VASCO
THE AUTHENTICATION COMPANY

DIGIPASS
authentication

DIGIPASS Authentication for Windows Logon

Getting Started Guide

1.1

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

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 Implementing DIGIPASS Authentication for Windows Logon..... 4
1.2 Topics Not Included..... 5
1.3 Available Guides..... 5
2 Installation and Setup..... 7
2.1 What You Need Before Starting..... 7
2.2 IDENTIKEY Server Setup..... 7
2.3 ODBC Instructions..... 8
2.4 Active Directory Instructions..... 10
2.5 Client-Side Setup..... 11
3 Test Logins..... 12
3.1 Test Process Overview..... 12
3.2 Test Online Authentication Only..... 13
3.3 Test Dynamic Client Registration..... 14
3.4 Test Online Authentication with Offline Authentication Enabled..... 15
3.5 Test Offline Authentication..... 15
3.6 Test Password Randomization..... 15
4 Set Up Live System..... 17
4.1 Checklist..... 17
5 Set Up Live System with IDENTIKEY Server on Linux..... 18
5.1 Checklist for IDENTIKEY Server in Linux Environment..... 18

1 Introduction

This Getting Started Guide will introduce you to DIGIPASS Authentication for Windows Logon. It will help you set up a basic installation of DIGIPASS Authentication for Windows Logon and get to know the product and the tools it includes. It covers only basic information and the most common configuration requirements. Other options and more in-depth instructions are covered in other manuals.

1.1 Implementing DIGIPASS Authentication for Windows Logon

This guide covers a basic deployment of DIGIPASS Authentication for Windows Logon, suitable for an evaluation or simple setup.

There are instructions in this manual for ODBC and Active Directory installations. If no environment is specified the instructions are the same for both ODBC and Active Directory.

IDENTIKEY Server Requirements for ODBC

- IDENTIKEY Server 3.1 SR1 installed, with standard configuration and embedded Postgres ODBC database
- IDENTIKEY Administration Web Interface installed

> **Note**
>
> For the Active Directory installation an existing Active Directory environment is expected, containing only one domain.

IDENTIKEY Server Requirements for Active Directory

- IDENTIKEY Server 3.1 SR1 installed, with standard configuration, on a Domain member server or Domain Controller
- IDENTIKEY Administration Web Interface installed
- Active Directory Users and Computers
- DIGIPASS Extension for Active Directory Users and Computers installed
- Active Directory used as the data store for IDENTIKEY Server

Test machine

- Windows XP, 2003, Vista or 2008 installed

- Member of the Active Directory domain

1.2 Topics Not Included

This guide does not cover topics such as:

- Installation instructions
- Detailed introduction to DIGIPASS Authentication for Windows Logon, its features and components
- Detailed instructions on the use of DIGIPASS Authentication for Windows Logon

1.3 Available Guides

The following DIGIPASS Authentication for Windows Logon guides are available:

DIGIPASS Authentication for Windows Logon Product Guide

The Product Guide will introduce you to the features and concepts of DIGIPASS Authentication for Windows Logon and the various options you have for using it.

DIGIPASS Authentication for Windows Logon Getting Started Guide

The Getting Started Guide will lead you through a standard setup and testing of key DIGIPASS Authentication for Windows Logon features.

DIGIPASS Authentication for Windows Logon User Manual

For users of DIGIPASS Authentication for Windows Logon.

DIGIPASS Authentication for Windows Logon Installation Guide

The Installation Guide will help you install and configure DIGIPASS Authentication for Windows Logon to your requirements.

1.3.1 IDENTIKEY Server Guides

The following guides are available for IDENTIKEY Server:

Product Guide

The Product Guide will introduce the features and concepts of IDENTIKEY Server and the various options you have for using it.

Windows Installation Guide

Use this guide when planning and working through an installation of IDENTIKEY Server in a Windows environment.

Linux Installation Guide

Use this guide when planning and working through an installation of IDENTIKEY Server in a Linux environment.

Administrator Reference

In-depth information required for administration of IDENTIKEY Server. This includes references such as data attribute lists, backup and recovery and utility commands.

Getting Started Guide

The Getting Started Guide will lead you through a standard setup and testing of key IDENTIKEY Server features.

Performance and Deployment Guide

Contains information on common deployment models and performance statistics.

Help Files

Context-sensitive help accompanies the Administration Web Interface and DIGIPASS Extension for Active Directory Users and Computers.

SDK Programmers Guide

In-depth information required to develop using the SDK.

2 Installation and Setup

2.1 What You Need Before Starting

- Installation disk or executable
- DIGIPASS Authentication for Windows Logon Installation Guide

2.2 IDENTIKEY Server Setup

2.2.1 IDENTIKEY Server Version

IDENTIKEY Server 3.1 SR1 or greater is required for use with DIGIPASS Authentication for Windows Logon.

2.2.2 Installing DIGIPASS Authentication for Windows Logon

DIGIPASS Authentication for Windows Logon is delivered as part of the IDENTIKEY Server installation, for IDENTIKEY Server 3.1 SR1 or greater. To activate DIGIPASS Authentication for Windows Logon you must have the appropriate License Key.

2.2.3 Create Test Policy

To create the required Test Policy:

1. Open the Administration Web Interface.
2. Click on Policies -> Create.
3. Enter the required information:
   a. Policy ID: Test
   b. Inherits from: Windows logon online authentication - Windows Back-End
   c. Enter a description if desired.
4. Click on Create.

2.2.4 Create Client Record

Create a Client record for the Windows machine on which the Windows Logon Module will be installed. To do this:

1. Open the Administration Web Interface.
2. Click on Clients -> Register.
3. Enter the required information:
   a. Type: IDENTIKEY Windows Logon Client
   b. Location: FQDN of the machine
   c. Policy: Test Policy
4. Click on Create.

2.2.5 Create Test Windows Account

Create a Windows account for the Test User. Ensure that the user has sufficient permissions to log into the machine.

2.2.6 Test Standard Windows Logon

Log in to Windows on the test machine, using the test Windows User account and the static Windows password created for the account.

This test should succeed.

2.3 ODBC Instructions

2.3.1 Import User records

Demo Users may be used for the testing and familiarisation tasks in this guide. The .csv file for these is located in <IDENTIKEY Server installation directory>\dpx.

1. Open the Administration Web Interface.
2. Click on Users -> Import.
3. Enter or browse for the import path and filename for the .csv file. Click Upload.
4. On the Import Users tab, leave the settings as they are and click Import.
5. Click on Finish.

2.3.2 Import DIGIPASS Records

Before a DIGIPASS may be assigned to a User, a record for it must be imported into the data store. This record includes all important information about the DIGIPASS, including its serial number, Applications, and programming information. This information is transported to you in the form of a .dpx file.

A Response Only DIGIPASS Application is required for Windows Logon.

Demo DIGIPASS may be used for the testing and familiarisation tasks in this guide. The .dpx file for these is located in <IDENTIKEY Server installation directory>\dpx.

To import DIGIPASS records:

1. Open the Administration Web Interface.
2. Click on Digipass -> Import.
3. Enter or browse for the import path and filename for the DPX file.
4. Enter the transport key – this is 11111111111111111111111111111111 for the installed demo DIGIPASS DPX files (press the 1 key 32 times).
5. Click on Upload.
6. On the Applications tab ensure the applications are selected, and click Next.
7. On the Options tab click Import.
8. Click Finish on the Summary tab.

2.3.3 Assign DIGIPASS to Test User

Before a User can use a DIGIPASS to login, the DIGIPASS must be assigned to their User account within the data store.

To assign a DIGIPASS record to the Test User account:

1. Open the Administration Web Interface.
2. Click on Users -> Assign Digipass.
3. Leave all settings as they are. Click Search.
4. Click the check box to select a User. Click Next.
5. On the Search Digipass tab leave all the settings as they are. Click Search.
6. If more than one DIGIPASS is available, click the check box to select a DIGIPASS. Click Next.
7. On the Options tab click Assign.
8. Click Finish on the Finish tab.

2.4 Active Directory Instructions

2.4.1 Create a Test DIGIPASS User record

1. Open the Active Directory Users and Computers snap-in.
2. Find the test User account created earlier.
3. Double-click on the **User** account.
4. Click on the **Digipass User Account** tab.
5. Tick the **Enable Digipass** checkbox.
6. Click on **OK**.

2.4.2 Import DIGIPASS Records

Before a DIGIPASS may be assigned to a DIGIPASS User, a record for it must be imported into the data store. This record includes all important information about the DIGIPASS, including its serial number, Applications, and programming information. This information is transported to you in the form of a .dpx file.

A Response Only DIGIPASS Application is required for Windows Logon.

Demo DIGIPASS may be used for the testing and familiarisation tasks in this guide. The .dpx file for these is located in <**IDENTIKEY Server installation directory**>\dpx.

To import DIGIPASS records:

1. Open the Active Directory Users and Computers snap-in.
2. Right-click on Users.
3. Select Import Digipass.
4. Click on **Next**.
5. Enter or browse for the import path and filename for the DPX file.
6. Enter the transport key – this is 11111111111111111111111111111111 for the installed demo DIGIPASS DPX files (press the 1 key 32 times).
7. Click on **Next**.
8. Click on **OK**.

2.4.3 Assign DIGIPASS to Test User

Before a User can use a DIGIPASS to login, the DIGIPASS must be assigned to their User account within the data store.

To assign a DIGIPASS record to the Test User account:

1. Open the Active Directory Users and Computers snap-in.
2. Find the test User account created earlier.
3. Right-click on the User account.
4. Select **Assign Digipass**.
5. Search for DIGIPASS using the criteria on the **Search Digipass** tab.
6. Select **Search Now** to select a specific DIGIPASS to assign.
7. Select DIGIPASS from list if more than one is found.
8. Click **Next**.
9. Click **Assign**.
10. Click on **Finish**.

2.5 Client-Side Setup

2.5.1 Install the DIGIPASS Windows Logon Client

Install the Windows Logon Module on the test Windows machine. See the DIGIPASS Authentication for Windows Logon Installation Guide for more information.

2.5.2 Configure the DIGIPASS Windows Logon Client

Configure the Client to connect to the IDENTIKEY Server configured in 2.2 IDENTIKEY Server Setup.

See the DIGIPASS Authentication for Windows Logon User Manual for more information.

2.5.3 SSL Certificate

During IDENTIKEY Server installation, a self-signed SSL server certificate can be generated. This certificate can be used for all communication between the DIGIPASS Windows Logon clients and IDENTIKEY Server.

This self-signed certificate must be imported in the Windows certificate repository of the test machine where Windows Logon client is installed.

See the DIGIPASS Authentication for Windows Logon Installation Guide for more information.

3 Test Logins

This section will guide you through testing both online and offline OTP logins.

3.1 Test Process Overview

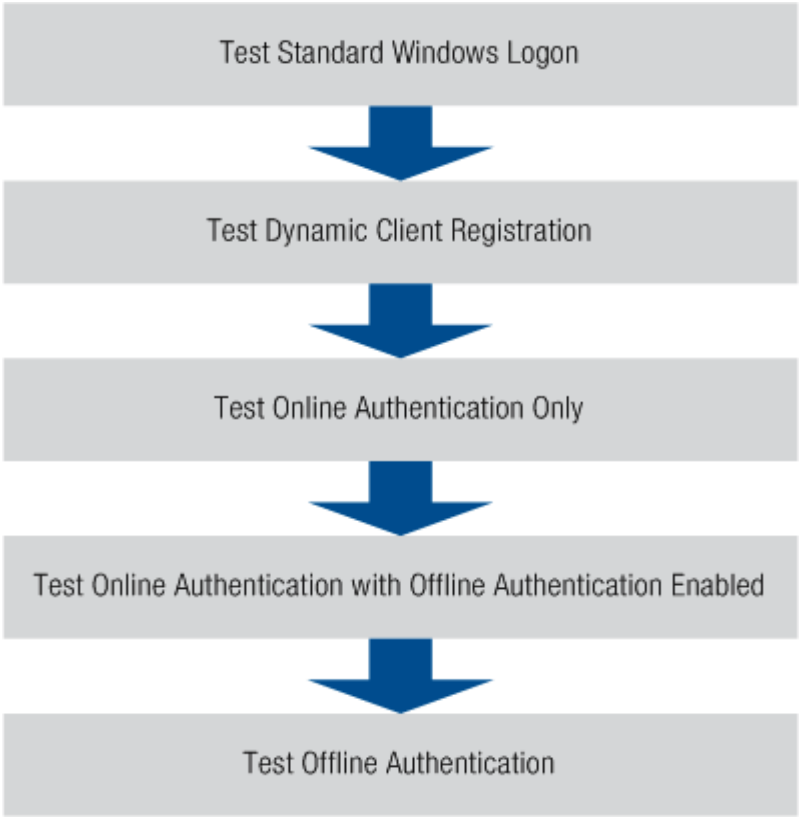

Image : Test Process Overview

3.1.1 Test Pre-requisites

If you are going to test all types of login methods and authentication options available, you will need:

- A DIGIPASS User account with a corresponding Windows User account
- A stored static password which is the same as the Windows account's password
- A DIGIPASS or Demo DIGIPASS with Response Only Application assigned to the DIGIPASS User account.
- A new Policy named 'Test'.

3.1.2 Modifying the Test Policy

Each scenario will require modification of the Test Policy created in 2.2.3 Create Test Policy. Use these instructions to edit the Test Policy:

1. Open the Administration Web Interface.
2. Click on Policies -> List.
3. Find and click on the Test Policy.
4. Click on the required tab:
   - Local Authentication and Back-End Authentication settings can be found under the Policy tab
   - Dynamic User Registration, Password Autolearn and Stored Password Proxy settings can be found under the User tab.
   - Application Type, Assignment Mode, Grace Period, Serial Number Separator and Search Upwards in Org. Unit Hierarchy settings can be found under the Digipass tab.
5. Click on Edit.
6. Make the required changes.
7. Click on Save.

3.2 Test Online Authentication Only

3.2.1 Static Password

Modify Test Policy

Make these changes to the Test Policy (see 3.1.2 Modifying the Test Policy for instructions):

- Set Local Auth. to Digipass/Password.
- Set Password Autolearn to Yes.

Check Grace Period

Check the record for the DIGIPASS being used for testing. The grace period should be set for a time in the future. If it is not, the static password login will fail.

Test Login

Attempt a test login using the test User's User ID and static Windows password.

The login should succeed.

3.2.2 One Time Password

Modify Test Policy

Make these changes to the Test Policy (see 3.1.2 Modifying the Test Policy for instructions):

- Set Application Type to Response Only.

Test Login

Attempt a test login using the test User's User ID and the current One Time Password from the test User's token.

The login should succeed.

3.2.3 Retest Static Password

Check Grace Period

Using the Active Directory Users and Computers snap-in, check the record for the DIGIPASS being used for testing. The grace period should be set for a time in the past.

Test Login

Attempt a test login using the test User's User ID and static Windows password.

The login should fail.

3.3 Test Dynamic Client Registration

> **Note**
>
> Dynamic Component Registration will fail if a PTR record does not exist on the DNS server for the client machine. A reverse zone must be implemented in order for DCR to function correctly.

Modify Test Policy

Make these changes to the Test Policy (see 3.1.2 Modifying the Test Policy for instructions):

- Set Dynamic Component Registration to Enabled.

Delete Client Record

Using the Administration Web Interface, delete the Client record in IDENTIKEY Server for the test Windows machine.

Test Login

Attempt a test login using the test User's User ID and the current One Time Password from the test User's token.

The login should succeed.

Check the Client List in the Administration Web Interface. A record should now exist for the test Windows machine.

3.4 Test Online Authentication with Offline Authentication Enabled

Modify Test Policy

Make these changes to the Test Policy (see 3.1.2 Modifying the Test Policy for instructions):

- Set **Offline Authentication** to Enabled

Tracing

Enable Tracing in the DIGIPASS Windows Logon Client.

Test Login

Log in to Windows using an OTP.

The login should succeed.

Check the trace file to see if data was returned.

3.5 Test Offline Authentication

1. Disconnect the test machine from the network.
2. Log in to Windows on the test machine, with the Test User account, using an One Time Password.

The login should succeed.

3.6 Test Password Randomization

Modify Test Policy

Make these changes to the Test Policy (see 3.1.2 Modifying the Test Policy for instructions):

- Set **Password Randomization** to Enabled

Connectivity

Reconnect the test machine to the network.

Test Login

1. Log in to Windows, with the Test User account, using an OTP.
2. Log out.
3. Uninstall the Windows Logon Module from the test machine.
4. Restart the machine.
5. Attempt a login to the test computer, with the Test User account, using the old Windows password only.

The login should fail.

4 Set Up Live System

4.1 Checklist

- ❒ **Import More DIGIPASS**
  Import all required DIGIPASS records
- ❒ **Create DIGIPASS User Accounts**
  If required, manually create DIGIPASS User accounts. Alternatively, enable Dynamic User Registration in DIGIPASS Authentication for Windows Logon.
- ❒ **Assign DIGIPASS records to DIGIPASS User Accounts**
  Decide on the type of DIGIPASS assignment to deploy, and begin the deployment process.
- ❒ **SSL Server Certificate**
  Acquire and install a commercial SSL certificate for each IDENTIKEY Server
- ❒ **Register IDENTIKEY Servers with DNS Server**
  If the DIGIPASS Windows Logon module will be using the IDENTIKEY Server Discovery feature, use the Administration Web Interface to register each IDENTIKEY Server with its local DNS server.
- ❒ **Configure default Windows Logon Client record**
  Ensure that the default Windows Logon Client record uses the correct settings for a live environment, as this record will be used for all Client records created via Dynamic Client Registration. In particular, ensure that it links to the correct Policy for your setup.
- ❒ **Configure Dynamic Client Registration**
  If required, enable Dynamic Client Registration in the Policy used by the default Windows Logon client.
- ❒ **Install Password Synchronization Manager**
  Install the Password Synchronization Manager on a Domain Controller. This will allow IDENTIKEY Server to receive updates on any Windows static password changes for DIGIPASS Users.
- ❒ **Install and Configure DIGIPASS Windows Logon client**
  The DIGIPASS Windows Logon client should be installed on all machines which will be used in One Time Password logins. Configuration should include:
  - IDENTIKEY Server Discovery, if required
  - Location of a specific IDENTIKEY Server if Server Discovery is not enabled

5 Set Up Live System with IDENTIKEY Server on Linux

You can use DIGIPASS Authentication for Windows Logon with IDENTIKEY Server in a Linux environment. To do this you must have an Active Directory back-end, and the following rules must be applied:

1. If Active Directory has been installed with SSL enabled, a CA certificate must be installed with Active Directory.It must be copied to the IDENTIKEY Server <install directory>\VASCO\Identikey 3.2\certs directory using one of the following methods:

   a. Go to the certificate Store on Windows and export the certificate(s). The certificates will be exported as .cer files, and they must be converted to .pem files.

      OR

      Use the following command:

      openssl s_client -connect <name of domain controller>

      Copy each certificate returned into its own file and save each as a .pem file.

   b. Whether the certificate is downloaded or exported from Windows, the .pem file must be renamed by first using the following command to acquire the hash:

      openssl x509 -noout -hash -in certname.pem

   c. Record the hash which is the result of this command, and rename the .pem file to be hashvalue.0. For example, if the hash result is 54321, the certname.pem file created above will be renamed to 54321.0. The newly renamed file must be saved in:

      Windows

      <IDENTIKEY Server install-dir>\certs.

      Linux

      In the chroot environment,

      etc/ssl/certs

All the tests detailed in 2 Installation and Setup can be carried out on the Linux system in just the same way.

5.1 Checklist for IDENTIKEY Server in Linux Environment

- ❒ **Import More DIGIPASS**
  Import all required DIGIPASS records
- ❒ **Create DIGIPASS User Accounts**
  If required, manually create DIGIPASS User accounts. Alternatively, enable Dynamic User Registration in DIGIPASS Authentication for Windows Logon.

- ❒ **Assign DIGIPASS records to DIGIPASS User Accounts**
  Decide on the type of DIGIPASS assignment to deploy, and begin the deployment process.

- ❒ **SSL Server Certificate**
  Acquire and install a commercial SSL certificate for each IDENTIKEY Server

- ❒ **Copy and rename Active Directory SSL Certificates**
  Copy Active Directory SSL Certificates to X509 format and save to appropriate location.

- ❒ **Register IDENTIKEY Servers with DNS Server**
  If the DIGIPASS Windows Logon module will be using the IDENTIKEY Server Discovery feature, use the Administration Web Interface to register each IDENTIKEY Server with its local DNS server.

- ❒ **Configure default Windows Logon Client record**
  Ensure that the default Windows Logon Client record uses the correct settings for a live environment, as this record will be used for all Client records created via Dynamic Client Registration. In particular, ensure that it links to the correct Policy for your setup.

- ❒ **Configure Dynamic Client Registration**
  If required, enable Dynamic Client Registration in the Policy used by the default Windows Logon client.

- ❒ **Install Password Synchronization Manager**
  Install the Password Synchronization Manager on a Domain Controller. This will allow IDENTIKEY Server to receive updates on any Windows static password changes for DIGIPASS Users.

- ❒ **Install and Configure DIGIPASS Windows Logon client**
  The DIGIPASS Windows Logon client should be installed on all machines which will be used in One Time Password logins. Configuration should include:
  - IDENTIKEY Server Discovery, if required
  - Location of a specific IDENTIKEY Server if Server Discovery is not enabled