Release Notes for **DIGIPASS Authentication for Microsoft ADFS 3.6.0**!

DIGIPASS Authentication for Microsoft ADFS is an add-on authentication module for Microsoft Active Directory Federation Services (ADFS) 3.0 and provides strong authentication using a DIGIPASS authenticator.

DIGIPASS Authentication for Microsoft ADFS contains an ADFS authentication provider that can be used as an additional authentication method. This allows authentication against AD as the primary authentication, and authentication via a DIGIPASS authenticator as the additional authentication.

1.1 Main Application Versions

This release includes:

- DIGIPASS Authentication for Microsoft ADFS 3.6.0, 64-bit

2 New Features and Enhancements

This chapter describes the different significant enhancements for this release of DIGIPASS Authentication for Microsoft ADFS.

2.1 Version 3.6 (March 2015)

2.1.1 Supported Authentication Methods

DIGIPASS Authentication for Microsoft ADFS 3.6.0 supports the following authentication methods:

- Response-Only login
- 1-Step Challenge/Response login
- 2-Step Challenge/Response login
- Virtual DIGIPASS login

2.1.2 Server Connection Management

The DIGIPASS Authentication Module provides flexibility in managing connections to multiple primary and/or backup authentication servers. This allows redundancy and load sharing over multiple servers. This includes different connection profiles and options the module supports.

For further and more detailed information on the module features and functionalities, refer to the DIGIPASS Authentication for Microsoft ADFS Administrator Guide.

2.1.3 Software Requirements

For the operation of the DIGIPASS Authentication Module, the users must have administration rights on the machine where the module is installed. Also, the following software requirements must be met:

2.1.3.1 Authentication servers

- IDENTIKEY Authentication Server 3.6.1 or higher
- IDENTIKEY Appliance / IDENTIKEY Virtual Appliance 3.6.8.1 or higher

The authentication server must be pre-installed and running prior to the installation of the DIGIPASS Authentication Module.

2.1.3.2 Operating systems

- Microsoft Windows Server 2012 R2, 64-bit

2.1.3.3 Authentication services

- Microsoft ADFS 3.0

The authentication service must be pre-installed and running on the selected Windows server on which the DIGIPASS Authentication Module will be installed.